Příloha č. 1: Technická specifikace

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

OBSAH

VYUŽITÉ ZDROJE

Nejsou

SEZNAM TABULEK

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
365x7x24	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
ACL	Access Control List
AD	Microsoft Active Directory
AVL	Systém sledování polohy vozidel
CD / CD-ROM / DVD / USB	Datový nosič
ČR	Česká republika
DB	Databáze
DC	Datové centrum
EKP	Elektronická karta pacienta
EU	Evropská unie
FW	Firewall
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob
GIS	Geografický informační systém
GUI	Grafické uživatelské rozhraní
HW	Hardware
HZS (ČR)	Hasičský záchranný sbor České republiky
ICT	Informační a komunikační technologie
IOP	Integrovaný operační program
IP	Internet Protocol
IROP	Integrovaný regionální operační program
IS	Informační systém
IT	Informační technologie
IZS	Integrovaný záchranný systém
KII	Kritická informační infrastruktura
ks	Počet kusů
LAN	Lokální počítačová síť

Zkratka/pojem	Význam
LCT	Linkový radiový komunikační terminál radiové sítě Pegas/Matra
MS	Microsoft
MV ČR	Ministerstvo vnitra České republiky
MZD	Mobilní zadávání dat
NDIC	Národní dopravní informační centrum
NIS IZS	Národní informační systém IZS
OŘ	Operační řízení
OS	Operační systém
PAK	Pardubický kraj
PČR	Policie České republiky
PD	Projektová dokumentace
PNP	Přednemocniční neodkladná péče
RCT	Radiový komunikační terminál radiové sítě Pegas/Matra
SaP	Síly a prostředky
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory
SMS	Krátká textová zpráva
SNMP	Simple Network Monitoring Protocol
SQL	Strukturovaný dotazovací jazyk pro práci v relačních databázích
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

Zkratka/pojem	Význam
ZZOS	Záložní zdravotnické operační středisko
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS PAK	Zdravotnická záchranná služba Pardubického kraje

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

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

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

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

1. Informační systém zdravotnického operačního střediska ZZS PAK – jedná se o primární IS sloužící pro hlavní činnost ZZS PAK, tj. poskytování PNP na území Pardubického kraje.
2. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS PAK zajišťující komunikaci mezi zaměstnanci ZZS PAK 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 PAK 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 PAK 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. 4 – Rozsah dodávky a souvisejících služeb.

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

2 ČLENĚNÍ DOKUMENTU

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

- **Kapitola 3 – Předmět a rozsah dodávky** – kapitola obsahuje požadavky na dodávky a služby (Dílo), které musí zhotovitel splnit ve svém řešení a ve své nabídce. Kapitola obsahuje základní koncept řešení, legislativní požadavky, konkrétní funkční a technické požadavky na řešení předmětu plnění v rámci VZ.
- **Kapitola 5 - Harmonogram** – kapitola obsahuje harmonogram realizace předmětu plnění VZ.
- **Kapitola 6 – Místa plnění** – kapitola obsahuje místa plnění v rámci realizace předmětu plnění VZ.
- **Kapitola 7 – Výchozí stav** – kapitola obsahuje popis výchozího stavu pro realizaci předmětu VZ, tj. uvedení seznamu dotčených subjektů, jejich vztah k předmětu VZ, informační a komunikační technologie a vybavení, kterými subjekty disponují nebo které budou k dispozici pro realizaci VZ, případně další organizační a technické podmínky, které jsou důležité pro realizaci VZ.

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

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

3 PŘEDMĚT A ROZSAH DODÁVKY

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

Cílem projektu je zvýšení kybernetické bezpečnosti pro následující IS:

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

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

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

b) nástroj pro ochranu integrity komunikačních sítí

c) nástroj pro ověřování identity uživatelů

e) nástroj pro ochranu před škodlivým kódem

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

j) kryptografické prostředky

i) aplikační bezpečnost

Rozsah dodávky je uveden v následující kapitole.

4 ROZSAH DODÁVKY A SOUVISEJÍCÍCH SLUŽEB

4.1 VYMEZENÍ PŘEDMĚTU A ROZSAHU DODÁVKY

Rozsah dodávky je následující:

#	Položka rozpočtu	Počet	Stručný popis položky
1	FireWall(y) s IPS pro ZOS	1 soubor	Dodávka Firewallu s IPS pro ochranu interní sítě ZZS, segmentů sítě ZZS a pro ochranu proti útokům z externích sítí v ZOS včetně zajištění vysoké dostupnosti. Součástí je dodávka, instalace, nastavení, propojení s dalšími síťovými prvky, implementace nastavení a pravidel a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
2	Aplikační firewall pro IS ZOS	1 ks	Dodávka aplikačního firewallu pro IS ZOS který bude chránit webové služby před potenciálními útočníky, kteří by mohli využít zranitelná místa aplikací nebo protokolů pro sledování nebo modifikaci dat nebo ohrožení chodu takové aplikace. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
3	Systémy pro sběr dat (logů) o síťovém provozu	1 soubor	Dodávka systémů pro sběr dat (logů) o síťovém provozu a to jak na vstupu do interních sítí tak také v rámci serverů VMWare. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby.
4	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí	1 soubor	Dodávka systému analýzy bezpečnostních logů (OŘ/infrastruktura). Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a související služby.
5	Analytické nástroje pro ZOS ZZS PAK	1 soubor	Dodávka analytického nástroje pro ZOS ZZS PAK pro vytváření bezpečnostních analýz. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a související služby.
6	Pokročilé notifikační nástroje	1 soubor	Dodávka pokročilého notifikačního nástroje nejenom pro bezpečností události ale i pro mimořádné události OŘ.

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

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

#	Položka rozpočtu	Počet	Stručný popis položky
			a následné periodické testování bezpečnostních zranitelností systémů, které komunikují s externími subjekty. Součástí je dodávka, instalace, nastavení, implementace a související služby.
17	Bezpečnostní audit a penetrační testy	1 soubor	Bezpečnostní audit a penetrační testy v souladu se standardy ZKB a závěrečných testů zranitelnosti z externí sítě na systémy IS ZOS a Elektronickou poštu.

Tabulka 2: Předmět a rozsah dodávky

4.1.1 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení
2. Provedení bezpečnostního auditu.
3. Zpracování návrhu dodávky a konfigurace technických opatření v souladu s výstupy a doporučeními vyplývající z bezpečnostního auditu, související konzultace.
4. Dodávka, implementace, instalace, zapojení a konfigurace technických opatření v souladu s výstupy a doporučeními vyplývající z bezpečnostního auditu.
5. Konfigurační změny zabezpečovaných IS a implementace změn informačních systémů a jejich součástí.
6. Ověření funkčnosti dodaných technologií, zabezpečovaných IS a jejich (sou)částí.
7. Provedení penetračních testů.
8. 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.
9. Zpracování bezpečnostní dokumentace včetně hodnocení aktiv a rizik s tím, že bezpečnostní dokumentace by měla plně reflektovat veškeré technologické a funkční změny.
10. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem (správci).
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 PAK. Po stránce nepřetržitého provozu ZZS PAK předpokládá pouze plánovanou odstávku pouze na nezbytnou dobu.
2. Požaduje se kontinuita nastavených parametrů IS a existujících technologií a jiných aspektů provozu. Nepředpokládá investici do opětovného zadávání a pořizování těchto údajů.

4.1.2 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou dotčeny následující oblasti stávajícího řešení:

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

4.1.3 Vyloučení z dodávky

Předmětem dodávky není:

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

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

4.2 VÝCHODISKA A PŘIPRAVENOST

Pro řešení jsou stanovena následující východiska:

#	Popis východiska
1.	Zdravotnická záchranná služba Pardubického kraje je základní složkou IZS a v souladu s legislativou plní úkoly i v případě mimořádných událostí a krizových situací, kdy může být těmito událostmi/situacemi zasaženo i zdravotnické operační středisko (ZOS) a došlo by tedy k omezení, případně znemožnění poskytování úkolů ZZS PAK. Z uvedeného plyne, že informační systémy podporující procesy poskytování PNP ze strany ZZS PAK 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 Pardubického kraje“, který byl Pardubickým krajem realizován pro Zdravotnickou záchrannou službu Pardubického kraje (ZZS PAK) v rámci Integrovaného operačního programu (IOP), výzvy č. 11. Současné řešení musí plnit podmínku zajištění udržitelnosti projektu „Krajský standardizovaný projekt zdravotnické záchranné služby Pardubického 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.	V roce 2019 probíhá realizace a bude dokončen projekt „Rozvoj informačních systémů a technologií ZZS PaK – záložní zdravotnické operační středisko“ v rámci IROP, výzvy č. 28, registrační číslo CZ.06.3.05/0.0/0.0/16_044/0005151. V tomto projektu je budováno záložní ZOS (IS ZZOS) v záložní lokalitě (VZ Chrudim). Technologie a rozšíření ZOS a vybudování ZZOS jsou předmětem zabezpečení technologiemi dodávanými v rámci dodávek uvedených dále v tomto dokumentu.
4.	Připravenost datových center bude zajištěna min. v následujícím rozsahu: 1. Dostatečně kapacitní napájení datového centra pro umístění technologií. 2. Klimatizace v datovém centru. 3. Strukturovaná kabeláž v rámci DC, mezi DC a mezi dodávanými technologiemi a zabezpečovanými IS. 4. Napojení na ostatní komunikační technologie.

#	Popis východiska
5.	Nutnost zajištění ochrany osobních údajů a bezpečnosti v souladu s legislativou a moderními principy – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR), zákona č. 181/2014 Sb. – Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a požadavky kladené na KII.

Tabulka 3: Východiska

Další východiska jsou definována výchozím stavem uvedeným v kap. 7 – Výchozí stav.

4.3 ZÁKLADNÍ POŽADAVKY NA ZABEZPEČENÍ IS

Základní požadavky na požadované řešení jsou následující:

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

Detailní popis požadavků na dodávky je uveden v následující kapitole.

4.4 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

4.4.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

#	Požadavek
P.1	Dodávané technologie musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR).
P.2	Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy a technologiemi ZZS PAK.
P.3	Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz dodávaných technologií min. po dobu účinnosti servisní smlouvy.
P.4	Zaručená perspektiva rozvoje a podpory je minimálně po dobu dalších 6 let od uvedení do provozu.

#	Požadavek
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.

4.4.2 FireWall(y) s IPS pro ZOS

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

#	Požadavek
FireWall s IPS pro ZOS	
P.11	Dodávka redundantního firewallu s IPS pro řízení bezpečného přístupu mezi vnějšími sítěmi (internet, NIS IZS, PČR atd.) a vnitřní sítí ZZOS a ZOS.
P.12	Dodávka redundantního FireWallu pro primární ZOS: 1. Může se jednat jak o rozšíření stávajícího řešení (viz kapitola 7.4 – Stav ostatních informačních a komunikačních technologií) nebo o jeho nahrazení. 2. FireWall bude oddělovat externí sítě připojené v rámci primární ZOS (internet apod.) 3. Stavový aplikační firewall jako samostatné HW zařízení, který musí nabízet a. Dynamický a statický NAT/PAT (překlad IP adres). b. Podporu dynamických směrovacích protokolů RIP, OSPF, BGP a Policy based Routing. c. Plnou podporou protokolu IPv6.

#	Požadavek
	d. Realizace redundance pro případ výpadku ve formě Active/Active failover, Active/Standby failover (redundance se stávajícím prvkem nebo jeho nahrazení a zajištění redundance nově dodanými prvky). e. Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru. f. Podpora filtrace Ipv4, Ipv6 a filtrace podle identity uživatele nebo jeho skupiny definované v AD. 4. Aplikační firewall a. Pokročilá hloubková analýza dat na aplikačních vrstvách ISO modelu b. Podpora pasivního monitorování (TAP režim) c. Rozeznávání a kategorizace aplikací, geografických lokalit, uživatelů d. Možnost rozšíření o identifikace a zamezení přístupu na nedůvěryhodné či škodlivé webové stránky – filtrace podle reputace serverů e. Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, uzly botnet sítí f. Možnost integrovat vlastní reputační databáze 5. IPS senzor, který musí nabízet a. Možnost definovat typ provozu předávaný k inspekci do IPS b. Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti c. IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií d. Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací e. IPS musí umět detekovat a blokovat útoky průzkumných aktivit f. IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS g. IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C h. aktuálních databázích AV dodavatelů i. Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry j. Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat k. Podpora databází reputací adres v internetu (Security Intelligence) 6. VPN koncentrátor a. Zakončení „full-tunnel“ IPSec nebo SSL VPN pro alespoň 300 současné připojených uživatelů – licence pro 25 uživatelů b. Možnost rozšíření (licence apod.) „odlehčené“ SSL VPN pro uživatele formou zabezpečeného přístupu na webový portál bez nutnosti tlustého klienta c. Zakončení alespoň 300 současně připojených site-to-site Ipsec tunelů d. Implementace Ipsec musí podporovat protokoly IKEv1 i IKEv2 a šifrovací standardy 3DES/AES a algoritmy nové generace popsané ve standardu NSA Suite-B

#	Požadavek
	7. Výkonnostní parametry a provedení a. Minimální propustnost NGFW (hloubková inspekce) 850 Mbps b. Minimální propustnost NGFW (hloubková inspekce + IPS modulem) minimálně 450 Mbps. c. Minimální propustnost pro Ipsec VPN komunikaci (šifrování 3DES/AES) 250 Mbps d. Formát zařízení Appliance v provedení do racku max 2RU e. Samostatný port pro management f. Minimální 8 portů pro data 10/100/1000 BaseT Ethernet g. Podporovaný počet VLAN min. 100 Součástí dodávky je implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) Podpora na 5 let typu NBD pro celé dodané řešení této části, oprava v místě instalace zařízení včetně aktualizací všech signatur a SW komponent včetně jejich funkčnosti.
P.13	Umístění firewallu s IPS do DC v rámci primárního zdravotnického operačního střediska.
P.14	FireWall musí být v redundantním provedení (HW a SW).
P.15	Nastavení pravidel pro kontrolu přístupu do segmentů IS ZOS a ZZOS z externích sítí před případnými externími i interními útoky. Konfigurace FireWallu bude realizována na základě požadavků ZZS s přihlédnutím ke konfiguraci stávajících oprávnění v rámci centrálního FireWallu v ZOS. Nastavení bude umožňovat bezproblémový chod IS OŘ ze ZOS (stávajících technologií) včetně využití připojení k externím sítím v ZOS (internet apod.). Pro konfiguraci přístupu vzdálených uživatelů v rámci VPN bude využito stejné konfigurace jako v době implementace FW (centrální RADIUS serverů), tak aby byla umožněna jednotná konfigurace těchto přístupů bez ohledu na lokalitu přístupu. *Konfigurace stávajících firewallů a nastavení sítě budou poskytnuty v rámci implementační analýzy.*
P.16	Výchozí nastavení pravidel pro alertování upozorňující na bezpečnostní události detekované na tomto bezpečnostním prvku. *Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v rámci implementační analýzy.*
P.17	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5). Včetně specifikace korelace kritických bezpečnostních alertů z tohoto bezpečnostního prvku týkajících se IS ZOS.
P.18	Dodávka FireWallu jako kompaktního zařízení, tj. HW včetně vnitřního SW zajišťujícího všechny požadované funkcionality. Pro případný podpůrný SW sloužící pro instalaci, konfiguraci a aktualizace FW ZZS umožní využití stávající virtualizační infrastruktury ZZS za předpokladu, že nepřesáhne požadavek na jeden server (4 vCPU, 8 GB RAM a 500 MB vHD, OS MS Windows Server 2016 Standard nebo Linux). V případě

#	Požadavek
	vyšších požadavků na server dodavatel dodá i nezbytný HW a systémový SW včetně licencí pro běh podpůrného SW (HW ve verzi rack mount).
P.19	Možnost aktivace/deaktivace izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů ze systému IS OŘ (viz kap. 4.4.8 – Úpravy IS ZOS). Vlastní izolace bude provedena na firewallech v rámci ZOS (součástí dodávky) a ZZOS (součinnost poskytne ZZS).
P.20	Bude proveden detailní záznam událostí izolace systému IS ZOS včetně jejich časové souslednosti, případně o uživatelích, kteří opatření realizovali, a to jak do logu IS OŘ, tak do systému analýzy bezpečnostních logů (viz kap. 4.4.5).

Tabulka 5: FireWall(y) s IPS pro ZOS

4.4.3 Aplikační firewall pro IS ZOS

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

#	Požadavek
P.21	Dodávka webového aplikačního firewallu pro zabezpečení webových služeb (web services) v rámci externí komunikace IS ZOS. Minimálně je třeba zabezpečit následující aplikace: 1. Endpoint NIS IZS (SOS5) – publikováno do sítě NIS IZS 2. SOSView – publikováno do sítě Internet Jedná se o služby IS ZOS dostupné z externích sítí.
P.22	Funkcionalita webového aplikačního firewallu (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu s minimální propustností 200Mbps. K těmto základním bezpečnostním politikám požadujeme implementaci dalších dodatečných bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem.
P.23	Je požadováno, aby WAF obsahoval technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní robotické klienty). WAF také zajistí ochranu před únosy HTTP relací. WAF musí podporovat SSL terminaci.
P.24	Aplikační firewall musí plnit následující min. parametry: 1. Ochrana proti aplikačním DoS a DDoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky, SYN flood, HTTP flood aj.) 2. Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, remote command execution a ostatním útokům podle OWASP Top 10 3. Ochrana proti manipulaci s cookies 4. Ochrana parametrů webové aplikace 5. Session Management – ochrana proti únosům relací 6. Brute Force Ochrana – ochrana před prolomení hrubou silou

#	Požadavek
	7. Detekce a potlačení robotických uživatelů aplikace 8. Ochrana AJAX a JSON aplikací, zabezpečení XML komunikace 9. Možnost rozšíření o detekci a ochranu před robotickými klienty pro nativní mobilní aplikace IOS a Android 10. Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům) 11. Automatická instalace a aktualizace databáze pro detekci útoků, botnetů nebo kampaní kybernetických útoků 12. Blokování útočníků na základě geolokace 13. Podpora různých typů reportů – PCI, geolokační reporty, OWASP Top 10 14. Identifikace zařízení a potlačení škodlivých zařízení v bezpečnostní politice (fingerprinting) 15. Podpora rozkládání zátěže na více než 3 servery a podpora různých typů mechanismů rozkladu zátěže, minimálně kruhová metoda (round-robin), vážená kruhová metoda s (weighted round-robin) podle počtu spojení 16. Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, HTTP cookie 17. Podpora REST API pro správu a monitoring zařízení 18. Možnost doprogramovat filtrovací pravidla pro aplikace 19. Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force), mitigace DDoS útoků založená na behaviorální analýze 20. Podpora SSL (šifrování a dešifrování) 21. Povoleni jednotlivých HTTP metod pro jednotlivá URL 22. Detekce anomálií a podezřelých operacích na aplikační vrstvě 23. implementace (instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 24. záruka a aktualizace SW apod. na 5 let.
P.25	Implementace WAF na externě dostupné aplikace IS ZOS včetně jejich optimalizací a nastavení pravidel optimalizovaných pro chod těchto aplikací/rozhraní s ohledem na jejich funkčnost a dostupnost s detailní znalostí těchto aplikací/rozhraní.
P.26	Pro chod aplikačního FW je možné využít jak HW, který bude součástí dodávky řešení (viz kap. 4.4.8) 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.27	Umístění aplikačního firewallu do DC v rámci primárního zdravotnického operačního střediska. S možností migrace do ZZOS v případě plné aktivace ZZOS (s možností využití stávající virtualizační platformy ZZOS).
P.28	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5). WAF musí podporovat logování ve formátu minimálně Syslog, a případně s navrženým logovacím systémem (viz kap. 4.4.5).

#	Požadavek
	Součástí předávání logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí musí být veškeré kritické bezpečnostní události související s chráněnými aplikacemi ZOS a případných útocích na ně vedených. Součástí předávaných logů musí být také varování před nestandartními stavy jako jsou anomální nárůsty požadavků, pokusy o přístup do nepublikovaných částí aplikací apod. WAF musí dále předávat logy o veškerých přístupech (úspěšné i neúspěšné) do managementu WAF a informace o změnách konfigurací WAF.

Tabulka 6: Aplikační firewall pro IS ZOS

4.4.4 Systémy pro sběr dat (logů) o síťovém provozu

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

#	Požadavek
P.29	Je požadováno ucelené škálovatelné řešení umožňující dlouhodobé i real – time monitorování sítě na bázi technologie NetFlow složené z: 1. Sondy síťového provozu (virtuální i fyzické) 2. Kolektoru síťového provozu 3. Modul automatického vyhodnocování IP toků
P.30	Minimální požadovaná funkční specifikace sondy pro virtualizační platformu: 1. specializované dedikované zařízení (sonda) ve formě virtuálního zařízení virtualizační platformy pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5, v9, IPFIX) včetně pokročilých funkcí filtrování exportů, rozpoznávání aplikací, extrakce informací o http a SIP provozu a sledování performance metrik (server response time, jiter, round trip time, delay), 2. dostupné jako virtuální zařízení pro navrženou virtualizační platformu, 3. sonda s 1 monitorovacím portem 10GbE, 4. detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik, podpora monitorování MAC adres, standardů NEL, NSEL, 5. podpora vzorkování na úrovni paketů i toků, 6. podpora filtrování a export datových toků na základě AS, 7. zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS, 8. časová synchronizace zařízení proti centrálnímu zdroji času na síti, 9. podpora autentizace vůči LDAP (Active Directory), 10. řízení uživatelského přístupu
P.31	Minimální požadovaná funkční specifikace fyzické sondy: 1. specializované dedikované zařízení (sonda) ve formě fyzického zařízení pro vytváření detailních statistik IP toků o dění na síti směrované na monitorovací porty sondy. 2. stejné požadavky jako u sondy pro virtualizační platformu (předcházející požadavek) 3. sonda s 1 monitorovacím portem 1GbE
P.32	Minimální požadovaná funkční specifikace kolektoru síťového provozu:

#	Požadavek
	Specializované zařízení (kolektor) určené pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat. 1. Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. 2. Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení. 3. Rack mount zařízení, snadná instalace do stávající síťové infrastruktury. 4. Datové úložiště minimálně o velikosti 1TB, použití RAID5. 5. Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. 6. Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. 7. Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. 8. Podpora autentizace vůči LDAP (Active Directory). 9. Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. 10. Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2, IPFIX položek proměnlivé délky. 11. Schopnost sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. 12. Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace, jako jsou název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu. 13. Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel). 14. Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem. 15. Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. 16. Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. 17. Časová synchronizace zařízení proti centrálnímu zdroji času na síti. 18. Možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232). 19. Podpora autentizace vůči LDAP (Active Directory). 20. Řízení uživatelského přístupu.
P.33	Minimální požadovaná funkční specifikace automatického vyhodnocování IP toků: 1. Rozšiřující systém na kolektor pro automatické vyhodnocování IP toků provádějící automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém založen na pokročilých metodách tzv. behaviorální analýzy, které umožňují odhalovat hrozby a incidenty, které překonaly zabezpečení na

#	Požadavek
	perimetru nebo bezpečnostní ochranu koncových stanic, a pro které dosud není dostupná signatura. 2. Výkon zpracování min. 1000 toků/s. 3. Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. 4. Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. 5. Systém podporuje persistenci doménových jmen, tedy uložení doménového jména původce události v okamžiku zaznamenání výskytu této události. 6. Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. 7. Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. 8. Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. 9. Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. 10. Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. 11. Detekované události je možné automaticky agregovat tak, aby související události byly prezentovány v rámci pojmenované hrozby (např. infikované zařízení v síti, chybně nakonfigurované zařízení, používání nevhodných aplikací nebo služeb apod.). 12. Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. 13. Veškerá funkcionalita detekce anomálií je založena na vyhodnocování flow dat bez nutnosti paketové analýzy, např. nasazení speciálních senzorů výrobce, systém nevyžaduje viditelnost na úrovni zrcadlení provozu. 14. Součástí události je identifikace uživatele získaná z externího zdroje uživatelské identit v okamžiku detekce události, tato informace je perzistentní.
P.34	Instalace a konfigurace dodávaných komponent a celkového řešení.
P.35	Záruka 5 let, režim 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně aktualizace SW.

Tabulka 7: Systémy pro sběr dat (logů) o síťovém provozu

4.4.5 Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

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

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

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

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

#	Požadavek
	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.41	Záruka 5 let, 5x8, garantovaná doba opravy do následujícího pracovního dne na místě včetně update SW a všech modulů.
P.42	Součástí dodávky musí být instalace a konfigurace řešení, včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou.
P.43	Je požadováno za 1 měsíc a za 3 měsíce vyhodnocení provozu a doladění korelačních pravidel na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.44	Implementace notifikací s využitím jak stávajících notifikačních nástrojů ZZS, tak s využitím pokročilého notifikačního nástroje, který je součástí dodávky tohoto projektu (viz. kap. 4.4.7). Notifikace budou prováděny následujícími nástroji: 1. Email 2. SMS 3. Hlasová zpráva (text-to-Speech) 4. Push aplikace na mobilní zařízení 5. Využití záložního svolávacího systému (jiná ZZS) *Pro notifikaci emailem bude využíván protokol SMTP.*
P.45	Pro analytickou práci s logy aplikací, bezpečnostních a síťových systémů využívaných v rámci ZZS nebo dodávaných v rámci dodávky je požadována dodávka nástroje pro logování z IT infrastruktury: 1. Aktivní prvky (sítě) 2. Informační systémy – IS ZOS/ZZOS a systém elektronické pošty 3. Databáze (ORACLE, MS SQL) 4. Operační systémy (MS Windows, Linux) – servery, pracoviště ZOS/ZZOS V případě, že se bude jednat o jeden nástroj zajišťující všechny uvedené služby, musí nástroj umožnit samostatný přístup k různým službám pro různé osoby na základě oprávnění

#	Požadavek
	definovaného správcem a možnost instalace na oddělený samostatný server (log server v kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW).
P.46	Dodávka a implementace nástroje na logování z IT infrastruktury, IS ZOS a elektronické pošty, tzn. aktivní prvky, aplikace, operační systémy apod. ve kterém bude možnost plošně prohledávat sesbíraná data a mít k dispozici statistiku a analytické funkce – přičemž zdrojem dat může být stávající syslog systém ZZOS a bude rozšířen o následující funkce: 1. Schopnosti provádět korelace přes více datových zdrojů a hledání specifických vzorů 2. Dlouhodobé retence dat (minimálně 3 měsíce, optimálně 6 měsíců) 3. Předpokládaný objem logovaných dat do 2 GB za den, licence s podporou na nebo licence opravňující produkt využívat po dobu min. 5 let a min. v uvedeném objemu za den. 4. Jeden společný datový sklad pro všechna indexovaná data – jeden dotaz nebo report může zahrnout všechna indexovaná data 5. Není třeba vytvářet datové schéma nebo připravit vyhledávací dotazy ještě před indexováním 6. Možnost využití nestrukturovaných souborů a datového skladu bez pevného schématu (bez relační databáze s pevným schématem) 7. Schopnost indexovat a připravit pro vyhledávání všechna originální data bez jakékoliv modifikace (bez normalizace/redukce dat) 8. Automatická komprese indexovaných dat pro redukci nároků na úložný prostor 9. Flexibilní nastavení uchování dat s možností odstupňování řízení toho, co se stane s postupně stárnoucími daty. Neaktuální data mohou být přesunuta na externí (levnější) datové úložiště k archivaci a (nebo) smazána. 10. Flexibilní kontrola přístupu na základě rolí pro řízení přístupu uživatelů a přístupů přes API. 11. Integrace autentizace a autorizace s Microsoft Active Directory, případně samostatný oddělený systém pro auditní účely (mimo stávající systém AD). 12. Generování hashe pro každou událost v době indexování tak aby umožnilo při vyhledávání zjistit, zda s daty nebylo manipulováno 13. Monitoring své vlastní konfigurace a využití s cílem udržet si kompletní, digitálně podepsané auditní záznamy o tom, kdo přistupuje k systému, jaké dotazy spouští, na jaké reporty se dívá, jaké konfigurační změny provádí a další. 14. Řešení by mělo umožnit snadné vytváření široké palety vizualizací (nejen pevně dané, předpřipravené reporty) 15. Dostupné vizualizace by měly zahrnovat: čárový graf, časový graf, plošný graf, sloupcový graf vertikální, sloupcový graf horizontální, jediná hodnota s trendem (růst, pokles), koláčový graf, bodový graf, bublinový graf, ciferníkový (budíkový) ukazatel, graf typu teploměr (zobrazení hodnoty ve vztahu k rozsahu), geolokační mapa, graf zobrazující rozložení hodnot v geografických regionech, kruhový graf, výplňový graf, tabulky (vč. doplňkových funkcí jako jsou automatické sumy, procentuálních vyjádření, číslování řádků, atd.)

#	Požadavek
P.47	Implementace nástroje na logování bude obsahovat nejenom zprovoznění a základní nastavení systému ale vytvoření i reportů a dashboardů (náhledů) na jednotlivé komponenty IT infrastruktury a IS ZOS. Minimálně následující náhledy: 1. Aktivní prvky (LAN/WAN/FW) – přihlášení, změny konfigurací, chyby atd. 2. FW/VPN – přístupy (oprávněné a neoprávněné) včetně geolokace (zobrazení na mapě a v tabulce) 3. Operační systémy a databáze IS ZOS – přihlášení, chyby atd. 4. Emailová komunikace – přístupy (oprávněné a neoprávněné) včetně geolokace, chyby systému atd.
P.48	Je požadována realizace jednotného bezpečnostního portálu pro správce a management ZZS, který bude zahrnovat dodané technologie v rámci projektu. Minimální požadavky na přehledový bezpečnostní portál: 1. Webové rozhraní 2. Autentizace/autorizace uživatelů proti Microsoft Active Directory 3. Zobrazení posledních incidentů na základě analýzy bezpečnostních logů 4. Zobrazení VPN připojení (úspěšné i neúspěšné) 5. Zobrazení přihlášení do aplikací IS ZOS (úspěšné i neúspěšné) 6. Zobrazení přehledu emailové komunikace ZZS (chyby, vytížení apod.) 7. Možnost dalšího rozvoje dle požadavků ZZS – otevřený systém
P.49	Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí bude provozován na infrastruktuře (HW a systémový SW) požadovaný a dodávaný dle kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW..

Tabulka 8: Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí

4.4.6 Analytické nástroje pro ZOS ZZS PAK

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

#	Požadavek
P.50	V rámci stávajícího analytického systému ORACLE BI (produkt SOS-BI), požadujeme rozšířit datovou základnu o import a normalizaci dat bezpečnostních logů z aplikací IS ZOS. Vytvoření vzorových analýz nad bezpečnostními daty z hlediska pokusu o zneužití přístupu k jednotlivým aplikacím a modulům IS ZOS. Uživatelé tohoto analytického nástroje pak budou schopni vytvářet vlastní analýzy nad bezpečnostními záznamy aplikací IS ZOS a budou tak schopni definovat požadavky na konfiguraci aktivních incidentů v rámci systému analýzy bezpečnostních logů. Systém analýzy bezpečnostních logů bude moci být aktualizován na základě konkrétních požadavků správců systému IS OŘ zjištěných v analytickém nástroji pro ZOS.
P.51	Je vyžadováno stanovení základní kategorie možných bezpečnostních incidentů a tomu bude přizpůsobena struktura uložení dat bezpečnostních logů v databázi datového skladu tak, aby byla

#	Požadavek
	optimální pro dané analýzy. Uživatel tak bude mít k dispozici snadno použitelné údaje v datových kostkách (oblasti dat).
P.52	Je požadováno, aby data bezpečnostních logů byla navázána na stávající datové objekty, jako jsou události (hlášení) a pacienti. Tím musí být umožněno v analýzách vyhledávat anomální chování i na základě příslušnosti dat, ke kterým byl v aplikacích a modulech IS ZOS zachycen přístup. Například aktivní událost, výjezd a ošetření pacienta řeší určitý okruh zaměstnanců, kteří jsou v události, výjezdu a v kartě pacienta zaznamenaní (dispečer, posádka, doktor). Přístup k datům od uživatele mimo okruh těchto zaměstnanců může naznačovat bezpečnostní incident, který by, obzvlášť při četnějším výskytu u daného uživatele, měl být sledován a řešen.
P.53	Požadované řešení má umožnit analýzy bezpečnostních logů i na základě anomálií v časovém sledu. Například zaměstnancovo (uživatelovo) nezvyklé navýšení počtu prohlížených a/nebo modifikovaných záznamů v určitém měsíci / týdnu / dni oproti ostatním měsícům / týdnům / dnům může naznačovat bezpečnostní incident.
P.54	Musí být možné analýzy na základě objemu dat, ke kterým uživatel modulu IS ZOS přistupoval oproti ostatním jeho kolegům ve stejné funkci (porovnání vůči standardnímu chování)
P.55	Možnost dohledání detailů všech přístupů k datům na základě znalosti konkrétní události, resp. existujícího bezpečnostního incidentu / nahlášeného úniku dat.
P.56	Analytické nástroje pro ZOS ZZS PAK budou provozovány nově dodávané infrastruktuře (HW a systémový SW) v kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW). Dodavatel musí provozní požadavky dodávané technologie zohlednit v rámci navrhovaného HW a SW.
P.57	Není požadováno navýšení ani změna stávajících licencí. Součástí dodávky je systémová podpora na 5 let.

Tabulka 9: Analytické nástroje pro ZOS ZZS PAK

4.4.7 Pokročilé notifikační nástroje

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

#	Požadavek
P.58	Je požadována dodávka a realizace pokročilého notifikačního nástroje vč. instalace a propojení se systémem operačního řízení (IS OŘ), propojený se stávajícím svolávacím systémem implementovaným v rámci ZZOS ZZS PaK, napojení na stávající telefonní systém, s následujícími požadovanými funkcemi: 1. Aplikační rozhraní pro uvedené funkce pro systém operačního řízení (IS OŘ), a pro monitorovací systém. 2. Instalace ve virtualizovaném prostředí VMWare s možností migrace v rámci virtualizované platformy (nezávislost na HW). 3. U všech hlasových úloh možnost programově nastavit číslo volajícího v rámci aplikačního rozhraní (v součinnosti s konfigurací stávající telefonní ústředny).

#	Požadavek
	4. Hlasové úlohy: a. Prozvánění k výjezdu. b. Přehrání hlasové zprávy pomocí převodu textu na hlasovou zprávu (text-to-speach) s podporou češtiny. c. Přehrání zprávy s očekávanou návratovou hodnotou (v podobě tónové volby) – například Ano/Ne, přičemž dotaz a způsob odpovědí je zadáván konfiguračně v rámci systému operačního řízení (IS OŘ) a předáván aplikačním rozhraním. d. Kapacita hlasového svolávání až 30 hlasových spojení v jednom okamžiku. e. Úprava systému operačního řízení pro napojení na notifikační nástroj (detailní požadavky jsou uvedeny v kap. 4.4.8). Pokročilý notifikační nástroj musí umožnit všechny scénáře uvedené v kap. 4.4.8. 5. SMS úlohy a. Odesílání SMS, a to prostřednictvím internet připojení – stávající „O2 Connector“ (zajistí Zadavatel) a pomocí GSM brány pro 4 SIM. Primárně přes „O2 Connector“, záložní způsob přes GSM bránu. b. Dodávka GSM brány pro 4 SIM integrované s nabízeným svolávacím systémem. GSM brána připojena k infrastruktuře pomocí IP protokolu (ethernet port). Vlastní SIM karty zajistí Zadavatel. c. Licence notifikačního nástroje pro využití min. 1x SMS connector a 4x SIM. d. Odesílání definovaných, případně uživatelsky modifikovaných zpráv. e. Odesílání zpráv s dotazem na uživatele a přijetím a předáním jeho odpovědi dále do operačního řízení. 6. Mobilní aplikace a. Odeslání zpráv na mobilní zařízení b. Odesílání zpráv s dotazem na uživatele a přijetím a předáním jeho odpovědi dále do operačního řízení. c. Podpora mobilních platforem min. iOS a Android 7. Integrační úlohy a. Vyhodnocení odpovědí svolávaných skupin uživatelů a jejich přehledné zobrazení. b. Plná aplikační integrace s IS OŘ (viz kap. 4.4.8).
P.59	Integrace notifikačního nástroje musí umožnit využití všech technologií nástroje pro doručení požadované zprávy. Pokročilý notifikační nástroj musí být schopen při výpadku jakékoliv technologie (Internet, telefonie, GSM SMS) doručit požadovanou zprávu ke koncovému uživateli jinou dostupnou technologií.
P.60	Vlastní inicializaci notifikace bude možné provádět jak z IS OŘ, tak z monitorovacích systémů (jako upozornění na aktuální problém).
P.61	Zadavatel zajistí SIM karty a konektor k mobilnímu operátorovi pro odesílání SMS a SIP trunk pro hlasové služby. Pro odesílání zpráv do mobilní aplikace bude využito stávajícího internet připojení.

#	Požadavek
P.62	Notifikační nástroj pro ZOS ZZS PAK bude provozován na infrastruktuře (HW a systémový SW) požadovaný a dodávaný dle kap. 4.4.15 – Infrastruktura (HW) a systémový SW pro běh dodávaného SW.

Tabulka 10: Pokročilé notifikační nástroje

4.4.8 Úpravy IS ZOS

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

#	Požadavek
Napojení na Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5)	
P.63	Je požadována úprava systémů IS ZOS pro zaznamenávání činností v rámci operací těchto systémů do externích systémů pro následné zpracování a analýzy – Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (viz kap. 4.4.5).
P.64	**IS OŘ:** Předávání logů z IS OŘ do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.65	**IS OŘ:** Napojení na pokročilé notifikační nástroje (viz kap. 4.4.7) – je požadována úprava IS OŘ tak aby, byl schopen využívat jak pokročilý notifikační nástroj (viz kap. 4.4.7) implementovaný v ZOS, tak stávající svolávací systém provozovaný v rámci ZZOS, dle dostupnosti požadovaných technologií a to minimálně s následujícími požadavky: 1. Možnost zadávat text zprávy pro notifikace a to jak technologií hlasového svolávání (text-to-speach), tak pro SMS a datový kanál (mobilní aplikace). 2. Možnost definování textu otázky a odpovědí pro úlohy svolávání vyžadující odpověď koncového uživatele. Integrace s vyhodnocením odpovědí koncových uživatelů v závislosti na typu svolávání. 3. Předávání zprávy k odeslání notifikačním nástrojům přes integrační rozhraní 4. a rozšíření o volitelné texty a využití funkce text-to-speach v rámci systému operačního řízení (IS OŘ) a to jak běžných informací, tak i modulu hromadného neštěstí. 5. Jednoduchý proces přepínání využívaného rozhraní mezi pokročilým notifikačním nástrojem v ZOS a svolávacím systémem ZZOS.
P.66	**GIS:** Předávání logů z GIS do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systému 2. Chybná přihlášení do systému Logy jsou ukládány na diskové úložiště, odkud mohou být automatizovaně zpracovávány Systémem analýzy bezpečnostních logů. V případě využití této možnosti je součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.

#	Požadavek
P.67	**EKP/MZD:** Předávání logů z EKP/MZD do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.68	**IS Pojišťovna:** Předávání logů z IS Pojišťovna do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systémů a modulů 2. Chybná přihlášení do systému a modulů 3. Operace s daty (pořízení, modifikace a zobrazení) 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS
P.69	**Systém sledování vozidel (AVL):** Předávání logů z AVL do systému analýzy bezpečnostních logů v následujícím rozsahu: 1. Přihlášení a odhlášení do systému 2. Chybná přihlášení do systému 3. Informace odeslání informací k dané události do technologie AVL ve voze 4. Možnost předávání logů s anonymizovanými položkami – dle druhu informace a účelu jejího pořízení – na základě konzultace a požadavků ZZS Logy jsou ukládány na diskové úložiště, odkud mohou být automatizovaně zpracovávány Systémem analýzy bezpečnostních logů. V případě využití této možnosti je součástí dodávky parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.70	**Svolávací systém** využívá data IS OŘ a jeho volání je realizován z IS OŘ, tj. data budou sbírána cestou IS OŘ.
P.71	**Telefonní ústředna** je integrována s IS ZOS prostřednictvím JTAPI a CTI rozhraní stávající telefonní ústředny. Vlastní přístup na server stávající telefonní ústředny je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky je parsování logů, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.72	**Záznamový systém (REDAT)** je uzavřené řešení pro nahrávání hovorů. Dispečeři ZOS mají přístup k nahrávkám prostřednictvím systému IS OŘ, který loguje přístupy k aplikačnímu serveru systému REDAT v rámci IS OŘ. Tyto informace jsou tak předávány v rámci přeposílání logů IS OŘ. Součástí dodávky je parsování logů záznamového systému přes IS OŘ, jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.73	**Integrace telefonie a radiofonie** je vázaná na dané dispečerské pracoviště a informace o přihlášení a přístupu uživatele budou brány z IS OŘ dle toho, který dispečer na daném pracovišti pracoval (vlastní integrace nevyužívá speciální přístupy a ovládá komunikační prostředky na

#	Požadavek
	daném pracovišti). Vlastní přístup na server určený pro integraci je logován v rámci systémových prostředků OS. Data jsou tedy sbírána na systémové úrovni. Součástí dodávky parsování logů z IS OŘ je jejich analýza a ukládání do Systému analýzy bezpečnostních logů.
P.74	**Záložní IS ZOS (ZZOS):** ZZOS využívá v současné době repliku některých systémů IS ZOS (IS OŘ, AVL/GIS, MZD/EKP). Je požadováno, aby pro tyto systémy byla sbíraná data stejná v primární i záložní lokalitě.
P.75	Aplikační SW na pracovištích ZOS/ZZOS: Vlastní přístup do OS na pracovištích ZOS a ZZOS bude logován v rámci systémových prostředků operačního systému. *Sbíraná data z operačních systémů a dalších technologie na pracovištích ZOS/ZZOS budou sbírána na systémové úrovni.*
Napojení IS OŘ na FireWall(y) s IPS pro ZOS (viz kap. 4.4.2)	
P.76	V rámci IS OŘ bude možné přijímat i alerty upozorňující na bezpečnostní události, a to nejenom z uvedených bezpečnostních prvků ale všech komponent zabezpečení. Bude se jednat o alerty bezpečnostních událostí relevantních k provozu centrálního dispečinku a celého IS ZOS s kritickou důležitostí. Bezpečnostní alerty v rámci IS ZOS budou definovány a konfigurovány na základě požadavků ZZS v systémech analýzy a sběru bezpečnostních logů, který tyto alerty bude předávat do IS OŘ – dispečerského pracoviště. Tak bude aktivně informován provoz centrálního dispečinku ZOS o vážných bezpečnostních událostech.
P.77	Oprávněné osoby centrálního dispečinku budou mít možnost pomocí rozhraní v IS ZOS (IS OŘ) na základě vzniklých bezpečnostních událostí a jejich průběhu rozhodnout o možnosti aktivace (a následné deaktivace) izolace systému IS ZOS od externích sítí nebo i od interních LAN/WAN segmentů. Vlastní izolace bude realizována na uvedených bezpečnostních prvcích (ZOS/ZZOS). Oprávněný uživatel bude před vlastní aktivací daného typu izolace informován o rozsahu izolace a z toho plynoucích omezení centrálního dispečinku a IS ZOS. O těchto událostech bude proveden detailní záznam událostí včetně jejich časové souslednosti a uživatelích, kteří taková opatření realizovali a neprodleně automaticky informováni definovaní pracovníci ZZS v rámci stávajícího svolávacího systému ZZS.
Autentizace uživatelů operačního řízení prostřednictvím AD	
P.78	V rámci sjednocení ověřování identity uživatelů v rámci IT a operačního řízení je požadováno využití stávající domény v rámci Microsoft Active Directory. Pro tyto účely požadováno rozšíření stávajícího IS ZOS o možnost autentizace a autorizace v rámci struktury MS Active Directory.
P.79	**IS OŘ:** Správce IS OŘ bude pak schopen zvolit způsob autentizace jednotlivých uživatelů dle potřeb ZZS a typu modulů/subsystémů. Je požadováno, aby bylo možné plně využít pro autentizaci a autorizaci uživatelů IS OŘ jednotných účtů v rámci MS Active Directory. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.

#	Požadavek
P.80	**EKP/MZD:** EKP/MZD musí umožňovat autentizaci a autorizaci uživatelů jak interní (stávající stav) nebo v rámci MS Active Directory. Správce IS v návaznosti na okolní systémy bude schopen zvolit způsob autentizace EKP/MZD dle požadavku ZZS. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů.
Integrace s personálním systémem	
P.81	Je požadováno rozšíření stávajícího personálního systému o integraci s centrálním Active Directory ZZS s četností aktualizace dat minimálně 1x za den.
P.82	IS OŘ a EKP/MZD pak musí umožnit využití integrace s personálním systémem, a to jak při zakládaní uživatele a případně jejich základní role v rámci personálního systému (která se promítne do AD) využití zneplatnění účtů uživatelů, u kterých bude ukončen pracovní poměr (zneplatnění/vymazání účtu v AD). Tím bude zajištěna maximální aktuálnost uživatelských účtů zaměstnanců ZZS.
Monitoring a reporting a přístupů	
P.83	Pro správu a reporting oprávnění bude dodán i samostatný portál pro správu uživatelů IS OŘ a přiřazování jejich rolí. Tento portál bude sloužit pro vedoucí pracovníky OŘ, kteří budou tato oprávnění spravovat a kontrolovat a monitorovat.
P.84	Součástí dodávky bude nástroj pro reportingu všech změn provedených jednotlivými uživateli/administrátory v rámci Microsoft Active directory (AD) ZZS (počet zaměstnanců – potenciálních uživatelů 600), tak aby bylo možné kontrolovat změny oprávnění, které byly v rámci AD provedeny. Je požadováno reportovat minimálně: 1. Vytvoření nového uživatele nebo skupiny 2. Vymazání uživatele nebo skupiny 3. Zneplatnění (disable) uživatele 4. Přidání člena skupiny 5. Vymazání člena skupiny
Infrastruktura (HW) a systémový SW pro úpravy IS ZOS	
P.85	Stávající infrastruktura (HW) a systémový SW pro běh IS ZOS po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh IS ZOS.

Tabulka 11: Úpravy IS ZOS

4.4.9 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.86	Napojení na Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a předávání následujících dat ze systému elektronické pošty: 1. Úspěšná a neúspěšná připojení k systému dostupnými protokoly 2. Využívání systému elektronické pošty jednotlivými uživateli 3. Dostupné bezpečnostní logy používaného systému 4. Dostupné chybové a provozní logy používaného systému Předávání veškerých logů systému do nástroje/rozhraní pro logování.
P.87	Toto nastavení realizovat pro všechny komponenty systému elektronické pošty.
P.88	Předávání logů systému online prostřednictvím syslog služby.
P.89	Součinnost při konfiguraci FireWallu ZOS a konfigurace FireWallu ZZOS pro získávání informací o bezpečnostních událostech na prvcích FireWall, týkajících se systému elektronické pošty. Minimálně: 1. Odepření přístupu z dané IP adresy na systém (reputace dynamický ACL apod.) 2. IPS a AntiMalware události 3. Identifikace chyb v protokolu
P.90	Systém dynamických ACL na základě parametrického vyhodnocení bezpečnostních logů systému. Dynamický ACL bude vytvářen prostřednictví analýzy logů na základě neoprávněného přístupu k systému. Pro vytváření dynamických ACL bude možné systémově nastavovat následující parametry: 1. Počet špatných přihlášení k danému protokolu 2. Minimální čas od posledního výskytu špatného přihlášení Publikace dynamického ACL pro systém elektronické pošty bude pro účely aktualizace pravidel FireWallu realizována web serverem jako standardní textový soubor s výčtem (list) IP adres (jedna IP na jednom řádku).
P.91	Nástroj/rozhraní pro logování bude zpracovávat i uvedený dynamický ACL pro systém elektronické pošty a zobrazovat časový průběh počtu IP adres obsažených v listu a upozorňovat na enormní nárůst.
P.92	Provedení konfigurace FireWallu ZOS (kap. 4.4.2) a součinnost pro konfiguraci FireWallu ZZOS pro implementaci dynamického ACL – aktualizace listu IP adres
P.93	Stávající infrastruktura (HW) a systémový SW pro běh elektronické pošty po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh elektronické pošty.

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

4.4.10 Dvoufaktorová autentizace administrátorských VPN přístupů

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

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

Tabulka 13: Dvoufaktorová autentizace administrátorských VPN přístupů

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

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

#	Požadavek
P.97	Pro zabezpečení přístupu do LAN/WAN sítě ZZS požadujeme implementaci technologie 802.1x na přístupových switchích centrální lokality a výjezdových stanovišť. Vlastní implementace bude využívat pro ověření zařízení a uživatelů autentizaci v rámci RADIUS serverů Microsoft NPS s integrací do jednotného Active Directory. Pro neautorizované zařízení a uživatele bude vytvořena v rámci jednotlivých lokalit i GUEST VLAN s definovaně omezeným přístupem do sítě. Minimální požadavky: 1. Integrace s RADIUS servery Microsoft NPS v rámci AD ZZS 2. Konfigurace všech stávajících LAN prvků umožňujících konfiguraci 802.1x v rámci WAN sítě ZZS 3. Vytvoření GUEST VLAN ve všech lokalitách WAN ZZS a její zabezpečení v rámci dostupných technologií v dané lokalitě 4. Vzorová konfigurace PC a NB pro 802.1x 5. Konfigurace speciálních zařízení (Tiskárny apod.) bez podpory 802.1x 6. Testovací provoz implementace bez reálného odepření přístupu včetně vyhodnocení provozu

#	Požadavek
	7. Přechod do provozního režimu včetně odepření přístupu neautorizovaným zařízením
P.98	Správce infrastruktury musí být informován o všech neoprávněných pokusech s maximálním rozsahem informací o takovém pokusu (Datum a čas, MAC adresa, prvek, port apod.). Informace musí být možné získávat online při výskytu nebo reportem za dané časové období.
P.99	Součástí implementace bude i systém logování výskytu jednotlivých zařízení (MAC adres) v rámci WAN ZZS. Systém bude umožňovat reporting nejenom MAC adres, ve kterých lokalitách, prvcích a portech se daná MAC adresa vyskytovala, ale též od kdy do kdy byla připojena a jakou IP adresu v rámci WAN ZZS obdržela. Reportovací systém bude udržovat databázi výskytu MAC adres a přidělených IP adres jednotlivým MAC adresám s časovou závislostí. Musí být tedy realizována integrace s používanými DHCP servery Microsoft. Reportovací sytém musí umožňovat získávat přehled i o připojených zařízeních do aktivních prvků, které nebudou podléhat autentizaci prostřednictvím 802.1x.
P.100	Pro některé lokality bude třeba realizovat i dodávku aktivních prvků typu přepínač s podporou 802.1x jedná se celkem o 2 ks přepínačů (switchů) které musí plnit následující min. parametry (každý jeden switch): 1. provedení rack mount 2. ethernetový spravovatelný přepínač vrstvy 2 3. min. 24x 10/100/1000Mbs PoE+ TP portů a 4 x 1Gportů SFP 4. minimální propustnost přepínacího subsystému min. 56Gbps 5. možnost zapojení více switchů do jednoho stacku (přepínače se chovají jako jeden z pohledu managementu i připojených zařízení – včetně automatického load balancingu), kapacita propojení 80Gbps – součástí dodávky nejsou požadovány technické prostředky (porty/modul) pro realizaci vlastního stacku, 6. podpora VLAN (min. 1000), 7. software podporující CLI (Telnet/SSH), SNMP management, včetně omezení přístupu na management z definovaných adres a subnetů, 8. bezpečnost – port security a implementace 802.1X, automatické zařazování do VLAN 802.1x – RADIUS server Windows AD, 9. podpora „jumbo“ rámců, 10. detekce protilehlého zařízení (např. CDP nebo LLDP), 11. podpora IPv4 a IPv6, 12. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 13. veškerý potřebný drobný materiál (kabely apod.) 14. Záruka min. na 5 let.

Tabulka 14: Dodávka a implementace technologií 802.1x pro zabezpečení přístupů do LAN sítě

4.4.12 Zabezpečení systému elektronické pošty před škodlivým kódem

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

#	Požadavek
P.101	Je požadováno plně redundantní řešení pro kontrolu poštovního provozu (EmailSecurity) s veřejnou sítí Internet, včetně antispamové a antivirové ochrany. Řešení může být formou virtuálního appliance do Vmware – rozšíření počtu virtuálních strojů musí být bezplatné (neomezený počet virtuálních strojů v rámci jedné sítě), případně dedikovaným HW (primární a sekundární) nebo kombinací těchto variant. Požaduje se dodávka licencí i pro testovací prostředí na samostatné virtuální appliance. Dodané licence musí umožnit převedení licencí mezi uvedenými variantami (HW/virtual). Licence musí umožnit instalaci další virtuální appliance i v záložní lokalitě. V nabídce bude uveden způsob řešení a způsob redundance.
P.102	Minimální požadavky na EmailSecurity řešení: 1. Řešení musí být výkonově dimenzováno minimálně na 1000 uživatelů a licencováno na 1500 chráněných stanic (využíváno celkem 600 uživateli) 2. nabízené zařízení je možné provozovat v clusteru v režimu loadbalancing, 3. Reputační filtrování na základě zdrojových IP adres odesílatele a reputační způsob blokování spamu na úrovni TCP spojení 4. Možnost nastavení anti-spam akce pro pozitivní nebo podezřelý spam: Doručit, zahodit, karanténa, doručit jako přílohu, přesměrovat 5. Per-user anti-spam karanténa s ověřováním pomocí LDAP 6. Definice whitelist a blacklist pro každého uživatele v karanténě 7. Periodické zasílání notifikací o novém spamu v karanténě pro každého uživatele 8. Možnosti uživatele pro práci se spamem v karanténě: Smazat, doručit, přidat do whitelistu 9. Možnost označit/klasifikovat email jako spam přímo z emailového klienta 10. Detekce a klasifikace marketingových emailů, které nejsou spam 11. Podpora pro současné kontroly více antivirovými engines přímo na zařízení včetně detekce viru uvnitř víceúrovňového archivu 12. Možnost opravy zavirovaných příloh nebo jejich zahození 13. Automatická aktualizace všech antimalware signatur v intervalu 5 minut či méně 14. Per-user nebo per-group nastavení pro Anti-spam a Anti-virus akce pro příjemce či odesílatele 15. Možnost vytváření sofistikovaných filtrů na emailovou komunikaci s možností filtrace na obsah hlaviček, těla i příloh emailu 16. kontrola příchozí i odchozí poštovní komunikace na jednom zařízení zároveň, 17. Filtrování obsahu a ochrana proti úniku dat a. Podpora váhových slovníků b. Podpora pro mezinárodní a multibyte umístění (nejlépe podpora UTF8) c. "Pattern matching" uvnitř vícevrstvých archivů d. Plná podpora regulárních výrazů pro "pattern matching" e. Plnohodnotný a pravdivý filetype matching (ne na základě MIME type / filename)

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

Tabulka 15: Zabezpečení systému elektronické pošty před škodlivým kódem

4.4.13 Kontrola přístupu do sítě Internet – webSecurity

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

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

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

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

Tabulka 16: Kontrola přístupu do sítě Internet – webSecurity

4.4.14 Nástroje pro zajištění šifrování dat na PC/NB

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

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

Tabulka 17: Nástroje pro zajištění šifrování dat na PC/NB

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

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

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

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat (min. 5 let a min. v rozsahu stávajícího IS ZOS) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.118	Dodávka infrastruktury a běhového prostředí pro následující části dodávky: 1. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (kap. 4.4.5) 2. Pokročilé notifikační nástroje (kap. 4.4.7) 3. Zabezpečení systému elektronické pošty před škodlivým kódem (kap. 4.4.12) 4. Kontrola přístupu do sítě Internet – webSecurity (kap. 4.4.13) Následující požadavky na infrastrukturu (HW) a systémový SW pro běh dodávaného SW jsou minimální, tj. pokud mají dodávky dodavatele nároky vyšší, navrhne dodavatel odpovídající řešení a v nabídce jej popíše.
P.119	Dodávka min. 3 ks virtualizačního serveru s min. konfigurací: 1. provedení rack mount pro až 8 2,5“ pozic, maximální velikost 1U, pro přístup ke všem komponentám serveru bez použití nářadí 2. interaktivní LCD display či obdobný systém indikující základní informace o systému (min. IP adresa, stav serveru a výpis chybových stavů), možnost nastavení IP konfigurace OOB managementu na čelním panelu 3. minimálně jeden šestnáctijádrový procesor s hodnotou dle SPECint_rate2006 base min. 1700 bodů a dle SPECfp_rate2006 base min. 1300 pro 2 CPU konfiguraci (údaje musí být k dispozici na www.spec.org) 4. min. 192 GB RAM (min. 32GB moduly 2666MHz) s možností rozšíření na 24 DIMM pozic 5. min. 2x 32 GB (flash či netočící médium) v raid 1 pro hypervizor 6. min. 1x 400 GB SSD s minimální hodnotou denního přepisu 3 7. hw řadič s min. 2GB cache a podporou raid 0, 1, 5, 6 8. min. 2x 1Gbase-T ethernet síťové porty typu LOM s podporou IPv4, IPv6 9. min. 4x 10GbE SFP+ porty 10. 2 redundantní síťové napájecí zdroje min. 750 W 11. rackové lyžiny a rameno na kabeláž na zadní straně serveru 12. management serveru nezávislý na operačním systému s dedikovaným USB či SD úložištěm dostupným i v případě výpadku interních disků, poskytující management funkce a vlastnosti: webové rozhraní a dedikovaná IP adresa, sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory); podpora virtuální mechaniky

#	Požadavek
	13. vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému 14. management musí podporovat dvoufaktorovou autentikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP 15. požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH 16. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server 2016, Red Hat Enterprise Linux a SUSE 17. licence Microsoft Windows Server 2016 Datacenter pro požadovaný případně dodaný počet jader (vyšší hodnota) pro provoz jak nových, tak stávajících Windows Serverů na dodávaném HW. 18. podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení 19. je vyžadována kompatibilita se stávajícím prostředím – server bude zařazen do stávající infrastruktury a virtualizačního prostředí
P.120	Dodávka min. 1 ks samostatného log serveru s min. konfigurací: 1. provedení Rack mount (včetně potřebných montážních komponent a ramene pro kabeláž) 2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty 2. minimálně jeden šestnáctijádrový procesor s hodnotou dle SPECint_rate2006 base min. 1700 bodů a dle SPECfp_rate2006 base min. 1300 pro 2 CPU konfiguraci (údaje musí být k dispozici na www.spec.org) 3. min. 32 GB RAM (min. 8 GB moduly 2666MHz typu DDR4) 4. min. 5x 4 TB disk min 7200 otáček a min 3x 1,92 TB SSD s min DPWD 3 5. min. 4x 1Gbase-T ethernet síťové porty s podporou IPv4, IPv6 6. 2 redundantní síťové napájecí zdroje min. 750W 7. Interface: 4 x USB (1 vpředu, 2 vzadu, jeden uvnitř) a sériový port 8. hw řadič s min. 2GB cache a podporou raid 0, 1, 5, 6, 50, podpora SED disků a SSD disků, podpora globálního i dedikovaného hot-spare 9. certifikace pro aktuální verze VMware ESX, vSphere, Windows Server 2016, Red Hat Enterprise Linux a SUSE 10. management serveru nezávislý na operačním systému s dedikovaným USB či SD úložištěm (data na úložišti musí být dostupná i v případě výpadku interních disků a musí být možné ji rozdělit na několik nezávislých partition s možnosti volby boot sekvence) poskytující management funkce a vlastnosti: webové rozhraní a dedikovaná IP adresa, sledování hardwarových senzorů (teplota, napětí, stav, chybové senzory) 11. vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému 12. management musí podporovat dvou faktorovou autentifikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP 13. požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH

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

#	Požadavek
	23. podpora na 5 let typu 24x7x365 s reakční dobou 4 hodiny, oprava v místě instalace zařízení, servis je poskytován výrobcem zařízení 24. je vyžadována kompatibilita se stávajícím prostředím – datové úložiště bude zařazeno do stávající infrastruktury (napojení na stávající 10g switche – ISCSI a připojení k virtualizačnímu prostředí) a.
P.122	Dodávka a instalace systémového SW – požadujeme dodávku systémového SW pro všechny nabízené systémy. Jedná se o minimálně následující systémový SW: 1. Operační systémy serverů, kde požadujeme dodávku všech licencí potřebných operačních systémů a mimo to požadujeme jako součást HW virtualizačního serveru (viz požadavek na dodávku jednoho virtualizačního serveru výše) licenci Windows Datacenter pro provoz jak nových, tak stávajících Windows Serverů na dodávaném HW. 2. Databáze pro dodávané systémy. 3. Pro virtualizaci dodávaných serverů požadujeme kompatibilní řešení se stávající virtualizací tak, aby bylo možné zařadit do jedné konfigurační konzole – minimálně licence virtualizačního SW pro dodávaný počet CPU kompatibilní se stávajícím virtualizačním SW (viz kap. 7.4), s podporou výrobce na 5 let. 4. Pro zařazení virtualizačních serverů do systému zálohování je požadována dodávka licence kompatibilního systému zálohování pro dodávané konfigurace virtualizačních serverů. ZZS poskytne součinnost při konfiguraci do stávajícího zálohovacího řešení. Stávající technologie, na které je odkazováno, jsou uvedeny v kap. 7.4 – Stav ostatních informačních a komunikačních technologií. V případě, že nabízené řešení vyžaduje další nespecifikovaný systémový SW tak musí být součástí nabídky.
P.123	Součástí dodávky je integrace dodávaných technologií do stávajícího monitorovacího nástroje (WhatsUp firmy Ipswitch), který není součástí dodávky tohoto projektu. Monitoring musí jednoznačně identifikovat chod jednotlivých komponent.
P.124	Součástí dodávky je zařazení dodávané infrastruktury do stávající infrastruktury (napojení na stávající 10g switche – ISCSI a připojení k virtualizačnímu prostředí) včetně dodávky potřebných kabelů. Návrh propojení do stávající infrastruktury bude součástí implementační analýzy a návrhu řešení a bude podléhat schválení zadavatelem.
P.125	Součástí dodávky není strukturovaná kabeláž.
P.126	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích.

Tabulka 18: Infrastruktura (HW) a systémový SW pro běh dodávaného SW

4.4.16 Nástroje pro bezpečnostní audit a penetrační testy

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

#	Požadavek
P.127	Je požadována dodávka nástroje/nástrojů pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů (nástroj/nástroje budou využity v rámci kap. 4.4.17 – Bezpečnostní audit a penetrační testy.
P.128	Minimální rozsah: externí testy, interní testy a testy zranitelností operačních systémů, databází a informačních systémů (aplikací). Jedná se minimálně o: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací;
P.129	Je požadováno, aby nástroj/nástroje umožňoval: 1. Vzdálené privilegované a neprivilegované skeny 2. Neomezené množství koncových IP adres 3. Pravidelné aktualizace signatur/detekčních metod (cca 1x týdně)
P.130	Předmětem dodávky není periodické provádění testů zranitelností (nad rámec testů v rámci vedlejších aktivit), ale zajištění nástrojů pro provádění a vyhodnocování uvedených testů.
P.131	S ohledem na vysokou citlivost zpracovávaných dat musí být dodaný nástroj možné kompletně instalovat na server/počítač umístěný v lokální síti, která je pod správou Zadavatele. Výstupy z testů/skenů musí být rovněž zpracovávány lokálně, bez zasílání do cloudu. Dodaný nástroj musí umožňovat ovládání s pomocí webového GUI.
P.132	Instalaci skeneru musí být možné realizovat na prvky s operačními systémy Microsoft Windows 7 a vyšší, Microsoft Windows Server 2008 a vyšší, macOS i Linux. Součástí dodávky nebude HW, OS ani další aplikační vybavení nutné pro provoz nástroje. Předpokládá se instalaci na prostředky Zadavatele (virtuální server nebo testovací PC/notebook).
P.133	Dodané řešení musí podporovat realizaci vzdálených bezagentských privilegovaných i neprivilegovaných skenů neomezeného počtu zařízení/IP adres a musí být schopné realizovat bezpečnostní skeny webových aplikací.
P.134	Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech.
P.135	Součástí dodávky bude licence relevantního nástroje s podporou a funkčností po dobu 5 let, instalace a aktivace jednoho skeneru v prostředí Zadavatele a úvodní zaškolení administrátorů a uživatelů.

Tabulka 19: Nástroje pro bezpečnostní audit a penetrační testy

4.4.17 Bezpečnostní audit a penetrační testy

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

#	Požadavek
P.136	Bezpečnostní analýza stávajícího prostředí z pohledu souladu se zákonem 181/2014 Sb., ve znění pozdější novelizace a s vyhláškou 82/2018 Sb.
P.137	Hodnocení stávajícího rozsahu řízení bezpečnosti informací: 1. Politiky 2. Metodiky a. Metodika identifikace a hodnocení aktiv b. Metodika analýzy rizik 3. Proces a výstupy hodnocení aktiv 4. Proces a výstupy hodnocení rizik 5. Revize primárních a podpůrných aktiv, jejich vzájemné vazby, určení jejich hodnoty a hodnocení jejich správy garanty 6. Plán zvládání rizik 7. Prohlášení o aplikovatelnosti bezpečnostních opatření 8. Zajištění zpětné vazby 9. Plán rozvoje bezpečnostního povědomí 10. Strategie řízení kontinuity 11. Pravidla řešení kybernetických bezpečnostních incidentů 12. Pravidla řízení provozu ICT 13. Hodnocení definice kontextu organizace, hodnocení jeho rozdělení na vnitřní a vnější kontext a hodnocení SLA mezi těmito 2 kontexty
P.138	Přezkoumání implementace technických opatření do praxe. Technické ověření souladu implementace primárních a podpůrných aktiv dle požadavků ZKB: 1. Aplikace 2. Operační systémy 3. Síťové prvky 4. Bezpečnostní prvky 5. Fyzická bezpečnost 6. Zálohování 7. Apod.
P.139	Výsledkem auditu bude: 1. Zpráva z přezkoumání stávajícího prostředí Zadavatele s následujícím obsahem: a. Pro každé opatření bude uveden popis aktuálního stavu b. Zhodnocení z pohledu požadavků prováděcí vyhlášky KB (ZKB) c. Případné zhodnocení z pohledu „best practice“, pokud bude takovéto doporučení žádoucí. d. Každé opatření bude popsáno minimálně v rozsahu ½ A4.

#	Požadavek
	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.140	Provedení penetračních testů a testů zranitelnosti: 1. Provedení penetračních testů a testů zranitelnosti pro IS ZOS, IS ZZOS a systému elektronické pošty (informační systémy a technologie jsou popsány v kap. 7.2 – Informační systémy k zabezpečení). 2. Pro systémy IS ZOS, IS ZZOS a Elektronickou poštu budou provedeny závěrečné testy zranitelnosti z externí sítě. V zájmu ověření korektního fungování webového aplikačního firewallu (WAF) a zajištění vysoké úrovně bezpečnosti provozovaných webových aplikací je požadováno provedení jednorázových penetračních testů.
P.141	Závěrečné testy zranitelnosti budou provedeny z externí sítě na IS ZOS, IS ZZOS a Elektronickou poštu. Jedná se tedy o testy zranitelnosti realizované přes bezpečnostní prvky – perimetry (FireWall) implementované v ZOS a ZZOS. Tyto testy musí obsahovat min.: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Brute Force – testování Brute Force Attack; 5. Web Applications – skenování webových aplikací; Účelem těchto testů je ověření konfigurace perimetrů a nalezení zranitelností publikovaných služeb/systémů.
P.142	Součástí bezpečnostního auditu budou i penetrační testy, které musí splňovat minimálně: 1. Penetrační testy se budou týkat uvedených aplikací provozovaných zadavatelem a jejich účelem bude identifikovat případné nedostatky v nastavení nasazeného WAF a odhalit případné zranitelnosti ve výše uvedených aplikacích, které jsou jím chráněny, a zajistit tak jejich bezpečnost v rámci plnění požadavků §25 vyhlášky 82/2018 Sb. v souladu s bezpečnostní strategií a dalšími dokumenty zadavatele.

#	Požadavek
	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.143	Výstupem testů zranitelnosti a penetračních testů musí být: 1. Závěrečná zpráva, která bude obsahovat soupis provedených testů a jejich výsledků, detailní popis odhalených zranitelností, ohodnocení jejich nebezpečnosti včetně konkrétního postupu umožňujícího jejich odstranění. 2. Doporučení řešení odhalených zranitelností – konkrétní postupy umožňující jejich odstranění u oblastí/technologií, které nejsou součástí dodávky. 3. Realizace opatření k odstranění odhalených zranitelností ve formě nastavení a implementace u oblastí, které jsou součástí dodávky.

Tabulka 20: Bezpečnostní audit a penetrační testy

4.4.18 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.144	Systém bude chránit osobní údaje pacientů a bude v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.145	Vybavení musí plnit podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
P.146	Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému. Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup.
P.147	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.148	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.149	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.150	Veškeré přístupy k datům a aktivita uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů.

#	Požadavek
P.151	Veškeré logy budou dostupné pro externí Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí.

Tabulka 21: Bezpečnostní požadavky

4.4.19 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.152	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.153	Počet uživatelů informačních systémů se nezmění.
P.154	Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování, bezplatné preventivní prohlídky v rámci poskytování servisních služeb. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce. Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.
P.155	Instalace do prostředí objednatele uvedeného v kap. 7.4 – Stav ostatních informačních a komunikačních technologií a kap. 7.2 – Informační systémy k zabezpečení.
P.156	V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.
P.157	Dodávka OS na servery, včetně instalace do prostředí objednatele, vč. potřebných licencí, pokud se jedná o licencovaný OS.
P.158	Všechny dodávané nebo upravované součástí systémů (OS, DB, IS, klientské aplikace) musí logovat svou činnost do logů s možností nastavit úroveň logování pro potřeby diagnostiky.
P.159	Zálohování – dodávaný systém (virtualizace, OS) a DB musí být schopny a připraveny na zálohování systémem objednatele, tj. pro virtualizaci, OS a DB musí existovat agenti umožňující zálohování ze strany objednatele. Informace k zálohovacímu systému objednatele jsou uvedeny v kapitole 7.4.1 – Datové centrum, HW infrastruktura, systémový SW.
P.160	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému (OS, DB, IS, …) pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.161	Dohled – dodávané systémy a technologie musí předávat informace o svém stavu (stavu služeb apod.) na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.

#	Požadavek
P.162	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.163	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 22: Provozní požadavky

4.5 POŽADAVKY NA SLUŽBY

4.5.1 Realizace předmětu plnění

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

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

      Popis bude obsahovat alespoň:
      i) Rozpracování návrhu řešení z nabídky zhotovitele z pohledu instalací a montáže dle informací z implementační analýzy
      ii) Upřesnění rozhraní pro integraci na IS a technologie třetích stran (v případě nutnosti)
      iii) Způsob zajištění projektového řízení na straně zhotovitele pro realizaci předmětu plnění (harmonogram, projektový tým, koordinační mechanismy apod.)
      iv) Detailní návrh a popis postupu implementace, instalace a montáže předmětu plnění
      v) Detailní popis zajištění bezpečnosti systému a informací

         Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně aktivity vedené v kapitole 5 - Harmonogram, s uvedením konkrétních termínů, zhotovitel vhodným způsobem může rozšířit kritické milníky o další aktivity, které mohou být pro projekt klíčové.
      vi) Detailní popis navrhovaného seznámení s funkcionalitami, obsluhou dodávaných technologií a budoucím provozem.

2) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných subdodavatelů.
3) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele, alespoň v následujícím rozsahu:
   a) Vývoj na straně zhotovitele – vývoj jednotlivých systémů, úpravy existujících produktů, jejich parametrizace a nastavení, vývoj a ověřování integračních rozhraní, součinnost se třetími stranami v souvisejících oblastech.
   b) Instalace a implementace do prostředí objednatele v testovacím režimu.
   c) Interní ověření na straně zhotovitele a příprava podkladů pro ověření na straně objednatele (dokumentace, organizace testování a další).
   d) Příprava a naplnění základních dat – z integračních úloh, číselníky, uživatelé a další.

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

4) **Dodávka předmětu plnění**. Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:
   a) Instalace, upgrade a zahoření HW na místě,
   b) Instalace a nastavení HW a SW budou provedeny kvalifikovanými osobami pro dané typy zařízení
   c) Nastavení HW a aplikací
5) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.
6) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.
7) **Realizace pilotního provozu** k ověření funkčnosti systému na menším obejmu dat, s menším počtem uživatelů a na menším počtu zařízení.
8) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.
9) **Zpracování dokumentace skutečného provedení, systémové a provozní dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:

Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení a	Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému.

Název	Popis
systémová/provozní dokumentace	
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 23: 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.

4.5.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií

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

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

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

4.6 ZÁRUKY

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

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

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

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

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

Poskytovatel zajistí HelpDesk pro hlášení vad.

5 HARMONOGRAM

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

#	Fáze	Doba trvání od zahájení	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude dnem podpisu smlouvy na dodávku.
2	Analýza a návrh řešení	45	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace.
3	Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury.	160	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	160	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	170	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	170	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	170	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
8	Převedení do zkušebního provozu.	170	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
9	Bezpečnostní audit a penetrační testy	180	Zpracování a předání bezpečnostního auditu a penetračních testů. *Pozn.: zpracování bezpečnostního auditu bude zahájeno při zahájení realizace. Jedná se o termín předání a akceptace výstupů.*
10	Ukončení realizace dodávky.	180	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 24: Harmonogram

Doplňující informace:

- Pod pojmem „den“ je míněn kalendářní den.

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

6 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

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

Tabulka 25: Místa plnění

7 VÝCHOZÍ STAV

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

7.1 ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA PARDUBICKÉHO KRAJE (ZADAVATEL)

Kontext ZZS PAK v rámci řešení projektu je následující:

1. ZZS PAK 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 PAK musí zajistit výkon veřejné správy v oblasti zdravotnické záchranné služby a podmínky pro zajištění připravenosti poskytovatele zdravotnické záchranné služby (ZZS PAK) 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 PAK je využíván elektronická pošta.

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

7.2 INFORMAČNÍ SYSTÉMY K ZABEZPEČENÍ

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

Všechny uvedené IS jsou umístěny, provozovány a využívány uživateli v sídle ZZS PAK na adrese Průmyslová 450, 530 03 Pardubice. 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 PAK a záložního datového centra v objektu VZ Chrudim v lokalitě Dr. Milady Horákové 1798/47, Chrudim. ZZS PAK má v záložní lokalitě k dispozici datové centrum, rozvodné místnosti a pracoviště uživatelů těchto IS tak, aby byla zajištěna provozuschopnost a bezpečnost provozovaných IS i v případě kybernetických bezpečnostních událostí, mimořádných událostí a krizových situací.

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 PAK 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 Pardubického kraje	Informační systém a technologie pro podporu činností zdravotnického operačního střediska (ZOS) a posádek v terénu, vč. komunikace s posádkami, mezi posádkami a složkami IZS. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZS PAK, tj. poskytování PNP na území Pardubického kraje.	Informační systém (IS)
Elektronická pošta	Zdravotnická záchranná služba Pardubického kraje	Systém pro příjem a odesílání elektronické pošty v rámci komunikace ZZS PAK. Jedná se o hlavní informační systém ZZS PAK zajišťující komunikaci mezi zaměstnanci ZZS PAK a podporu výkonu jejich činností.	Informační systém (IS)

Tabulka 26: Výčet IS k zabezpečení

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

7.2.1 IS ZOS

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

7.2.1.1 Informační systémy a aplikační software ZOS

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

IS, SW, subsystém	Výchozí stav
IS OŘ	Jedná se o produkt S.O.S. (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. 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).

IS, SW, subsystém	Výchozí stav
	Poskytuje funkcionalitu pro všechny činnosti ZOS ZZS počínaje náběrem tísňové výzvy (calltaking) přes operační řízení po vyhodnocení činnosti ZOS. Základní moduly implementované na ZZS PAK: 1. Dispečink 2. Základna 3. Správa a evidence směn 4. Svolávání 5. Statistiky 6. Administrace 7. Správa stanic Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. Integrace telefonie – příjem tísňové výzvy. b. Integrace na GIS – zobrazení polohy tísňové výzvy, polohy výjezdu, lokalizace v mapě apod. c. Integrace na systém sledování vozidel – předávání výzvy k výjezdu, příjem a sledování stavů, sběr informací o výjezdu vozidel. d. MZD/EKP – předávání dat o pacientovi/pacientech k výjezdu pro posádku/posádky a příjem dat o pacientech zpět. e. Integrace na záznamový systém – připojování záznamů hovorů, přehrávání záznamů a identifikace hovoru. f. Národní dopravně informační centrum – odesílání informací do NDIC o dopravních nehodách ze zaznamenaných událostí. g. Integrace telekomunikací a radiokomunikací – pro ovládání spojení a příjem statusů z RS. 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 PAK. 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:

IS, SW, subsystém	Výchozí stav
	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 a SaP dalších složek IZS v rámci integrace na NIS IZS. 4. Lokalizace pro IS OŘ, vyhledávání v mapě a další geografické služby. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. IS OŘ – lokalizace, zobrazování výzev, událostí, poloh vozidel a další služby. b. Systém sledování vozidel (AVL) – čerpání poloh a stavů vozidel a jejich zobrazování v mapě. 2. Externí a. Národní informační systém IZS (NIS IZS) – výměna dat o událostech a SaP s tímto systémem. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
EKP/MZD	Jedná se o produkt společnosti EMD dodaný a využívaný většinou ZZS v ČR. Elektronická karta pacienta (EKP) slouží pro zaznamenávání všech relevantních údajů o výjezdech a pacientech v rámci těchto výjezdů. Data jsou na vstupu čerpána z IS OŘ a následně během nebo po ukončení výjezdu z MZD, kontrolována a následně zpracována do formy pro vykazování pojišťovnám. 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.

IS, SW, subsystém	Výchozí stav
	b. IS Pojišťovna – předávání zpracovaných dat z výjezdu pro vyúčtování zdravotním pojišťovnám. 2. Externí a. eHealth PAK – napojení na nemocnice v Pardubickém kraji. 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. Logy jsou ukládány do tabulky v DB MS SQL v rámci datového centra. Přístup ke čtení k uvedené tabulce bude zajištěn v rámci součinnosti, struktura tabulky bude poskytnuta v rámci implementační analýzy.
IS Pojišťovna	Jedná se o produkt společnosti EMD dodaný a využívaný většinou ZZS v ČR. Slouží pro vyúčtování poskytnuté zdravotnické péče zdravotním pojišťovnám. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. EKP/MZD – přebírání dat o pacientech a výjezdech pro vyúčtování. 2. Externí a. Informační systémy zdravotních pojišťoven. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. 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. Logy jsou ukládány do tabulky v DB MS SQL v rámci datového centra. Přístup ke čtení k uvedené tabulce bude zajištěn v rámci součinnosti, struktura tabulky bude poskytnuta v rámci implementační analýzy.
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

IS, SW, subsystém	Výchozí stav
	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.
Svolávací systém	Je součástí IS OŘ (systém SOS) – viz výše. Subsystém je plně funkční a jeho funkčnost bude rozšířena dle požadavků v kap. 4.4.8 a 4.4.7.
Telefonní ústředna	Telefonní ústředna je produkt Cisco Call Manager. Telefonní ústředna připojená na příjem tísňové linky 155 u telekomunikačního operátora. Telefonní ústředna je interně napojena na: 1. Nahrávací systém (REDAT) pro nahrávání veškerých hovorů a přebírání lokalizace hovorů. 2. Integrace telefonie a radiofonie pro řízení a obsluhu volání přes ústřednu. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Záznamový systém (REDAT)	Jedná se o produkt ReDat společnosti RETIA, a.s. Záznamový systém (REDAT) slouží pro záznam telefonních hovorů na tísňové lince, záznam všech hovorů na ZOS, a to jak telefonních, tak radiofonních. 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.

IS, SW, subsystém	Výchozí stav
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. 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 PAK má v externí lokalitě k dispozici dispečerská pracoviště a repliku IS ZOS, kterou je možné aktivovat a provozovat jako dispečink v této lokalitě. ZZOS byl vybudován v rámci projektu „Rozvoj informačních systémů a technologií ZZS PaK – záložní zdravotnické operační středisko“ v rámci IROP, výzvy č. 28. Subsystémy v záložní lokalitě jsou totožné, jako systémy v primární lokalitě a jedná se o systém IS OŘ, MZD/EKP, Pojišťovna, AVL, GIS a nahrávání hovorů.

Tabulka 27: IS ZOS

7.2.1.2 Pracoviště ZOS

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

Prvek	Údaj(e), parametry a informace
Počet pracovišť	Počet pracovišť: 7 + 1 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 Možnost připojení až 4 monitorů full HD (1920x1080) DVI/HDMI/DP Velikost paměti: 2 GB DDR3 SDRAM

Prvek	Údaj(e), parametry a informace
	Síťové rozhraní: 10/100/1000 Gigabit Ethernet Porty: USB 2.0 (z toho min 2x USB 3.0), 4x DVI/HDMI/DP, 1 RJ-45, 1 sluchátka, 1 vstup pro mikrofon, podpora dotykových obrazovek
Klávesnice	Počet ks / pracoviště: 1 Standardní plnohodnotná klávesnice.
Myš	Počet ks / pracoviště: 1
LCD monitory	Počet ks / pracoviště: 2 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 100 mm, matné provedení Přídavné reproduktory na spodní hraně monitoru, celkový výkon: min 10 wattů, ovládání: zapnutí/vypnutí, hlasitost, výstup na sluchátka, napájení z 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 100 mm
IP telefon	Počet ks / pracoviště: 1 Kompatibilní s integrací telefonie a telefonní ústřednou.
Náhlavní souprava	Počet ks / pracoviště: 1 Drátová náhlavní souprava
Radiové terminály Pegas/Matra (RCT)	Počet ks / ZOS: 2 Technologie TETRAPOL, připojení do sítě PEGAS využívané složkami IZS. Jedná se o záložní komunikační vybavení, primárně jsou pracoviště napojena přes integraci radiofonie k LCT.

Tabulka 28: Pracoviště ZOS

7.2.2 Elektronická pošta

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

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

Přístup je na základě identifikace a autorizace uživatele (v současné době bez napojení na AD), nicméně neprobíhá systematický sběr logů (provozních dat) a vyhodnocení kybernetických bezpečnostních událostí.

Elektronická pošta je provozována následujícím způsobem:

1. Je provozována v primárním datovém centru ZZS PAK – detaily viz kap. 7.3 – Umístění.
2. Systém elektronické pošty využívá systém Kerio Connect ve verzi 9.x na OS Debian
3. Aktiva jsou sdílenými aktivy v rámci primárního DC v rámci samostatného virtuálního serveru. V rámci projektu budou zabezpečena jen centrální aktiva v DC.
4. Provoz je zajištěn v režimu 7x24x365 – Elektronická pošta sice není kritickým systémem, ale je provozována nonstop z důvodu specifického provozu ZZS.
5. Součástí projektu je zajištění Nástroje pro ochranu před škodlivým kódem, tj. technické opatření „e) nástroj pro ochranu před škodlivým kódem“.
6. Součástí projektu jsou nástroje pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí, tj. technické opatření „h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“. Nástroje pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí budou také zpracovávat i bezpečnostní logy centrálního mailového systému ZZS a vyhodnocovat tak případné bezpečnostní události v rámci systému elektronické pošty.

7.3 Umístění IS ZOS, ZZOS, systému elektronické pošty a DC

V následující tabulce jsou uvedena umístění IS ZOS:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Pardubického kraje	Průmyslová 450, Pardubice PSČ: 530 03	Datové centrum ZZS PAK a všechna aktiva IS ZOS umístěná v tomto DC. Dispečerská pracoviště ZOS, kde jsou aktiva (pracoviště) operátorů ZOS.

Místo	Adresa	Předmět realizace
Záložní zdravotnické operační středisko ZZS PAK a záložní datové centrum	Dr. Milady Horákové 1798/47, Chrudim	Záložní zdravotnické operační středisko ZZS PAK a záložní datové centrum jsou umístěny v externí lokalitě v objektu ZZS – VZ Chrudim na uvedené adrese. V této lokalitě je umístěna technologie ZZOS, která je propojena s primárním datovým centrem ZZS PAK a primárním IS ZOS. V lokalitě je dostupná DB replika systému operačního řízení a záložní dispečerská pracoviště. Hlasové spojení je realizováno pomocí krizových mobilních přístrojů a ručních radiostanic. Předmětem projektu bude zabezpečení i aktiv záložního IS ZOS umístěného do tohoto DC.

Tabulka 29: Umístění

7.4 STAV OSTATNÍCH INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

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

7.4.1 Datové centrum, HW infrastruktura, systémový SW a technologie

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

Parametr	Údaj(e), parametry a informace
Datové centrum	
Záložní zdroj el. energie	Primární DC: 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): UPS APC Smart-UPS RT 6000VA (4200W). Nově dodávaná technologie bude napojena na tento záložní zdroj elektrické energie. Záložní DC: Pro kratší výpadky je technologie napojena na bateriové záložní zdroje el. energie (UPS): UPS APC Smart-UPS RT 5000VA – bez diesel agregátu.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříních APC, které jsou umístěny v jedné řadě s dostupností jak zepředu, tak zezadu. Pro nově dodávané technologie ZZS zajistí umístění v rozsahu max. 25 U. Konkrétní umístění a zapojení budou předmětem implementační analýzy.

Parametr	Údaj(e), parametry a informace
Servery	Jako virtualizační servery jsou využívány tři servery DELL PowerEdge R720 a jsou doplněny jedním management serverem DELL PowerEdge R620. 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, SC3020 a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou vyhrazeny 10Gbps switche CISCO a DELL, které tak tvoří infrastrukturu pro iSCSI.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů byly dodány 3 licence Windows Server Datacenter včetně CAL licencí. 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: VMware vCenter Server Standard for vSphereVMware vSphere Standard (6 CPU).
DB	V rámci projektu 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.
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup & Replication pro VMware Enterprise Edition. ZZS poskytne součinnost pro zapojení nově dodávaných technologií a licencí do zálohování. Konkrétní nastavení bude předmětem implementační analýzy.
Syslog server	V rámci stávající infrastruktury ZZOS je provozován syslog server Syslog-ng.
Doména – Active Directory	V rámci infrastruktury je využívána stávající doména v rámci Microsoft Windows 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 150.
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.
Personální systém	V rámci stávajících systémů je využíván personální systém v rámci systému VEMA bez napojení na MS AD. Systém VEMA umožňuje napojení na MS AD.

Parametr	Údaj(e), parametry a informace
SOS-BI	Analytický nástroj využívající ORACLE BI (OBISE1) na OS Windows Srv.
Odesílání SMS	O2 Connector

Tabulka 30: Datové centrum, HW infrastruktura, systémový SW

7.4.2 Datové sítě

V rámci projektu budou využity následující sítě:

Datová síť	Popis
WAN ZZS	Bude využita pro komunikaci mezi lokalitami z důvodu nutné výměny dat souvisejících s realizací a provozem projektu.
NIS IZS / PČR	Napojení na služby NIS IZS a LCT terminály Pegas/Matra. Síťový provoz tohoto napojení bude v rámci dodaných výstupů projektu monitorován.
Internet	V centrální lokalitě je zajištěno připojení k internetu, které bude možné využít i pro požadavky technologií v rámci realizace a provozu projektu.

Tabulka 31: Datové sítě

7.4.3 Síťová infrastruktura

V následující tabulce je uveden popis síťové infrastruktury:

Parametr	Údaj(e), parametry a informace
Primární datové centrum ZZS	
Směrovače	Lokality ZZS jsou propojeny do jedné WAN sítě. Pro tyto účely jsou všechny lokality vybaveny směrovačem WAN operátora. Tyto směrovače jsou ve správě WAN operátora. Stávající WAN operátor je Ha-Vel.
Firewally	V rámci centrální lokality je umístěn centrální FireWall Cisco ASA 5516-X with FirePOWER services, 8GE, AC, DES, 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. Součástí FW jsou licence FirePower IPS and AMP Licences. FireWall odděluje interní síť ZZS nejenom od sítě Internet, ale i od ostatních externích sítí jako je NIS IZS a Krajská síť „LabeNet“. V lokalitě ZZOS je umístěn stejný FireWall.
LAN	V rámci centrální lokality jsou realizovány LAN prvky, a to na bázi switchů. Přičemž centrální stack switchů Cisco 3750 realizuje i routrování VLAN segmentů LAN sítě.
Připojení pracovišť ZOS	Vlastní připojení pracovišť ZOS je realizováno tak, aby výpadek jednoho prvku neznamenal výpadek celého ZOS, ale maximálně poloviny pracovišť. Připojení pracovišť je realizováno v dané lokalitě v rámci lokální LAN sítě.

Parametr	Údaj(e), parametry a informace
Připojení k lince 155	Telefonní ústředna operačního řízení Cisco Call Manager je napojena prostřednictvím hlasové brány a rozhraním ISDN30 do veřejné telefonní sítě. ISDN30 je vyhrazena pro používání linky 155 a pro potřeby dispečinku (operačního řízení). Telefonní ústředna operačního řízení je propojena k SIP trunk a k objektové ústředně. Komponenta telefonní ústředny je provozována i v rámci ZZOS a je schopna převzít funkci centrální ústředny i při výpadku primární lokality.
Připojení k síti NIS IZS – MV ČR (PČR) / NIS IZS	V rámci centrální serverovny je realizováno i napojení na síť NIS IZS a síť PČR. Toto je realizováno samostatnými zálohovanými linkami ve správě České Pošty (NAKIT) a tuto síť garantuje MV ČR.
Připojení ke krajské síti	ZZS má v centrální lokalitě realizováno i napojení na krajské nemocnice v rámci IS eHealth PAK, a to prostřednictvím krajské sítě „LabeNet“.
Připojení k internetu	V centrální lokalitě je i centrální napojení do sítě Internet. Toto připojení je zabezpečeno FireWallem (viz výše). Lokalita ZZOS disponuje samostatným připojením na internet. Poskytovatelem připojení do sítě Internet je Ha-Vel.
Datové centrum PČR	
Aktivní prvky	Připojení do datového centra PČR je realizováno samostatným L2 datovým okruhem určeným pouze pro připojení k LCT terminálů. Na straně PČR je umístěn Switch WS-C2960X-24TS-L, do kterého je připojena veškerá technologie na straně PČR.
Radiové terminály Pegas/Matra (LCT)	V lokalitě PČR je umístěno celkem 8 LCT terminálů propojených do sítě Pegas/Matra.

Tabulka 32: Síťová infrastruktura

7.4.4 Provoz

Provoz stávajícího řešení je zajišťován s následujícími parametry:

1. Provoz systému je v režimu 7x24x365 – jedná se o kritický systém, jehož služby jsou uživatelům k dispozici nonstop, protože ZZS poskytuje služby a plní své úkoly nonstop.
2. IS ZOS je provozován jako vysoce dostupný systém s řadou redundantních prvků přispívajících k vysoké dostupnosti a zajištění funkčnosti i v případech výpadků některých prvků.
3. V rámci provozu je zajištěn dohled, jak je uvedeno dříve v tomto dokumentu.
4. V rámci provozu je zajištěno zálohování, jak je uvedeno dříve v tomto dokumentu.
5. Technická a technologická podpora systému:
    a. Je zajišťována v režimu 7x24x365, aby byla zajištěna vysoká dostupnost dle předchozího bodu.
    b. Součástí je maintenance technologií a dodaného SW, technická a technologická podpora nad rámec záruky s kratšími SLA než v případě záruky.
    c. Je poskytován 1st level support, vyhodnocení hlášených problémů a řešení závad ze strany dodavatele a poskytovatele služeb technické a technologické podpory.

6. Administrace systému je v zodpovědnosti správců ZZS PAK.
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 PAK.
    c. Pozáruční servis HW a SW infrastruktury.

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

KONEC DOKUMENTU