Dodatek č. 4

ke smlouvě č. MPO 05/04400/02 a č. T-Mobile (T-Systems) 2005/268 ze dne 25. 5. 2005

o poskytování služby hostingového centra pro provoz informačního systému „Ústřední evidence podnikatelů – Registr živnostenského podnikání", ve znění Dodatku č. 1 ze dne 27. 4. 2006, Dodatku č. 2 ze dne 20. 4. 2009 a Dodatku č. 3 ze dne 6. 12. 2010 (dále jen „Smlouva")

kterou uzavřely:

Česká republika – Ministerstvo průmyslu a obchodu
se sídlem Na Františku 32, 110 15 Praha 1
IČ: 47609109
DIČ: CZ47609109, neplátce DPH
bankovní spojení: Česká národní banka, pobočka Praha 1
č. účtu: 1525-001/0710
zastoupené **Ing. Bc. Petrem Kameníkem, ředitelem odboru živností**
(dále jen „Objednatel")

a

T-Mobile Czech Republic a.s.
se sídlem Tomíčkova 2144/1,148 00 Praha 4
IČ: 64949681
DIČ: CZ64949681
bankovní spojení: 19-2271190247/0100
zastoupená **Ing. Liborem Komárkem – senior manažerem prodeje zákazníkům segmentu** (na základě pověření)
a
Ing. Miroslavem Kláskem – senior manažerem presalesu (na základě pověření)

(dále jen „Poskytovatel").

Obě smluvní strany uzavírají níže uvedeného dne, měsíce a roku, v souladu s čl. 9, bod 9.5 a čl.18, bod 18.4 Smlouvy, tento Dodatek č. 4 (dále jen „Dodatek") ke Smlouvě:

1 ÚVODNÍ USTANOVENÍ

1.1 Objednatel a společnost T-Systems PragoNet a.s. uzavřely spolu výše uvedeného dne Smlouvu. Právní nástupce společnosti T-Systems PragoNet a.s., společnost T-Systems Czech Republic a.s., a T-Mobile Czech Republic a.s., realizovaly s účinností k 1. 1. 2014 ve smyslu ustanovení § 1 odst. 2, § 60 a násl. a § 100 a násl. zákona č. 125/2008 Sb., o přeměnách obchodních společností a družstev, proces fúze sloučením. V důsledku realizace uvedeného procesu fúze sloučením došlo k zániku T-Systems Czech Republic a.s. bez likvidace a k přechodu veškerého jejího

jmění na T-Mobile Czech Republic a.s., která se stala univerzálním právním nástupcem T-Systems Czech Republic a.s..

1.2 S ohledem na skutečnosti uvedené v předchozím odstavci tak nadále bude v právních vztazích založených Smlouvu vystupovat namísto T-Systems Czech Republic a.s. společnost T-Mobile Czech Republic a.s.

2 *VÝCHODISKA A ÚČEL DODATKU*

2.1 Objednatel je dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a prováděcích předpisů k tomuto zákonu, povinen učinit technická a organizační opatření k zajištění kybernetické bezpečnosti významného informačního systému Registr živnostenského podnikání (dále jen „IS RŽP").

2.2 Objednatel v návaznosti na svou povinnost dle bodu 2.1 a v souladu se Smlouvou požádal Poskytovatele o předložení nabídky na implementaci vybraných opatření k zajištění procesu identifikace, vyhodnocování a zvládání jednotlivých bezpečnostních událostí a incidentů pro IS ŘZP a ochranu integrity komunikačních sítí IS RŽP (včetně služby Security Operation Center).

2.3 Nabídku na dodávku „Zabezpečení infrastrukturní části IS Registru živnostenského podnikání dle zákona o kybernetické bezpečnosti" (dále jen „Nabídka") předloženou Poskytovatelem Objednatel akceptoval na základě jejího projednání a schválení Řídící komisí IS RŽP, a to jak v části technického řešení, tak v části cenové.

2.4 Objednatel vyzval Poskytovatele, v souladu s aktuálním poklesem cen na trhu služeb poskytovaných dle Smlouvy, o předložení cenové aktualizace služeb hostingového centra. Nabídku cenové aktualizace služeb hostingového centra IS RŽP (dále jen „Cenová aktualizace") předloženou Poskytovatelem Objednatel akceptoval na základě jejího projednání a schválení Řídící komisí IS RŽP.

2.5 Účelem tohoto Dodatku je realizace vybraných opatření k zajištění kybernetické bezpečnosti IS RŽP a zároveň úprava ceny za služby poskytované dle Smlouvy.

3 *PŘEDMĚT DODATKU*

3.1 Do čl. 1 bod 1.5 Přílohy č. 1 Smlouvy se doplňuje písmeno l) tohoto znění: „l) detekci, sběr a vyhodnocování bezpečnostních kybernetických událostí a incidentů v infrastrukturní části IS RŽP, včetně služby Security Operation Center, podle Nabídky na dodávku „Zabezpečení infrastrukturní části IS Registru živnostenského podnikání dle zákona o kybernetické bezpečnosti", která tvoří nedílnou součást této Smlouvy jako Příloha č. 1 Dodatku č. 4."

3.2 Do čl. 1 bod 1.6 Přílohy č. 1 Smlouvy se doplňuje písmeno c) tohoto znění: „c) ochranu integrity komunikačních sítí IS RŽP včetně služby Security Operation Center dle Nabídky na dodávku „Zabezpečení infrastrukturní části IS Registru živnostenského podnikání dle zákona o kybernetické

bezpečnosti", která tvoří nedílnou součást této Smlouvy jako Příloha č. 1 Dodatku č. 4."

3.3 V čl. 4 bod 4.4 Přílohy č. 1 Smlouvy písmeno b) zní:
„b) Maximální povolená doba výpadku infrastruktury zóny A provozního systému dle bodu 3.2 písm. a) této Přílohy, včetně provozního rozhraní IS RŽP na ostatní ISVS, činí v běžné pracovní době dle bodu 4.3 této Přílohy v případě, že nejde o rozsáhlou havárii, 60 minut. Stejná maximální povolená doba platí i pro nedostupnost funkcí IS RŽP pro uživatele B zóny provozního systému dle bodu 3.2 písm. b) této Přílohy vlivem výpadku infrastruktury A nebo B zóny".

3.4 Do čl. 10 Smlouvy se doplňuje bod 10.6 tohoto znění: „10.6 Nesplní-li Poskytovatel některou z povinností stanovených v Nabídce na dodávku „Zabezpečení infrastrukturní části IS Registru živnostenského podnikání dle zákona o kybernetické bezpečnosti", která tvoří nedílnou součást této Smlouvy jako Příloha č. 1 Dodatku č. 4, je Objednatel oprávněn účtovat Poskytovateli smluvní pokutu ve výši 5.000,- Kč za každé takové nesplnění/porušení povinnosti. Vedle smluvní pokuty je Poskytovatel oprávněn požadovat i náhradu případné škody, která by mu porušením/nesplněním povinnosti Poskytovatele vznikla."

3.5 Do čl. 4 Smlouvy se doplňuje bod 4.11 tohoto znění: „4.11 Poskytovatel se zavazuje, že poskytne potřebnou součinnost a přístup k dokumentům, které se týkají kybernetické bezpečnosti dle této Smlouvy, a k podpůrným aktivům IS RŽP, jejichž garantem je Poskytovatel, auditním/kontrolním orgánům v případě auditu/kontroly zaměřené na dodržování povinností Objednatele vyplývajících ze zákona č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a jeho prováděcích předpisů."

3.6 Měsíční paušální cena služeb dle Nabídky činí:

HW a SW licence	150 624 Kč
Implementace a provozní dokumentace	9 713 Kč
Průběžné poskytování služby	184 663 Kč
Celkem bez DPH	**345 000 Kč**

Cenová aktualizace činí:

Služba	Cena
TSS linky RŽP	stávající cena 530 352 Kč měsíčně
	nová cena 477 317 Kč měsíčně
	měsíční sleva 53 035 Kč
CSS hosting RŽP	stávající cena 2 927 746 Kč měsíčně
	nová cena 2 635 781 Kč měsíčně
	měsíční sleva 291 956 Kč.

Celková měsíční sleva bez DPH: 345 000 Kč

3.7 Měsíční paušální cena dle čl. 9 odst. 9.1 Smlouvy zůstává beze změny a činí 3 458 098 Kč, DPH 21% činí 726 200,58 Kč, celková cena včetně DPH činí 4 184 298,58 Kč.

4 *PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ*

4.1 Změna čl. 1 bodu 1.5 a 1.6 Přílohy č. 1 Smlouvy dle čl. 3 bodů 3.1 a 3.2 tohoto Dodatku a změna čl. 10 bod 10. 6 a čl. 4 bod 4.11 Smlouvy dle čl. 3 bodů 3.4 a 3.5 tohoto Dodatku nabudou účinnosti podpisem akceptačního protokolu, jímž bude potvrzeno dokončení realizace Nabídky. Stejným dnem nabude účinnosti i Cenová aktualizace dle čl. 3 bodu 3.6 tohoto Dodatku.

4.2 Tento Dodatek nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran. Dnem podpisu se stává tento Dodatek nedílnou součástí Smlouvy.

4.3 Ostatní ustanovení Smlouvy tímto Dodatkem nedotčená zůstávají v platnosti.

4.4 Nedílnou součástí tohoto Dodatku jsou přílohy:

a) **Příloha č. 1** – „Nabídka na dodávku „Zabezpečení infrastrukturní části IS Registru živnostenského podnikání dle zákona o kybernetické bezpečnosti"

b) **Příloha č. 2** – „Cenová aktualizace služeb hostingového centra IS RŽP"

c) **Příloha č. 3** – Pověření Ing. Libora Komárka a Ing. Miroslava Kláska

4.5 Tento Dodatek je sepsán ve čtyřech vyhotoveních s platností originálu, z nichž každá ze smluvních stran obdrží dvě vyhotovení.

V Praze dne 31. 5. 2016

Česká republika – Ministerstvo průmyslu a obchodu

.....

Ing. Bc. Petr Kameník
ředitel odboru živností

V Praze dne 31. 5. 2016

T-Mobile Czech Republic a.s.

.....

Ing. Libor Komárek
senior manažer prodeje

.....

Ing. Miroslav Klásek
senior manažer presalesu

Příloha č. 1

Nabídka na dodávku „Zabezpečení infrastrukturní části IS Registru živnostenského podnikání dle zákona o kybernetické bezpečnosti

Nabídka na dodávku „Zabezpečení infrastrukturní části IS Registru živnostenského podnikání dle zákona o kybernetické bezpečnosti“

T-Mobile Czech Republic a.s.
Tomíčkova 2144/1
148 00 Praha 4
IČO 64949681
DIČ CZ64949681
Spisová značka
B, vložka 3787, společnost je zapsána v OR vedeném Městským soudem v Praze
Bankovní spojení Komerční banka, a.s., Praha 2
Účet číslo 19-2271190247/0100
(dále jen „Dodavatel“)

Dodavatel a předkladatel nabídky:

Společnost	T-Mobile Czech Republic a.s.		
Sídlo: Ulice	Tomíčkova 2144/1		
Město	Praha 4	PSČ	148 00
IČ	64949681	DIČ	CZ64949681
Spisová značka	B. 3787 vedená u rejstříkového soudu v Praze		
Bankovní spojení			
Název banky	Komerční banka a.s., Praha 2		
Účet číslo	19-2271190247 (platby pro dodávky telefonů)	Kód banky	0100
Účet číslo	19-2235210247 (platby pro poskytnuté služby)	Kód banky	0100

(dále jen T-Mobile nebo TMCZ)

Nabídku předkládá a je oprávněn jednat:

Patrik Nikendey
Manažer rozvoje obchodních příležitostí pro státní správu
Tel.: +420 603 606 196
Mobil: +420 720 705 183
E-mail: patrik.nikendey@t-mobile.cz

Nabídku vypracoval:

Karel Galuška
Vedoucí týmu bezpečnosti a business konzultací
Tel.: +420 603 606 177
Mobil: +420 603 411 511
E-Mail: karel.galuska@t-mobile.cz

Nabídka byla vypracována dne 3. 2. 2016 a její platnost je omezena do 30. 4. 2016.

Tato nabídka je pouze základním přehledem nabízených služeb. Podmínky spolupráce budou sjednány v samostatné písemné smlouvě, popř. více smlouvách. Pokud se v nabídce hovoří o „smlouvě" a není uvedeno jinak, jedná se vždy o účastnickou smlouvu. Veškeré ceny uvedené v tabulkách jsou bez DPH.

Obsah

1. Profil dodavatele

Společnost **T-Mobile Czech Republic** je členem skupiny **Deutsche Telekom AG** a v České republice je předním operátorem, poskytujícím jak mobilní služby pro rezidentní klientelu a podnikatele, tak i IT služby pro firemní zákazníky. Integrací společnosti **T-Systems** zajišťujeme současně nabídku úplného portfolia komplexních služeb a péče o ICT i pro ty největší firemní zákazníky a to ve všech oborech – od automobilového průmyslu přes telekomunikace, finančnictví, strojírenství, obchod, služby, energetiku, až po veřejnou správu a zdravotnictví.

Našim hlavním mottem při poskytování ICT služeb v oblasti B2B je podpora zvýšení konkurenceschopnosti zákazníků; proto k nim přistupujeme **s maximální flexibilitou**, respektující jejich konkrétní situaci, ať už technologickou nebo finanční. Vždy jim nabízíme řešení, jež nejlépe vyhovují jejich potřebám a řeší je v celé šíři problematiky, se kterou se zákazníci setkávají. Jedinečná symbióza IT a telekomunikačních služeb, podpořená širokým know-how mateřské společnosti Deutsche Telekom, nám dovoluje realizovat komplexní ICT Službay i v oblasti systémové integrace. Díky trvalé kontrole nad všemi komponenty tak poskytujeme záruku vysoké kvality a spolehlivosti celého řetězce služeb až po jednotlivé aplikace u konkrétních uživatelů.

Dokážeme navrhnout řešení, která Vám přinesou:

- spokojenost vašich zákazníků
- rychlejší reakci na změny vašeho podnikatelského prostředí
- vyšší produktivitu a efektivitu vašich klíčových pracovních procesů (snížení chybovosti, zvýšení rychlosti zpracování)
- lepší připravenost na spolupráci s partnery
- zefektivnění vnitropodnikové komunikace
- optimální řízení a kontrolu hospodaření podniku
- optimální vyhodnocování a sledování efektivity a ziskovosti jednotlivých podnikatelských aktivit
- informace pro optimální financování a finanční řízení vaší firmy
- pomoc při odhalování rizik vašeho podnikání a umožní Vám sledovat trendy
- pomoc při snižování a optimalizaci provozních nákladů

2. Předmět nabídky

Předkládaná Nabídka na bezpečnostní Služby pro

Ministerstvo průmyslu a obchodu ČR
Na Františku 32
110 15 Praha 1
IČO: 47609109
(dále „Zadavatel")

popisuje optimální způsob pro řešení zabezpečení infrastrukturní části **IS Registru živnostenského podnikání** dle zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti.

IS Registru živnostenského podnikání je dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a Vyhlášky (č. 317/2014 Sb.) o významných informačních systémech a jejich určujících kritériích ze dne 15. prosince 2014 **významným informačním systémem (VIS)**, tj. **IS Registru živnostenského podnikání je významný informační systémem (VIS)**.

Nabídka popisuje řešení pro **implementaci vybraných opatření pro VIS** (přesný výčet opatření viz Služby) stanovené zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů a Vyhlášky (č. 316/2014 Sb.) o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) ze dne 15. prosince 2014.

Řešení pro splnění vybraných opatření pro **VIS je rozděleno do dvou Služeb**:

Služba 1 – v infrastrukturní části IS RŽP (včetně služby SOC). Ve spolupráci s poskytovatelem aplikační části IS Registru živnostenského podnikání zajištění procesu identifikace, vyhodnocování a zvládání jednotlivých bezpečnostních událostí a incidentů pro celý IS RŽP

Služba 2 – Ochrana integrity komunikačních sítí IS RŽP (včetně služby SOC)

V následující části jsou uvedeny Služby, které jsou předmětem nabídky.

3. Specifikace Služeb

Úroveň bezpečnosti ICT v jednotlivých státních organizacích se významně liší, protože neexistovala norma, která by nastavila jasný rámec s vymezením oblasti působnosti, zodpovědnosti a pravidel ve formě zákona.

Od 1. 1. 2015 tento rámec stanovuje zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů a Vyhláška (č. 316/2014 Sb.) o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) ze dne 15. prosince 2014.

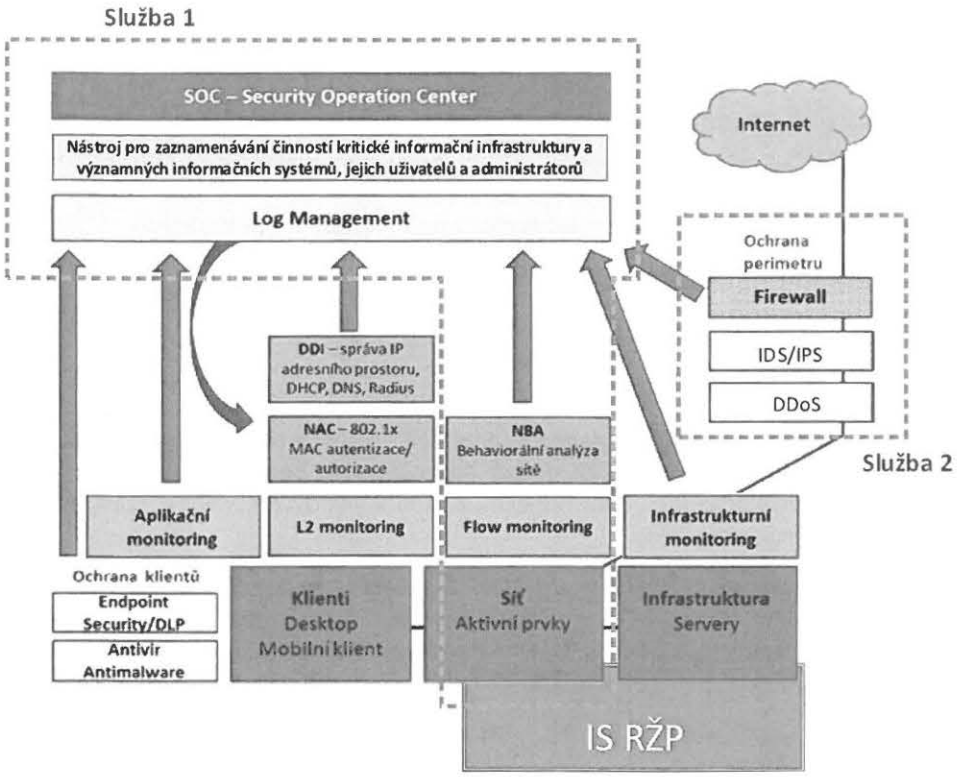
Doposud lokální sítě státních organizací zpravidla nejsou vybaveny nástroji:

- které jsou schopny zjistit anomálie v tomto segmentu – tedy stavy, kdy se zařízení chová jinak než by mělo (zjednodušeně je typickým příkladem neuvědomělé rozesílání spamů, kdy se „nevědoucí" odesílatel = jeho infikovaný počítač (přesněji emailový server) může dostat na tzv. Blacklist, což znamená, že jeho emaily budou blokovány),
- které umožňují předcházet bezpečnostním a provozním hrozbám (odrážet snahy např. o infikování počítačů),
- které jsou schopny reagovat na incidenty (již nakažený počítač, např. připojením na letišti) a
- které umožní zajistit kontinuitu a obnovu jejich klíčových procesů a činností na předem stanovené minimální úrovni, v případě jejich narušení nebo ztráty (politiky ochrany a systém zálohování). Rovněž přístup k bezpečnostní politice (ISMS ISO/IEC 27001), pokud byla nějaká stanovena, doposud nebyl jednotný.

Cesta k nutnému zabezpečení a řízení IT sestává z postupných kroků:

- roztřídíme (kategorizujeme) a zdokumentujeme naše IT vybavení (HW, SW),
- zdokumentujeme uživatele a vymezíme jejich práva přístupu do počítačové sítě a k aplikacím,
- definujeme a nastavíme obecná pravidla, kterými chceme omezit/řídit přístup do naší vnitřní sítě,
- vyřešíme zabezpečení uživatelských zařízení (notebooky a PC) za pomoci antivirových nástrojů,
- zajistíme naše data před zcizením, či zneužitím (DLP – Data Leak Prevention),
- stanovíme bezpečnou hranici mezi naší vnitřní sítí (LAN – Local Area Network) a vnějším světem (internet),
- zajistíme ochranu takto vymezené hranice (firewall),
- ujasníme si, jaká síťová zařízení (firewall, switch, router) chceme sledovat a řídit a jak chceme výstupy vizualizovat a uchovávat,
- zamyslíme se nad tím, které činnosti z výše uvedených lze zjednodušit či automatizovat.

3.1. Koncept nabízených Služeb



Obr.: Služby 1-2 v IS RŽP v kontextu požadavků zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti

Komplexní zabezpečení není jen ochrana zvenčí nebo zevnitř (a ta je především ve státní správě mnohem důležitější), nebo snad nákup drahé technologie a její zapojení do systému. Bezpečnost musí být realizována na základě komplexního přístupu, dle jednotlivých postupů a metodik. Pro státní správu nyní platí primární metodika a tou je zákon o kybernetické bezpečnosti a jeho prováděcí vyhláška.

Jak vybudovat bezpečné IS RŽP znázorňuje obrázek výše, a zahrnuje komplexní ochranu počítačové sítě a IS RŽP.

Tento koncept v sobě odráží jak požadavky ze strany zákona o kybernetické bezpečnosti, tak i zkušenosti z provedené analýza rizik pro IS RŽP.

3.2. Řízení implementace Služeb

Služba zahrnuje:

- **Sestavení realizačního týmu pro jednotlivé Služby**
- **Upřesnění /Zpracování harmonogramu dle Služeb**
- **Vytvoření plánu komunikace**
- **Vedení projektové dokumentace po dobu trvání implementační části Služeb**
- **Řízení rizik v průběhu implementace Služeb**
- **Ukončení projektové fáze Služby a zahájení poskytování Služeb**

Řízení projektové fáze (definice rozsahů, zpřesnění opatření, definice událostí apod.) Služeb je realizováno v souladu s metodikou PRINCE 2. Jedná se o jednu z nejuznávanějších a nejvíce používaných metodik projektového řízení. Jejím použitím budou eliminována mnohá rizika a Služby budou efektivně směřovány k dosažení cílů.

T-Mobile Czech Republic a.s. disponuje rozsáhnou skupinou specialistů vyškolených v používání této metodiky, kteří ji běžně praktikují jako metodu pro řízení dodávky Služeb. Mezi těmito specialisty se nachází i odborníci na informační bezpečnost, tohoto nastavení bude využito i v rámci nabízené dodávky.

Vzhledem k rozsahu, složitosti a charakteru Služeb je vhodnou metodikou pro řízení projektové fáze všech nabízených Služeb právě Prince 2.

Aplikace metodiky zajistí dostatečnou kontrolu a správné řízení základních projektových proměnných:

- Časového harmonogramu
- Nákladů
- Rozsahu Služeb
- Očekávaných přínosů Služeb
- Rizik
- Kvality

Metodika je postavena na těchto základních principech:

- Důraz na produkt (výsledek projektové fáze implementace Služby)
- Jasně definované role a zodpovědnosti
- Řízení pomocí etap
- Dohled nad projektem na základě výjimek (tedy při vybočení z definovaných mezí v některém parametru musí dojít bezprostředně k eskalaci a přijetí korektivního rozhodnutí)
- Poučení ze zkušeností
- Průběžné zdůvodňování přínosů projektu (s ohledem na případné měnící se podmínky)
- Přizpůsobení metodiky na dané parametry Služeb

Tak, aby řízení implementační fáze Služby bylo co nejefektivnější, bude realizováno přizpůsobení metodiky pro konkrétní podmínky Služby.

Po uskutečnění úvodní schůzky projektového týmu (každá Služba bude mít vlastní projektový tým sestavený z definovaných specialistů dle specializací) je vytvořen Manuál řízení projektu. Pokud to budou okolnosti vyžadovat, Manuál řízení projektu může být připraven pro každou Službu nebo bude jen jeden pro lepší administraci projektu. V tomto dokumentu se nastaví základní projektové vztahy, určí složení týmů pro další etapy, upřesní se obsah a termíny hlavních milníků implantační fáze Služby, termíny prezentací a akceptací dílčích výstupů i termín předpokládaného dokončení prací. Výstupem z této etapy je také harmonogram prací a určení odpovědných pracovníků za jednotlivé úkony.

Projektový tým vede Vedoucí projektu za Uchazeče (Dle potřeb může být ustanoven projektový tým pro každou Službu.). Způsob komunikace projektového týmu a další detaily řízení projektu upřesní projektový tým v Manuálu řízení projektu.

Dodavatel požaduje, aby byl pro realizace vytvořen projektový tým, ve kterém budou zastoupeni i zástupci Zadavatele. Účast subdodavatelů IS RŽP v projektových týmech je silně doporučena.

Za každou stranu musí být určen odpovědný pracovník za Dodavatele a Zadavatele. Ze strany Zadavatele je důležité, aby tento pracovník byl vybaven pravomocí sjednávat dílčí pracovní termíny, případně operativní změny v harmonogramu prací. Dále by měl mít pravomoc podepisovat akceptační protokoly v zastoupení Zadavatele.

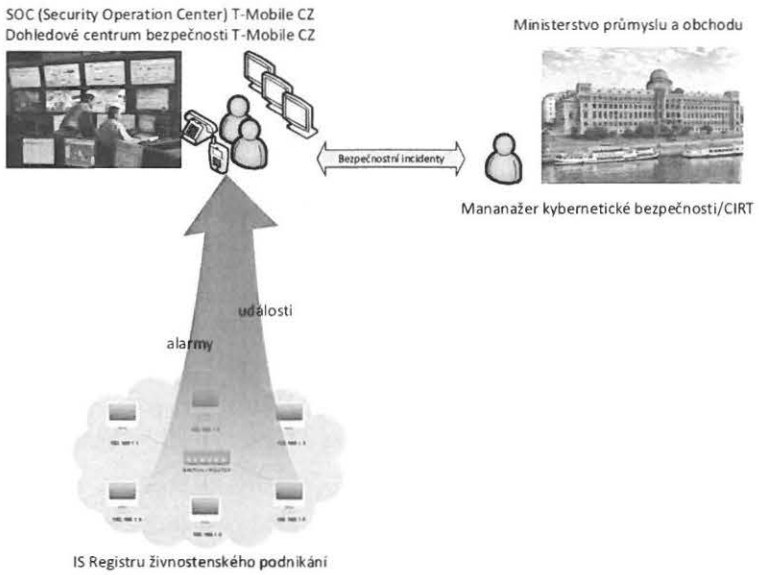
V případech, kdy bude nutno pro zpracování některých výstupů interních kapacit Zadavatele, bude tak postupováno po dohodě se Zadavatelem.

3.3. Služba Security Operation Center (SOC)

Služba zahrnuje:

- **Reporting**
- **Analýza reportů**
- **Návrh systematických opatření**
- **Monitoring v reálném čase**
- **Zakládání incidentů**
- **Návrhy řešení incidentů**
- **Analýza incidentů**
- **Bezpečnostní dohled**
- **Předschválená samostatná reakce**

Služba SOC – Security Operation Center (Dohledové centrum bezpečnosti) je nevyhnutnou součástí všech nabízených Služeb, aby byly naplněny požadavky zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. SOC poskytuje dohled nad nástroji Služeb 1 a Služeb 2.



Obr.: Služba SOC v kontextu IS RŽP

Služba SOC je poskytována formou kvalifikovaného bezpečnostního dohledu v nepřetržitém režimu, kdy operátoři SOC on-line sledují a vyhodnocují probíhající bezpečnostní události a reagují na ně.

Vedle automatického zakládání incidentu v Helpdesku IS RŽP jsou operátoři oprávněni zakládat incident ručně, podle svého odborného posouzení. Analýza události je zahájena okamžitě a zajištěna je také v nepřetržitém režimu rolí analytika. V pohotovosti je také pracovník nadstandardního provozu. Dochází-li k bezpečnostnímu incidentu, operátoři jsou oprávněni ukončit ohroženou službu či provést jiný, předem daný zásah, pokud symptomy a dopady přesně odpovídají check-listu.

3.4. Služba 1 – Detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí v IS RŽP

3.4.1. Požadavky na Službu 1

Seznam požadovaných opatření, které budou implementovány Službou 1 do IS Registru živnostenského podnikání:

Požadavky na Službu 1 vyplývající ze Zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti			**Požadavky na Službu 1 vyplývající z Akčního plánu pro splnění Zákona o kybernetické bezpečnosti a vyhlášky** *(označení dle plánu)*	**Zranitelnosti IS RŽP pokryty Službou 1 z Plánu zvládání rizik dle Analýzy rizik IS RŽP** *(označení dle plánu)*
vyhláška o kybernetické bezpečnosti	§ 22	**Nástroj pro detekci kybernetických bezpečnostních událostí** (1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.	**G03** - Nasazení a využití nástroje pro detekci a vyhodnocení bezpečnostních událostí dle požadavků ZKB / VKB **G04** - Nasazení, využití a údržba nástroje pro sběr a vyhodnocování kybernetických bezpečnostních událostí dle požadavků ZKB / VKB **G05** - Definovat postupy pro použití nástrojů pro oznamování bezpečnostních incidentů **G06** - Nastavit proces pravidelné aktualizace nastavení pravidel v nástroji pro detekci a vyhodnocování bezpečnostních událostí **G07** - Definovat postupy pro vyhodnocení informací z nástroje pro optimální nastavení opatření **G08** - Aktualizovat provozní postupy	**Z08** - Není nastavený proces pro vyhodnocování a řešení bezpečnostních událostí, včetně hlášení na NBÚ (evidence a vyhodnocení událostí, kategorizace incidentů, řešení incidentů) **Z09** - Nedostatečná detekce, monitorování bezpečnostních incidentů **Z10** - Nedostatečné vyhodnocování bezpečnostních událostí
		(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dál používá nástroj pro detekci kybernetických bezpečnostních událostí, které zajistí ověření, kontrolu a případně zablokování komunikace A. v rámci vnitřní komunikační sítě a B. serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.		
vyhláška o kybernetické bezpečnosti	§ 23	**Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí** (1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona používá nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními		

		potřebami a výsledky hodnocení rizik zajistí A. integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury, B. poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury a C. nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.		
		(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále zajistí A. pravidelnou aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování, a B. využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních		

		událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury. (Poznámka: Definovat postupy pro vyhodnocení informací z nástroje pro optimální nastavení opatření.)		
vyhláška o kybernetické bezpečnosti	§ 13	**Zvládání kybernetických bezpečnostních událostí a incidentů** Orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů B. připraví prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle § 21 až 23, provádí jejich vyhodnocení a identifikuje kybernetické bezpečnostní incidenty, C. provádí klasifikaci kybernetických bezpečnostních incidentů, přijímá opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, provádí hlášení kybernetického bezpečnostního incidentu podle § 32 a zajistí sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,...		
vyhláška o kybernetické bezpečn	§ 5	**Bezpečnostní politika** (1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona stanoví bezpečnostní politiku v oblastech		

osti		S. nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí, T. využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a... (Poznámka: V rámci Služby 1 budou pravidla stanoveny bezpečnostní politikou pro uvedené oblasti implementována.)		
		(3) Orgán a osoba uvedená v § 3 písm. c) až e) zákona pravidelně hodnotí účinnost bezpečnostní politiky a aktualizuje ji. (Poznámka: V rámci Služby 1 nastavit proces pravidelné aktualizace nastavení pravidel v nástroji pro detekci a sběr bezpečnostních událostí.)		
vyhláška o kybernetické bezpečnosti	§ 10	Řízení provozu a komunikací (3) Provozní pravidla a postupy orgánu a osoby uvedené v § 3 písm. c) a d) zákona obsahují C. postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech, D. spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží, E. postupy řízení a schvalování provozních změn... (Poznámka: Službou 1 budou implementovány C, D a E jen ve vztahu k nástroji pro detekci a sběr bezpečnostních událostí.)		

Požadavky na Službu 1 vyplývající ze Zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti			**Požadavky na Službu 1 vyplývající z Akčního plánu pro splnění Zákona o kybernetické bezpečnosti a vyhlášky** *(označení dle plánu)*	**Zranitelnosti IS ŘZP pokryty Službou 1 z Plánu zvládání rizik dle Analýzy rizik IS ŘZP** *(označení dle plánu)*
vyhláška o kybernetické bezpečnosti	§ 19	**Nástroj pro řízení přístupových oprávnění** (2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále používá nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik. (Poznámka: Služba 1 podporuje Nástroj pro řízení přístupových oprávnění z hlediska zaznamenávání použití přístupových oprávnění. Nástroj pro řízení přístupových oprávnění není předmětem implementace Služby 1.)	K01 - Definovat údaje, které budou v rámci logování zaznamenávány, tak aby naplňovaly požadavky VKB K02 - Implementovat logování v definovaném rozsahu v rámci IS RŽP K03 - Definovat proces a rozsah logování v případech použití přístupových oprávnění (Poznámka: V rámci Služby 1 bude definován proces a rozsah logování pro použitá přístupová oprávnění, tj. při použití různých oprávnění budou zaznamenávány Nástrojem pro zaznamenávání činností jiné činnosti uživatele.) K04 - Implementovat logování použití přístupových práv v rámci IS RŽP K05 - Definovat opatření pro ochranu auditních záznamů / logů K06 - Nastavit dobu archivace výše zmíněných logů na minimálně 3 měsíce	Z11 - Nedostatečné logování a kontrola činnosti kritických rolí (administrátorů, super uživatelů) v systémech (nedostatečná politika, rozsah logování, archivace a ochrana logů) Z25 - Nemožnost kontroly oprávněnosti změn v rejstříku autorizovaným uživatelem. Z12 - Nedostatečný nástroj pro sledování činností administrátorů
vyhláška o kybernetické bezpečnosti	§ 21	**Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů** (1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajistí A. sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a B. ochranu získaných informací před neoprávněným čtením nebo změnou.		

		(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona dále pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému zaznamenává A. přihlášení a odhlášení uživatelů a administrátorů, B. činnosti provedené administrátory, C. činnosti vedoucí ke změně přístupových oprávnění, D. neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů, E. zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, F. automatická varovná nebo chybová hlášení technických aktiv, G. přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a H. použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.		
		(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona záznamy činností zaznamenané podle odstavce 2 uchovává nejméně po dobu **3 měsíců**. (Poznámka: Služba 1 bude implementována tak, aby byla dodržena dobu archivace výše zmíněných logů minimálně 3 měsíce.)		

		(4) Orgán a osoba uvedená v § 3 písm. c) až e) zákona zajišťuje nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému. (Poznámka: Opatření bude v Službě 1 realizováno len ve vztahu k Nástroji pro zaznamenávání činností kritické informační infrastruktury.)		
vyhláška o kybernetické bezpečnosti	§ 10	**Řízení provozu a komunikací** (6) Orgán a osoba uvedená v § 3 písm. c) a d) zákona v rámci řízení komunikací B. určí pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi, C. provádí výměnu a předávání informací na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla dokumentuje a D. s ohledem na klasifikaci aktiv provádí výměnu a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací. (Poznámka: Ve vztahu k B, C a D bude Služba 1 definovat opatření pro ochranu auditních záznamů / logů.)		

3.4.2. Popis Služby 1

Činnosti, které budou implementovat opatření (viz 3.4.1) Službou 1 do IS Registru živnostenského podnikání a budou pravidelně poskytovány Zadavateli:

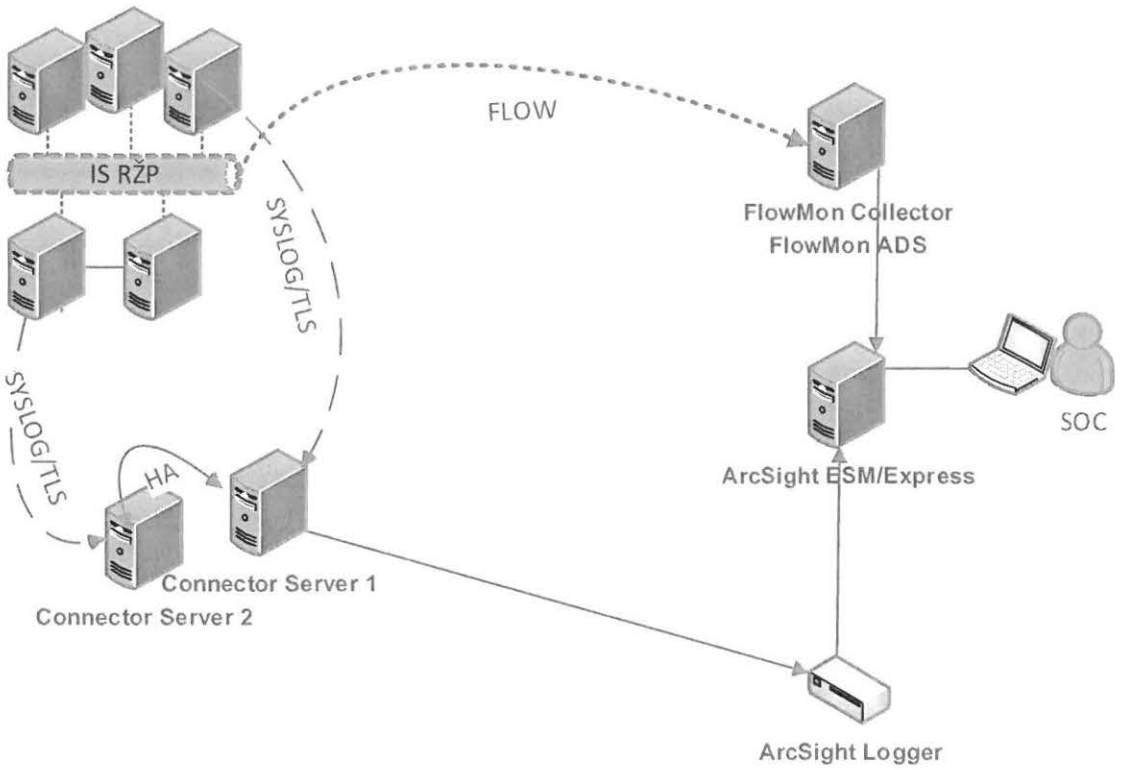
Služba 1. je poskytována zahájením implementační fáze.		Dodavatel Služby si bude dnem zahájení této fáze nárokovat u Zadavatele úhradu dojednané ceny za Službu 1 (viz kap. 4).
IMPLEMENTAČNÍ FÁZE SLUŽBY		
Identifikátor činnosti	**Činnosti v časové souslednosti**	**Popis činnosti a výstupy činnosti**
S1/01	Zahájení Řízení implementace Služby 1.	Dle zásad uvedených v kap. 3.2 je zahájeno řízení implementační fáze Služby 1. **Všechny písemné výstupy uvedeny v kap. 3.2** jsou Zadavateli předány jako výstup implementační fáze Služby 1.
S1/02	Popis architektury zapojení nástrojů Služby 1 v kontextu exitující architektury IS RŽP.	Dodavatel navrhne **popis architektury nástrojů Služby 1** a zapojení nástroje do IS RŽP a projedná v rámci projektového týmu pro Službu 1, je písemným výstupem implementační fáze Služby 1.
S1/03	Definovaní bezpečnostních událostí sledovaných nástrojem a míst detekce událostí. Definovaní pravidelných reportů pro Manažéra kybernetické bezpečnosti Zadavatele apod.	Dodavatel navrhne a projedná v projektovém týmu Služby 1 **seznam bezpečnostních událostí, místa sběru těchto událostí v IS RŽP, jejich kategorizaci**. Tento seznam je písemným výstupem implementační fáze Služby 1.
S1/04	Definování úkolů a instrukcí pro SOC. (Procesní postupy, komunikační matice, eskalační procedury, atd.)	Dodavatel navrhne **instrukci pro personál SOC** a projedná v projektovém týmu Služby 1, tak by se naplnili požadavky Zadavatele na způsob komunikace s Manažerem kybernetické bezpečnosti, hlášení bezpečnostních události apod.
S1/05	Implementace nástrojů Služby 1	Dodavatel zahájí instalaci HW a SW do prostředí IS RŽP. Dodavatel připojí v této činnosti nástroj k prvkům IS RŽP. Účast zástupců dodavatelů IS ŘŽP v projektovém týmu Služby 1 je pro stanovení správného postupu nasazení nástroje silně doporučena. Přesný harmonogram a postup nasazení a postup bude projednán v projektovém týmu Služby 1. Konečný harmonogram a postup instalace nástroje schválí Zadavatel po projednání v projektovém týmu Služby 1.
S1/06	Testování provozních parametrů a kompatibility nástroje a IS RŽP.	Dodavatel a provozovatelé IS RŽP provedou hodnocení nasazeného nástroje v rámci projektového týmu Služby 1, zda jsou ovlivněny kritické a provozní parametry IS RŽP. Dodavatel nástroje provede úpravy v parametrizaci nástroje, tak aby nebyl významně ovlivněn provoz IS RŽP.
S1/07	Sběr bezpečnostních událostí 1 fáze.	Dodavatel provede nastavení nástroje a zahájí sběr základních definovaných bezpečnostních událostí. Dodavatel nástroje a dodavatelé IS RŽP v rámci projektového týmu Služby 1 vyhodnotí min. po 2 týdnech provozu, zda jsou ovlivněny kritické a provozní parametry IS

		RŽP.
S1/08	Školení personálu SOC a Manažera kybernetické bezpečnosti.	Dodavatel provede školení obsluhy nástroje a uživatele nástroje. **Záznam o školení** je písemným výstupem
S1/09	Sběr bezpečnostních událostí 2 fáze.	Dodavatel provede nastavení nástroje a doplní nastavení nástroje o další definované bezpečnostní události. Dodavatel nástroje a dodavatelé IS RŽP v rámci projektového týmu Služby 1 vyhodnotí min. po 2 týdnech provozu, zda jsou ovlivněny kritické a provozní parametry IS RŽP. Dodavatel nástroje provede úpravy v parametrizaci nástroje, tak aby nebyl významně ovlivněn provoz IS RŽP.
S1/10	Sběr bezpečnostních událostí 3 fáze. Ukončení testovací fáze.	Dodavatel provede závěrečné nastavení nástroje a nastaví úplný sběr události dle definovaných bezpečnostních událostí. Dodavatel nástroje a dodavatelé IS RŽP v rámci projektového týmu Služby 1 vyhodnotí min. po 2 týdnech provozu, zda jsou ovlivněny kritické a provozní parametry IS RŽP. Dodavatel nástroje provede úpravy v parametrizaci nástroje, tak aby nebyl významně ovlivněn provoz IS RŽP. Testovací provoz je ukončen a změny lze provádět jen dle Postupu aktualizace sledovaných bezpečnostních událostí a nástroje.
S1/11	Akceptace Služby 1 Zadavatelem	Zástupce Zadavatele provede formální akceptaci provozu nástroje. **Akceptační protokol o provozu Služby 1** je písemným výstupem implementační fáze Služby 1.
S1/12	Definování postupu aktualizace sledovaných bezpečnostních událostí a nástroje do maximální disponibilní kapacity nástroje. Stanovení schvalovacího postupu pro změny v souvislosti s nástrojem.	Dodavatel navrhne **Postup aktualizace sledovaných bezpečnostních událostí a nástroje** a tento návrh projedná v projektovém týmu pro Službu 1. Tento postup je písemným výstupem implementační fáze Služby 1. Dodavatel stanovuje max. disponibilní kapacity[1] nástrojů Služby 1 pro vyžití Zadavatelem takto: • **HP ArcSight Logger, max. 200 EPS** • **Objem ukládaných logů 1,5 TB s retencí 6 měsíců** Tyto technické parametry tvoří hranice, které nelze při rozšiřování nástrojů Služby 1 překročit.
S1/13	Akceptace písemných výstupů za Službu 1 Zadavatelem.	Zástupce Zadavatele provede formální akceptaci všech písemných výstupů za Službu 1. Písemné výstupy jsou v této tabulce vyznačeny **tlustě**.
S1/14	Ukončení Řízení implementace Služby 1.	Projekty tým pro Službu 1 ukončí svou činnost a předá agendu personálu SOC.
Služba 1 je dále poskytována dle parametrů definovaných v implementační fázi.		Služba 1 již dále není řízena a poskytována dle projektových zásad definovaných v kap.

[1] Disponibilní výkon nástroje je množství prostředků/kapacita nástroje, které má Zadavatel max. k dispozici pro čerpání za sjednanou cenu. Je to rámec výkonu nástroje snížený o výkon již sledovaného provozu apod. Překročení disponibilního výkonu není buď technicky možné, nebo za stávající sjednanou cenu nelze výší výkon nástroje požadovat.

		3.2 Služba je dále řízena a poskytovaná dle procesní dokumentace (písemných výstupy implementační fáze Služby 1) definované a vytvořené v implementační fáze Služby 1.
PROVOZNÍ FÁZE SLUŽBY		
S1/15	Personál vykonává dohled nad všemi nástroji Služby 1. Personál SOC vykonává činnosti dle postupů (písemné výstupy) definovaných v implementační fázi Služby 1. Služba 1 je poskytována v rozsahu definovaném v implementační fázi.	Služba 1 je poskytována v rozsahu popsaném v této nabídce, smlouvě a dokumentech připravených v implementační fáze Služby 1 (viz výše).
S1/16	Aktualizace sledovaných bezpečnostních událostí nástrojem se provádí dle pravidel definovaných v implementační fázi Služby 1.	Jakékoli změny v souvislosti s nástrojem již je možné provádět jen dle **Postupu aktualizace sledovaných bezpečnostních událostí a nástroje,** který byl připraven v implementační fáze Služby 1.

3.4.3. Přehledová architektura zapojeni nástrojů Služby 1



Obr.: Přehledová architektura zapojení nástrojů Služby 1

3.4.4. Nástroj na detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí a nástroj pro zaznamenávání činností - ArcSight

HP ArcSight ESM/Express je nástroj Služby 1. - HP ArcSight ESM/Express zpřístupňuje možnosti nejmodernějších způsobů evidence a korelací všech možných událostí novému segmentu uživatelů. HP ArcSight ESM/Express analyzuje záznamy z libovolného zařízení přítomného ve vašem systému nebo síti, určuje, jestli se vyskytla nějaká potenciálně riziková událost a včas informuje administrátory o tom, co mají podniknout.

Systém ArcSight ESM monitoruje všechny události, které by mohly mít vliv na bezpečnost firmy – od pohybu osob po přístup k citlivým datům a využívání různorodých informačních zdrojů. Pomáhá vyhodnotit význam libovolných událostí v reálném čase tím, že je zařadí do správného kontextu. To znamená, že určí, kdo, co, kde a kdy tuto událost vyvolal, proč se tak stalo a jaký to má dopad na případná rizika pro IS RŽP.

HP ArcSight ESM/Express vytváří korelační infrastrukturu, která pomáhá identifikovat význam libovolné události zařazením do správného kontextu, to znamená určením, kdo, co, kde a kdy tuto událost vyvolal, proč se to stalo a jaký to má dopad na rizika daného byznysu. Korelace ArcSight ESM vedou na přesné a automaticky přidělované priority bezpečnostních rizik a porušení platných regulačních směrnic (Compliance Requirements) v oblasti, která je pro danou firmu relevantní. Infrastruktura ESM nabízí propracované možnosti sběru informací v té nejširší knihovně zdrojů událostí - shromažďuje záznamy z více než 275 zařízení a zdrojů událostí, včetně OS, síťových zařízení (routery, switche), síťových analyzátorů (síťové monitory a analyzátory provozu, NAC, NBA),

bezpečnostních řešení (IPS/IDS, firewally, VPN, skenery zranitelnosti), ale také záznamy a zprávy z aplikací, databází, z řešení identity management a z webových serverů a webově orientovaných aplikací. Události z různých zařízení téže rodiny (např. routery) jsou normalizovány, aby se daly navzájem snáze porovnávat a analyzovat. Volitelné Solution Packages nabízejí podporu a zaměření na nejdůležitější problémy a na takové iniciativy, jako jsou SOX, PCI, HIPAA, GLBA, monitorování uživatelů a administrátorů IT.

HP ArcSight ESM/Express nabízí řadu vymožeností, které zajišťují rychlý, pohodlný a intuitivní přístup k informacím. Nastavitelné a graficky bohaté řídicí pulty (dashboardy) obsahují pohledy přizpůsobené jak pro byznys, tak pro techniky a příslušným jedincům v organizaci poskytují dokonalý přehled. Na tzv. ESM Console je k dispozici jedinečný pohled na celkový stav firemní bezpečnosti, odvozený z potvrzených útoků a provozních rizik, zatímco geografické a síťové mapy dovolují pověřeným uživatelům dohlížet na jednotlivé oblasti, za něž v organizaci zodpovídají.

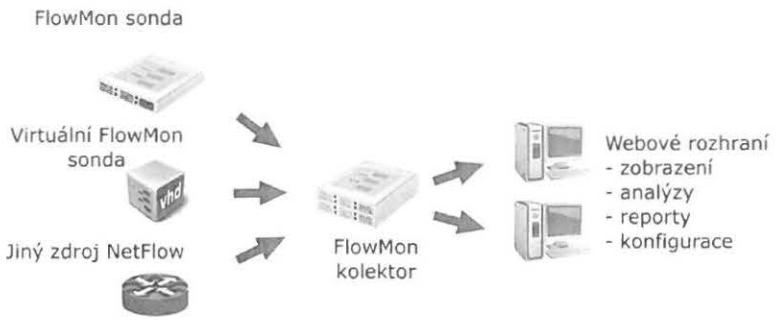
HP ArcSight ESM/Express vytváří obsažné technické, provozní a trendové sestavy, které informují o bezpečnostní situaci a splňují požadavky předepsaných výstupů. S tímto systémem výstupů je reporting pro vedení jednoduchý, protože lze využívat standardní a upravitelné šablony k hlášení o dodržování regulačních směrnic a nařízení (compliance status), o rizikách byznysu a profilování uživatelů. Vedle předpřipravených sestav a šablon dovoluje výstupní systém uživatelům vytvářet i vlastní nové sestavy a šablony pro plánovaná nebo ad-hoc požadovaná hlášení. Systém kombinuje bohatě korelované informace do komplexních pohledů, které všem zainteresovaným umožňují identifikovat rizikové oblasti, informují je o hodnotě a efektivnosti bezpečnostních opatření a jednoduše odpovídají na klíčové manažerské otázky. Sestavy ukazující trendy usnadňují sledování událostí a jejich důsledků v průběhu času. Za pomoci korelační technologie se vyhodnocování trendů dá využít i k simulacím scénářů "co když" a zjišťovat vlivy, které mají změny v bezpečnosti politice na celkovou bezpečnostní situaci a výskyt rizik ve společnosti.

HP ArcSight Logger je nástroj Služby 1. - ArcSight Logger nabízí nejmodernější a finančně efektivní správu záznamů dat libovolného typu, vhodnou k ochraně soukromých i veřejných organizací všech velikostí.

ArcSight Logger podporuje sběr syrových nebo nestrukturovaných záznamů z libovolných systémových nebo souborových protokolů (syslog ap.) a disponuje také obrovskou knihovnou konektorů (ArcSight Connectors), které dokáží sbírat údaje z více než 300 různých zdrojů generujících vlastní protokoly. Kromě toho zahrnuje i nástroj ArcSight FlexConnector, který možnosti sběru dat dále rozšiřuje i na libovolné zákaznické zdroje a firemní aplikace potřebné kvůli regulačním nařízením a forenznímu zkoumání. ArcSight Connectors se dají nasazovat jako software nebo jako speciální zařízení do datových center a do regionálních poboček, aby tam zajistily bezpečný a spolehlivý sběr údajů. Tyto konektory také nabízejí kontrolu šířky pásma, určování priorit pro posílání záznamů, lokální ukládání a další opatření za účelem minimalizace ztráty dat, resp. nežádoucího ovlivňování kritických podnikových procesů.

3.4.5. Nástroj pro detekci kybernetických bezpečnostních událostí – FlowMon

FlowMon kolektor je nástroj Služby 1. - FlowMon kolektory jsou výkonná zařízení pro sběr, zobrazení, analýzu a dlouhodobé uložení síťových statistik (NetFlow v5/v9, IPFIX, sFlow, případně další kompatibilní s technologií NetFlow) ze zařízení podporující technologii flow (switche, routery), FlowMon sond či jiných zdrojů. Pro tyto účely je vybaven velkým úložným prostorem s podporou technologie RAID. Jedná se o profesionální řešení pro střední a velké sítě. Uživatelské rozhraní umožňuje administrátorům i manažerům přehledně a jednoduše vizualizovat zjištěné statistiky. Pomocí speciálních dotazů lze zobrazit komunikaci mezi konkrétními stanicemi, s využitím dané služby, v určitém časovém rozmezí a mnoho dalších údajů potřebných pro provádění provozních i bezpečnostních analýz a dohled nad sítí. Pro efektivnější správu a včasné řešení nastalých problémů lze využít automatické upozorňování na anomální a nežádoucí stavy dle preferencí zákazníka.



Obr.: Možnosti připojení do FlowMon kolektoru

FlowMon kolektor se dodává v několika hardwarových konfiguracích podle poskytovaného výkonu (počet zpracovávaných toků za sekundu), velikosti diskového pole a typu použitého RAIDu. Základní verze se dodává jako kompaktní 1U řešení se softwarovou podporou RAID5 a úložnou kapacitou vhodnou pro sítě s nižším počtem zdrojů dat či krátkou historií pro uchovávání zaznamenaných statistik. Pro střední a velké sítě je vhodný model s velkým diskovým prostorem a s hardwarovým RAID5 či RAID6. FlowMon kolektor je dostupný i ve formě virtuálního zařízení pro nasazení ve VMware nebo Hyper-V virtuálním prostředí. Virtuální kolektory se liší výkonem a diskovou kapacitou pro uložení síťových statistik.

FlowMon ADS je nástroj Služby 1 – FlowMon ADS je moderní systém detekce anomálií a nežádoucího chování v datové síti, založený na permanentním vyhodnocování statistik o provozu na síti. Cílem řešení je odhalení provozních problémů a zvýšení vnější i vnitřní bezpečnosti datové sítě. Hlavní výhodou proti běžným IDS systémům či SNMP monitoringu je orientace na celkové chování zařízení na síti, což umožňuje reagovat na dosud neznámé nebo specifické hrozby. Výhodou oproti většině konkurenčních zařízení, je možnost nasadit zařízení do 30 minut bez jakéhokoliv narušení síťového provozu.

FlowMon ADS je navržen tak, aby jej bylo okamžitě možné nasadit a začít používat v různých prostředích. Zapojení samotného zařízení je velmi jednoduché a nijak neohrozí standardní chod síťové infrastruktury. První výsledky přitom přinese cca za 20 minut od zapojení.

3.4.6. Harmonogram implementace Služby 1

	Činnosti v časové souslednosti	TÝDEN (OD PODPISU SMLOUVY) 1	2	3	4	5	6	7	8	9	#	#	#	#	#	#	#	#	#
S1/01	Zahájení Řízení implementace Služby 1.																		
S1/02	Popis architektury zapojení nástrojů Služby 1 v kontextu exitující architektury IS RŽP.																		
S1/03	Definovaní bezpečnostních událostí sledovaných nástrojem a míst detekce událostí. Definovaní pravidelných reportů pro Manažéra kybernetické bezpečnosti Zadavatele apod.																		
S1/04	Definování úkolů a instrukcí pro SOC. (Procesní postupy, komunikační matice, eskalační procedury, atd.)																		
S1/05	Implementace nástrojů Služby 1																		
S1/06	Testování provozních parametrů a kompatibility nástroje a IS RŽP.																		
S1/07	Sběr bezpečnostních událostí 1 fáze.																		
S1/08	Školení personálu SOC a Manažera kybernetické bezpečnosti.																		
S1/09	Sběr bezpečnostních událostí 2 fáze.																		
S1/10	Sběr bezpečnostních událostí 3 fáze. Ukončení testovací fáze.																		
S1/11	Akceptace Služby 1 Zadavatelem																		
S1/12	Definování postupu aktualizace sledovaných bezpečnostních událostí a nástroje do maximální disponibilní kapacity nástroje. Stanovení schvalovacího postupu pro změny v souvislosti s nástrojem																		
S1/13	Akceptace písemných výstupů za Službu 1 Zadavatelem.																		
S1/14	Ukončení Řízení implementace Služby 1.																		
S1/15	Personál vykonává dohled nad všemi nástroji Služby 1. Personál SOC vykonává činnosti dle postupů (písemné výstupy) definovaných v implementační fázi Služby 1. Služba 1 je poskytována v rozsahu definovaném v implementační fázi.																		
S1/16	Aktualizace sledovaných bezpečnostních událostí nástrojem se provádí dle pravidel definovaných v implementační fázi Služby 1.																		

3.5. Služba 2 – Ochrana integrity komunikačních sítí IS RŽP

3.5.1. Požadavky na Službu 2

Seznam požadovaných opatření, které budou implementovány Službou 2 do IS Registru živnostenského podnikání:

Požadavky na Službu 2 vyplývající ze Zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti			**Požadavky na Službu 2 vyplývající z Akčního plánu pro splnění Zákona o kybernetické bezpečnosti a vyhlášky** *(označení dle plánu)*	**Zranitelnosti IS ŘZP pokryty Službou 2 z Plánu zvládání rizik dle Analýzy rizik IS ŘZP** *(označení dle plánu)*
vyhláška o kybernetické bezpečnosti	§17	**Nástroj pro ochranu integrity komunikačních sítí** (1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, zavede D. ...opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě.	N03 - Definovat opatření pro filtrování přenášených dat	Z27 - Systém není dostatečně ošetřen proti útoku typu DDoS
		(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále využívá nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.		

3.5.2. Popis Služby 2

Činnosti, které budou implementovat opatření (viz 3.5.1) Službou 2 do IS Registru živnostenského podnikání a budou pravidelně poskytovány Zadavateli:

Služba 2 je poskytována zahájením implementační fáze.		Dodavatel Služby si bude dnem zahájení této fáze nárokovat u Zadavatele úhradu dojednané ceny za Službu 2 (viz kap. 4).
IMPLEMENTAČNÍ FÁZE SLUŽBY		
Identifikátor činnosti	**Činnosti v časové souslednosti**	**Popis činnosti a výstupy činnosti**
S2/01	Zahájení Řízení implementace Služby 2.	Dle zásad uvedených v kap. 3.2 je zahájeno řízení implementační fáze Služby 2. **Všechny písemné výstupy uvedeny v kap. 3.2** jsou

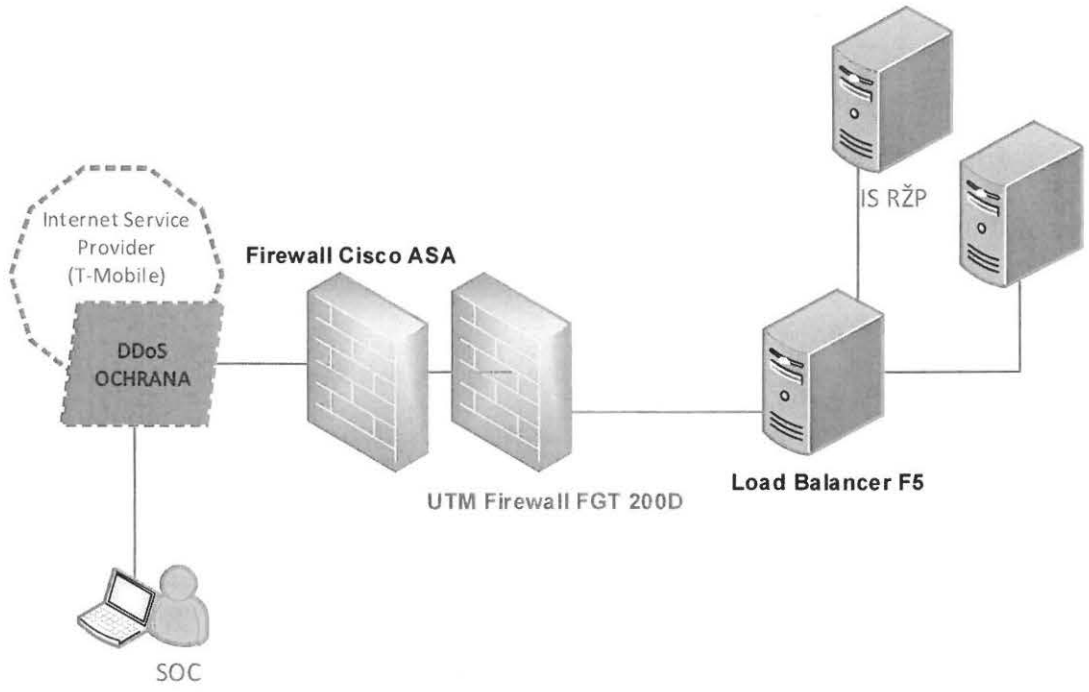
		Zadavateli předány jako výstup implementační fáze Služby 2.
S2/02	Popis architektury zapojení nástrojů Služby 2 v kontextu exitující architektury IS RŽP.	Dodavatel navrhne **popis architektury nástrojů Služby 2** a zapojení nástrojů do IS RŽP a projedná v rámci projektového týmu pro Službu 2, je písemným výstupem implementační fáze Služby 2.
S2/03	Definovaní bezpečnostních událostí sledovaných nástroji Služby 2 a míst detekce událostí. Definovaní pravidelných reportů pro Manažéra kybernetické bezpečnosti Zadavatele apod. Definice opatření pro filtrování přenášených dat.	Dodavatel navrhne a projedná v projektovém týmu Služby 2 **seznam bezpečnostních událostí (provoz), které budou blokovány nástroji Služby 2**. Tento seznam je písemným výstupem implementační fáze Služby 1.
S2/04	Definování úkolů a instrukcí pro SOC. (Procesní postupy, komunikační matice, eskalační procedury, atd.)	Dodavatel navrhne **instrukci pro personál SOC** a projedná v projektovém týmu Služby 2, tak by se naplnili požadavky Zadavatele na způsob komunikace s Manažerem kybernetické bezpečnosti, hlášení bezpečnostních události apod.
S2/05	Implementace nástrojů Služby 2	Dodavatel zahájí instalaci HW a SW do prostředí IS RŽP. Dodavatel připojí v této činnosti nástroj k prvkům IS RŽP. Účast zástupců dodavatelů IS ŘŽP v projektovém týmu Služby 2 je pro stanovení správného postupu nasazení nástroje silně doporučena. Přesný harmonogram a postup nasazení a postup bude projednán v projektovém týmu Služby 2. Konečný harmonogram a postup instalace nástroje schválí Zadavatel po projednání v projektovém týmu Služby 2.
S2/06	Testování provozních parametrů a kompatibility nástrojů Služby 2 a IS RŽP.	Dodavatel a provozovatelé IS RŽP provedou hodnocení nasazeného nástroje v rámci projektového týmu Služby 2, zda jsou ovlivněny kritické a provozní parametry IS RŽP. Dodavatel nástroje provede úpravy v parametrizaci nástroje, tak aby nebyl významně ovlivněn provoz IS RŽP.
S2/07	Testovací provoz 1 fáze.	Dodavatel provede nastavení nástrojů Služby 2 a zahájí blokaci bezpečnostních událostí/provozu. Dodavatel nástroje a dodavatelé IS RŽP v rámci projektového týmu Služby 2 vyhodnotí min. po 2 týdnech provozu, zda jsou ovlivněny kritické a provozní parametry IS RŽP.
S2/08	Školení personálu SOC a Manažera kybernetické bezpečnosti.	Dodavatel provede školení obsluhy nástroje a uživatele nástroje. **Záznam o školení** je písemným výstupem
S2/09	Testovací provoz 2 fáze.	Dodavatel provede nastavení nástrojů Služby 2 a doplní nastavení nástroje o další definované bezpečnostní události/provoz. Dodavatel nástrojů a dodavatelé IS RŽP v rámci projektového týmu Služby 2 vyhodnotí min. po 2 týdnech provozu, zda jsou ovlivněny kritické a provozní parametry IS RŽP. Dodavatel nástrojů provede úpravy v parametrizaci nástrojů, tak aby nebyl významně ovlivněn provoz IS RŽP.
S2/10	Testovací provoz 3 fáze. Ukončení	Dodavatel provede závěrečné nastavení

	testování.	nástrojů Služby 2. Dodavatel nástroje a dodavatelé IS RŽP v rámci projektového týmu Služby 2 vyhodnotí min. po 2 týdnech provozu, zda jsou ovlivněny kritické a provozní parametry IS RŽP. Dodavatel nástrojů Služby 2 provede úpravy v parametrizaci nástrojů, tak aby nebyl významně ovlivněn provoz IS RŽP. Testovací provoz je ukončen a změny lze provádět jen dle Postupu aktualizace sledovaných bezpečnostních událostí a nástroje.
S2/11	Akceptace Služby 2 Zadavatelem	Zástupce Zadavatele provede formální akceptaci provozu nástrojů Služby 3. **Akceptační protokol o provozu Služby 2** je písemným výstupem implementační fáze Služby 2.
S2/12	Definování postupu aktualizace nástrojů Služby 2 do maximální disponibilní kapacity nástroje. Stanovení schvalovacího postupu pro změny v souvislosti s nástroji Služby 2	Dodavatel navrhne **Postup aktualizace sledovaných bezpečnostních událostí a nástrojů** a tento návrh projedná v projektovém týmu pro Službu 2. Tento postup je písemným výstupem implementační fáze Služby 2. Dodavatel stanovuje max. disponibilní kapacity[2] nástrojů Služby 2 pro vyžití Zadavatelem takto: • **DDoS Ochrana, CCTP je max. 200 Mb/s** • **UTM Firewall FGT 200D, Výkon IPS sondy max. 1,7 Gb/s** Tyto technické parametry tvoří hranice, které nelze při rozšiřování nástrojů Služby 2 překročit.
S2/13	Akceptace písemných výstupů za Službu 2 Zadavatelem.	Zástupce Zadavatele provede formální akceptaci všech písemných výstupů za Službu 2. Písemné výstupy jsou v této tabulce vyznačeny **tlustě**.
S2/14	Ukončení Řízení implementace Služby 2.	Projekty tým pro Službu 2 ukončí svou činnost a předá agendu personálu SOC.
Služba 2 je dále poskytována dle parametrů definovaných v implementační fázi.		Služba 2 již dále není řízena a poskytována dle projektových zásad definovaných v kap. 3.2 Služba je dále řízena a poskytovaná dle procesní dokumentace (písemných výstupy implementační fáze Služby 2) definované a vytvořené v implementační fáze Služby 2.
PROVOZNÍ FÁZE SLUŽBY		
S2/15	Personál vykonává dohled nad všemi nástroji Služby 2. Personál SOC vykonává činnosti dle postupů (písemné výstupy) definovaných v implementační fázi Služby 2. Služba 2 je poskytována v rozsahu	Služba 2 je poskytována v rozsahu popsaném v této nabídce, smlouvě a dokumentech připravených v implementační fáze Služby 2 (viz výše).

[2] Disponibilní výkon nástroje je množství prostředků/kapacita nástroje, které má Zadavatel max. k dispozici pro čerpání za sjednanou cenu. Je to rámec výkonu nástroje snížený o výkon již sledovaného provozu apod. Překročení disponibilního výkonu není buď technicky možné, nebo za stávající sjednanou cenu nelze výší výkon nástroje požadovat.

	definovaném v implementační fázi.	
S2/16	Aktualizace parametrů nástrojů Služby 2 se provádí dle pravidel definovaných v implementační fázi Služby 2.	Jakékoli změny v souvislosti s nástrojem již je možné provádět jen dle **Postupu aktualizace sledovaných bezpečnostních událostí a nástrojů,** který byl připraven v implementační fáze Služby 2.

3.5.3. Přehledová architektura zapojeni nástrojů Služby 2



Obr.: Přehledová architektura zapojení nástrojů Služby 2

3.5.4. Nástroj pro ochranu integrity komunikačních sítí- DDoS Ochrana

DDoS je nástroj Služby 2 – DDoS ochrana - Operátorské řešení – Distribuované DoS útoky (DDoS) jsou jednou z nejzávažnějších hrozeb, jimž může čelit i IS RŽP. Závažnost a četnost těchto útoků je vysoká a ohrožení jsou vystaveny všechny druhy společností.

Pro zvýšení úrovně zabezpečení infrastruktury IS RŽP by bylo vhodné se zaměřit na její ochranu před útoky na známé zranitelnosti a doplnit ji o komplexní ochranu na aplikační i datové vrstvě (tzv. zařízení typu UTM) a o ochranu přístupové linky před DDoS útoky.

Ochranu vlastní aplikace před útoky na známé zranitelnosti, exploity apod. je nejvhodnější řešit pomocí patch managementu. Zároveň na ochranu proti neznámým tzv. „Zero-day" útokům na aplikační vrstvě nasadit dedikované zařízení zahrnující IPS a další sofistikované ochranné techniky.

K zajištění ochrany přístupových linek před DDoS útoky z internetu doporučujeme využít operátorské řešení DDoS ochrana.

Vlastnosti nástroje DDoS ochrana:

- Proaktivní kontrola a spolehlivá podpora (24 hodin denně, 7 dní v týdnu) zajišťující maximální funkčnost
- Nepřetržitá ochrana

- Odhalování různých druhů útoků v reálném čase
- Vysoká úroveň služeb zaručující včasné upozornění SOC a nejvyšší snížení rizik
- Využití specializovaných zdrojů, které čerpají z bohatých zkušeností se síťovou ochranou proti DDoS útokům
- SOC zajišťující hloubkovou kontrolu paketů
- Speciální portál pro sledování on-line zpráv a analýz

3.5.5. Nástroj pro ochranu integrity komunikačních sítí- UTM Firewall FGT 200D

UTM Firewall FGT 200D je nástroj Služby 2 – UTM (Unified Threat Management) zařízení poskytuje ochrany IPS (obecné i pro konkrétní aplikace a situace psané signatury), DLP, Application Control, AntiBOT, řízení obsahu (web content filtering) AV a AS kontroly a další ochranné funkcionality proti útokům z prostředí Internetu.

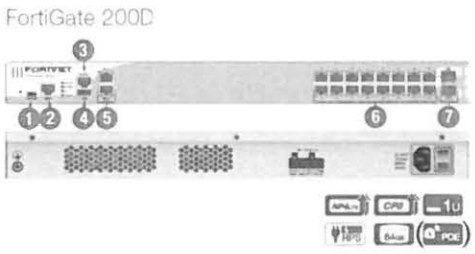
UTM zařízení chrání vnitřní síť před útoky pomocí známých i neznámých škodlivých kódů typu spyware, malware, botnety, VoIP hrozby, apod.
Kombinuje několik stupňů detekce narušení od rozpoznání útoků na základě signatur přes pravidla chování, anomálií provozu, rozpoznání aplikací a „Zero Day Attack" ochran. Poskytuje snadný přechod z detekce na prevenci, precizně a rychle blokuje hrozby bez zastavení legitimního provozu čímž šetří celkové náklady na provoz, ochranu a obnovu systémů.

Dále poskytuje v přehledné grafické formě informace o okamžitém stavu datových toků, jejich případných anomáliích a zastavených či aktuálních hrozbách. Tyto informace lze získat i zpětně za vybraná období ve formě tabulek i grafů.

Z pohledu síťové topologie je vhodné začlenit UTM zařízení mezi firewall Cisco ASA a LoadBalancery F5.

Vlastnosti nástroje UTM Firewall FGT 200D:

Navržené řešení je postaveno na 2 kusech hardwaru Next-Gen Firewalls (NGFW) - FortiGate-200D zapojených do HA Clusteru. Paketová propustnost zařízení je 3 Gbps (1518 Bytes/ 512 Bytes/ 64 Bytes), IPS propustnost 1,7 Gbps. Kapacita přístupových internetových linek IS RŽP je 100 Mbps. Navržená výkonnost bere ohled i na další parametry síťové výkonnost jako jsou konkurenční spojení, či potřeba nově otevíraných souběžných spojení v čase, stejně jako otázku zachování investic i v případě navýšení kapacit v budoucí době.



1. USB Management Port
2. Management Port
3. Console Port
4. USB Port
5. 2 x 10/100/1000 WAN Rozhraní
6. 16 x 10/100/1000 LAN Rozhraní
7. 2 x GbE SFP DMZ Rozhraní

3.5.6. Harmonogram implementace Služby 2

	Činnosti v časové souslednosti	TÝDEN (OD PODPISU SMLOUVY) 1 2 3 4 5 6 7 8 9 # # # # # # # # #
S2/01	Zahájení Řízení implementace Služby 2.	
S2/02	Popis architektury zapojení nástrojů Služby 2 v kontextu exitující architektury IS RŽP.	
S2/03	Definovaní bezpečnostních událostí sledovaných nástroji Služby 2 a míst detekce událostí. Definovaní pravidelných reportů pro Manažéra kybernetické bezpečnosti Zadavatele apod.	
S2/04	Definování úkolů a instrukcí pro SOC. (Procesní postupy, komunikační matice, eskalační procedury, atd.)	
S2/05	Implementace nástrojů Služby 2	
S2/06	Testování provozních parametrů a kompatibility nástrojů Služby 2 a IS RŽP.	
S2/07	Testovací provoz 1 fáze.	
S2/08	Školení personálu SOC a Manažera kybernetické bezpečnosti.	
S2/09	Testovací provoz 2 fáze.	
S2/10	Testovací provoz 3 fáze. Ukončení testování.	
S2/11	Akceptace Služby 2 Zadavatelem	
S2/12	Definování postupu aktualizace nástrojů Služby 2 do maximální disponibilní kapacity nástroje. Stanovení schvalovacího postupu pro změny v souvislosti s nástroji Služby 2	
S2/13	Akceptace písemných výstupů za Službu 2 Zadavatelem.	
S2/14	Ukončení Řízení implementace Služby 2.	
S2/15	Personál vykonává dohled nad všemi nástroji Služby 2. Personál SOC vykonává činnosti dle postupů (písemné výstupy) definovaných v implementační fázi Služby 2. Služba 2 je poskytována v rozsahu definovaném v implementační fázi.	
S2/16	Aktualizace parametrů nástrojů Služby 2 se provádí dle pravidel definovaných v implementační fázi Služby 2.	

4. Cenová nabídka

Název služby	Cena
Služba 1 – Detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí v IS RŽP (včetně služby SOC)	**345 000** Kč bez DPH /měsíčně
Služba 2 – Ochrana integrity komunikačních sítí IS RŽP (včetně služby SOC)	

5. Seznam konzultantů pro realizaci Služeb

Role v realizačním týmu	Jméno	Společnost
Vedoucí realizačního týmu	Karel Galuška, Ing.	T-Mobile Czech Republic
Projektová podpora	Michal Šťastný	T-Mobile Czech Republic
Manažer služeb	Jana Chrásková, Ing.	T-Mobile Czech Republic
Vedoucí konzultant	Miroslav Malířský	T-Mobile Czech Republic
Konzultant	František Kéri, Ing. EUR ING	T-Mobile Czech Republic
Konzultant	Miroslav Marcišin	T-Mobile Czech Republic
Konzultant	Milan Ryšavý, Ing.	T-Mobile Czech Republic
Konzultant	Marek Gemela, Ing.	T-Mobile Czech Republic
Konzultant	Josef Bartoš, Ing.	T-Mobile Czech Republic
Konzultant	Josef Pinc	T-Mobile Czech Republic

V případě požadavku zadavatele uchazeč zašle životopisy členů realizačního týmu.

6. Reference

Významné služby společnosti
T-Mobile Czech Republic a.s.

Zadavatel (Objednatel)	Název	Ministerstvo pro místní rozvoj	
	Sídlo	Staroměstské nám. 6, 110 15 Praha 1	
	IČ	66 00 22 22	
	Odpovědná osoba, která osvědčení vystavila	Jméno, funkce	RNDr. Blanka Fischerová, ředitelka Odboru správy monitorovacího systému
		Tel.	+ 420 224 861 412
		e-mail	blanka.fischerova@mmr.cz
Název Významné služby	Zajištění služby Bezpečnostního dohledu pro MS 2014+		
Popis poskytovaných služeb	Služba Bezpečnostního dohledu pro MS2014+ je souborem komplexních služeb bezpečnosti, které jsou poskytovány po dobu min. 4 let: 1) Služba BS01 – Informační bezpečnost – služba souvisí s řízením bezpečnosti informací v souladu se zásadami pro Systém řízení bezpečnosti informací (ISMS) dle normy ISO/IEC 27001. Služba obsahuje zavedení procesů, zásad, politik a metodik ISMS do prostředí systému MS2014+ pro administraci dotačních programů EU. Současně zavádí řízení bezpečnostních incidentů a dalších procesů vyžadovaných ISMS. 2) Služba BS02 – Ochrana osobních údajů – služba zajišťuje ochranu osobních údajů v souladu s požadavky zákona 101/2000 Sb. 3) Služba BS03 – Bezpečnostní monitoring – služba aktivně monitoruje a vyhodnocuje prostředí a Aplikaci MS2014+ z hlediska bezpečnost. Služba aktivně vyhledává slabá místa a zranitelnosti a následně jsou tyto nálezy vnitřním procesem řízeně odstraňovaný. 4) Služba BS04 – Kontrola kvality poskytovaných služeb – služba vyhodnocuje kvalitu služeb poskytovaných dodavateli a všech subjektů podílejících se na realizaci, provozu, správě a podpoře Aplikace MS2014+. Byla vyhotovena metodika řízení kvality pro definici ukazovatelů kvality apod. 5) Služba BS05 – Audit prostředí – Služba zajišťuje v prostředí a Aplikaci MS2014+ veškeré činnosti související s:		

	a. Kontrolou bezpečnosti b. Penetrační testy c. Audit prostředí. Služba poskytuje podporu Objednatele při certifikačních auditech a kontrolách třetích stran.	
Doba realizace Významné služby	Zahájení	07/2015
	Ukončení	doposud

Zadavatel (Objednatel)	Název	Ministerstvo pro místní rozvoj	
	Sídlo	Staroměstské nám. 6, 110 15 Praha 1	
	IČ	66 00 22 22	
	Odpovědná osoba, která osvědčení vystavila	Jméno, funkce	Renata Entová, Vedoucí oddělení Koncepce informačních technologií
		Tel.	+420 224 861 270
		e-mail	Renata.Entova@mmr.cz
Název Významné služby	Diferenční analýza prostředí Zadavatele k požadavkům Zákona o kybernetické bezpečnosti České republiky 181/2014 Sb.		
Popis poskytovaných služeb	Je provedena diferenční analýza prostředí Zadavatele vůči požadavkům Zákona o kybernetické bezpečnosti. Výstupem služby je dokument, který popisuje současný stav, hodnotí soulad s požadavky Zákona, případně identifikuje soulad s „best practice" a popisuje doporučená nápravná opatření.		
Doba realizace Významné služby	Zahájení	10/2015	
	Ukončení	doposud	

Zadavatel (Objednatel)	Název	Energetický Regulační Úřad	
	Sídlo	Masarykovo náměstí 5, 586 01 Jihlava	
	IČ	70894451	
	Odpovědná osoba, která osvědčení vystavila	Jméno, funkce	Richard Tesař
		Tel.	+420 564 578 697
		e-mail	richard.tesar@eru.cz
Název Významné služby	Diferenční analýza prostředí Zadavatele k požadavkům		

	Zákona o kybernetické bezpečnosti České republiky 181/2014 Sb.	
Popis poskytovaných služeb	Byla provedena diferenční analýza prostředí Zadavatele vůči požadavkům Zákona o kybernetické bezpečnosti. Výstupem služby je dokument, který popisuje současný stav, hodnotí soulad s požadavky Zákona, případně identifikuje soulad s „best practice" a popisuje doporučená nápravná opatření.	
Doba realizace Významné služby	Zahájení	06/2015
	Ukončení	09/2015

Zadavatel (Objednatel)	Název	T-Systems Belgium N.V.	
	Sídlo	't Hofveld 8 Groot-Bijgaarden 1702	
	IČ	8108	
	Odpovědná osoba, která osvědčení vystavila	Jméno, funkce	Martin David Senior Information Security Manager TESTA-ng - Public Sector & Healthcare
		Tel.	+32 2 300 91 63 ext 9163 (phone) +44 (0) 7595541397 (mobile)
		e-mail	David.Martin@external.t-systems.com
Název Významné služby	Zpracování analýzy a implementace v oblasti bezpečnosti		
Popis poskytovaných služeb	Služby spočívající v zajištění komplexní analýzy a mapování procesů fyzické, personální, administrativní a informační bezpečnosti, dále kybernetické bezpečnosti, ochrany osobních a citlivých údajů, bezpečnosti informačních a komunikačních systémů a informačních systémů infrastruktury. Součástí předmětu plnění je posouzení, resp. analýza stávající struktury zajištění a řízení bezpečnosti Objednatele a její soulad s platnou legislativou, normami, nejlepšími zkušenostmi, současnými technologickými trendy. Součástí předmětu plnění je rovněž implementační část navržených řešení bezpečností politiky pro Objednatele v rámci poskytovaných služeb pro Evropskou komisy.		
Doba realizace Významné služby	Zahájení	02/2014	
	Ukončení	Dosud	

Zadavatel (Objednatel)	Název	T-Systems Belgium N.V.	
	Sídlo	't Hofveld 8 Groot-Bijgaarden 1702	
	IČ	8108	
	Údaj o objednateli	Komerční společnost	
	Odpovědná osoba, která osvědčení vystavila	Jméno, funkce	Michal Kováč ICT OPERATIONS SECURITY
		Tel.	+32 491 166 662
		e-mail	M.Kovac@t-systems.com
Název Významné služby	Řízení kontinuity činností		
Popis poskytovaných služeb	Služby spočívající v řízení kontinuity činností jak je požadováno ISO/IEC 27001. Předmět plnění spočívá v poskytnutí služby dle mezinárodně uznávaného standardu v oblasti návrhu systému řízení kontinuity činností (ČSN ISO 22301) nebo kontinuity služeb (ISO 20000), přičemž služba je poskytnuta pro informační systém a jeho provoz pro společnost British American Tobacco p.l.c. Součástí služby je návrh detailních havarijních plánů, přičemž lze doložit, že uchazečem navržené havarijní plány prošly úspěšnou implementací a testováním. Součástí služby byla úspěšná implementace a testování havarijních plánů.		
Doba realizace Významné služby	Zahájení	03/2013	
	Ukončení	12/2014	

7. Obchodní ujednání

Na smlouvu, kterou s Vámi T-Mobile případně uzavře ohledně předmětu této nabídky, a to i v případě, kdy Vaše společnost nabídku T-Mobile akceptuje s odkazem na obchodní podmínky odlišné se ustanovení § 1751 odst. 2 občanského zákoníku neuplatní. Pokud by však ustanovení předchozí věty bylo posouzeno jako neplatné, tak v případě, kdy smluvní strany se odkážou v nabídce na uzavření smlouvy a přijetí nabídky na obchodní podmínky, které si odporují, není smlouva uzavřena.

Uzavření smlouvy na plnění je ze strany T-Mobile vázáno na interní odsouhlasení pověřenými osobami v T-Mobile, které se nezúčastnily vyjednávání o podmínkách návrhu Smlouvy, a proto si T-Mobile vyhrazuje právo smlouvu neuzavřít, a to v kterékoli fázi jednání, zejména pokud nebudou získána potřebná interní schválení, přičemž smluvní strany nepovažují uplatnění tohoto práva ze strany T-Mobile za nepoctivé. Důvody neuzavření Smlouvy nebo neuskutečnění transakce není T-Mobile povinen Vaší společnosti sdělit.

8. Závěr

Jménem společnosti T-Mobile Vám děkujeme za čas a energii, kterou jste věnovali studiu naší nabídky. Věříme, že vás zaujala a jsme připraveni na následné osobní setkání, na kterém můžeme projednat případné úpravy navrhovaného řešení tak, aby co nejvíce vyhovovalo potřebám Ministerstva průmyslu a obchodu

Příloha č. 2.

Cenová aktualizace služeb hostingového centra IS RŽP

T-Mobile

Nabídka cenové aktualizace služeb hostingového centra IS RŽP pro:

Ministerstvo průmyslu a obchodu

Dodavatel nabídky: T-Mobile Czech Republic a.s. Tomíčkova 2144/1 148 00 Praha 4 IČ: 649 49 681 DIČ: CZ64949681	Spisová značka B, vložka 3787, společnost je zapsána v OR vedeným Městským soudem v Praze Bankovní spojení Komerční banka, a.s., Praha 2 Účet číslo 19-2271190247/0100 (dále jen „T-Mobile")

Úvodem

Vážení,

v návaznosti na výstupy z jednání Řídící komise informačního systému Registr živnostenského podnikání a v souvislosti s provedenou technologickou optimalizací, si Vám dovolujeme předložit návrh cenové aktualizace služeb hostingového centra dle smlouvy č. MPO 05/04400/02.

V případě Vašeho zájmu bychom s Vámi rádi, na příštím jednání Řídící komise informačního systému Registr živnostenského podnikání, projednali další postup.

Nabídka služeb T-Mobile je určena pro:	
Zadavatel	Ministerstvo průmyslu a obchodu
Ulice, č. p./č. o.	Na Františku 32
PSČ 118 00	Praha 1
IČ:	47609109

Nabídku vypracoval:

Patrik Nikendey
Manažer prodeje klíčovým zákazníkům
T-Mobile Czech Republic a.s.
Adresa: Tomíčkova 2144/1, 149 00 Praha 4
Tel.: 720705183
E-mail: patrik.nikendey@t-mobile.cz

Za T-Mobile Czech Republic a.s. předkládá: Patrik Nikendey

Nabídka byla vypracována dne 4. 3. 2016 a její platnost je omezena do 30. 6. 2016.

Cenová nabídka

Dovolujeme si Vám předložit nabídku na snížení cen měsíčních paušálních plateb za poskytování služeb hostingového centra informačního systému Registr živnostenského podnikání.

Pro přehlednost uvádíme původní i nově navrhované ceny, všechny částky jsou uvedeny bez DPH.

Služba	**Cena**
TSS linky RŽP	stávající cena 530 352 Kč měsíčně
TSS linky RŽP	nová cena 477 317 Kč měsíčně
TSS linky RŽP	měsíční sleva 53 035 Kč
CSS hosting RŽP	stávající cena 2 927 746 Kč měsíčně
CSS hosting RŽP	nová cena 2 635 781 Kč měsíčně
CSS hosting RŽP	měsíční sleva 291 965 Kč
Původní měsíční cena celkem	3 458 098 Kč
Nová měsíční cena celkem	3 113 098 Kč
Celková měsíční sleva	**345 000 Kč**

Příloha č. 3

Pověření Ing. Libora Komárka a Ing. Miroslava Kláska