KATALOGOVÝ LIST KYBE_SP/006	
Název služby:	**Poskytování Služeb kybernetické bezpečnosti**

1 Období poskytování služby

Služba je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby.

Název milníku	Termín splnění milníku
Zahájení poskytování služby	20.3.2019
Zahájení poskytování služby v rozsahu odst. 3.4	1.12.2020
Ukončení poskytování služby	20. 3. 2023

Službu podpory provozu dle tohoto Katalogového listu lze v souladu s odst. 5.2 a odst. 22.7 Smlouvy vypovědět samostatně.

2 Režim poskytování služby

Jednotlivé části služby podle tohoto Katalogového listu budou poskytovány takto:

Část Služby	Doba poskytování
Bezpečnostní monitoring	24x7
Podpora provozu IISSP pro Služby dle Katalogových listů části D přílohy č. 1 této Smlouvy v oblasti kybernetické bezpečnosti	8-16 v pracovní dny
Analýza rizik	1 x ročně
Podpora bezpečnostních produktů SAP	24x7 nebo v době dle jednotlivých činností

3 Popis rozsahu služby

Obsahem Služby podle tohoto Katalogového listu je zajištění kybernetické bezpečnosti pro IISSP. Komplexní služba se dělí na následující oblasti:

3.1 Bezpečnostní monitoring

3.1.1 Popis služby

Předmětem Služby je nepřetržitý bezpečnostní monitoring v režimu 24x7 (dále jen „Služba") aktiv objednatele. Bezpečnostní monitoring je prováděn dohledovým pracovištěm a expertním týmem OCKB – SOC SPCSS. Součástí bezpečnostního monitoringu je detekce kybernetických bezpečnostních událostí (dále jen „KBU") pomocí nástroje SIEM, jejich vyhodnocování a zvládání, dokumentování kybernetických bezpečnostních incidentů (dále jen „KBI"), jejich analýza a návrhy na opatření. V rámci služby je poskytován incident management včetně přípravy podkladů pro příslušné orgány v souladu se zákonem

č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění a podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, případně na základě dohody smluvních stran.

Součástí dodávky Služby Bezpečnostní monitoring jsou:

- proces zvládání KBU, KBI (incident management)
- detekce, sběr, uchovávání a vyhodnocování kybernetických bezpečnostních událostí a incidentů, monitoring databází a aplikací;
- zpracování Zprávy o stavu Služby určené objednateli (předávána v měsíčním intervalu);
- ukládání security logů minimálně po dobu definovanou ZoKB.

Pravidelným měsíčním výstupem Služby je zpracování dokumentů Zpráva o stavu bezpečnosti a Zpráva o úrovni a rozsahu Služby, které jsou základem pro průběžné zlepšování Služby v přirozeně proměnlivém bezpečnostním prostředí. Zpráva o stavu bezpečnosti obsahuje řešení a stav BH, KBU, KBI za uplynulé období a návrhy na nápravná opatření. Zpráva o úrovni a rozsahu Služby obsahuje plnění parametrů SLA. Tyto zprávy budou zahrnuty v měsíčních zprávách Služby.

3.1.1.1 Procesy zvládání KBU, KBI

Procesy zvládání KBU, KBI:

- provedení klasifikace KBU, KBI;
- zabezpečení procesu zvládání BH, KBU, KBI;
- zpracování návrhu na realizaci opatření formou definice zadání pro požadavky na změnu (RFC)
- zpracování dokumentace KBU a KBI včetně uchovávání relevantních dat v SIEM nástroji (logů, událostí, „offense"), vedení záznamů v SD o průběhu řešení, zavedení a aktualizace znalostní báze v SD;
- zpracování Zprávy o stavu bezpečnosti a Zprávy o stavu služby (předávána v měsíčním intervalu);
- iniciace bezpečnostních varování a opatření včasné reakce v případech velmi závažných a závažných KBI;
- příprava podkladů pro příslušné orgány v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění a podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, případně na základě dohody smluvních stran.

3.1.1.2 Detekce, sběr, uchovávání a vyhodnocování logů, KBU a KBI

Soubor aktivit a procesů v oblastech monitoringu a detekce, jejich vyhodnocování a zvládání, dokumentování BH, KBU a KBI, jejich analýzy a návrhů na zlepšování bezpečnosti IS ve správě objednatele.

Monitoring a detekce KBU a KBI v režimu 24x7 je zajištěna dohledovým pracovištěm SPCSS, SIEM nástrojem, expertním týmem CKB-SOC a bezpečným úložištěm zdrojových dat. SIEM nástroj v reálném čase monitoruje a vyhodnocuje probíhající události na sledovaných aktivech a na základě implementovaných pravidel automaticky sestavuje bezpečnostní výstrahy, které nesou informace o narušení bezpečnostního stavu. Tato funkcionalita je zajištěna sběrem událostí v nástroji SIEM z vybraných zdrojů logů, které jsou definovány na základě podkladů od objednatele, resp. na základě analýzy rizik. Tím tato část Služby naplňuje požadavky § 21 - § 23 VoKB.

Vyhodnocování a klasifikace KBU a KBI a určování adekvátních reakcí je prováděno, evidováno a vyhodnocováno v aplikaci Service Desk v souladu s § 24 - § 27 VoKB.

Nástroj Service Desk je jednotné prostředí pro řízení procesu Incident Management, evidenci, sledování řešení a vyhodnocování bezpečnostních hlášení, kybernetických bezpečnostních událostí a incidentů oznámených uživateli, bezpečnostními rolemi a Administrátory nebo detekovaných technickými prostředky. Service Desk je prostředím, které slouží jako podklad pro expertní tým CKB – SOC při zvládání kybernetických bezpečnostních událostí a incidentů definovanými procesy zvládání KBU a KBI a také pro řízení změn. Tím tato část Služby naplňuje povinnosti uložené v § 10 - § 11 VoKB.

Logy získané z monitorovaných systémů se uchovávají v úložišti systému SIEM po dobu minimálně 18 měsíců, dle § 22, odst. (3) VoKB. Archivace logů nad rámec § 22, odst. 3 VoKB, může být sjednána dohodou smluvních stran.

3.1.2 Komponenty tvořící službu

Níže uvedené komponenty služby jsou nedílnou součástí služby a není možné je ze služby vyjmout.

3.1.2.1 Uživatelská behaviorální analýza

Analýza chování uživatelů (UBA) analyzuje aktivitu uživatelů a zjišťuje, zda došlo ke zneužití pověření uživatele. UBA přidává kontext uživatele k síti, protokolu, zranitelnostem a ohrožení dat rychleji a přesněji detekuje útoky. Bezpečnostní analytici mohou snadno zobrazit rizikové uživatele, zobrazit jejich anomální aktivity a zkoumat konkrétní podkladové protokoly, logy a toky dat, která přispěla k hodnocení rizika uživatele.

3.1.2.2 Monitoring NetFlows

Hlavním účelem služby je monitorování síťového provozu na základě IP toků, které poskytuje podrobný pohled do provozu na síti v reálném čase. S pomocí NetFlow statistik lze odhalovat vnější i vnitřní incidenty, úzká místa v síti, dominantní zdroje provozu, efektivněji plánovat budoucí rozvoj sítě, sledovat, kdo komunikoval s kým, jak dlouho a s pomocí kterého protokolu.

3.1.3 Knowledge Base pro zvládání KBU/KBI

Knowledge Base pro oblast kybernetické bezpečnosti je součástí aplikace Service Desk, která obsahuje základní problémy a situace. Obsah Knowledge Base je aktualizován a rozšiřován o řešené situace včetně Best Practices pro jejich řešení.

3.1.4 Výstupy a akceptace poskytované služby

Pravidelným měsíčním výstupem Služby je zpracování dokumentů Zpráva o stavu bezpečnosti a Zpráva o úrovni a rozsahu Služby, které jsou základem pro průběžné zlepšování Služby v přirozeně proměnlivém bezpečnostním prostředí. Zpráva o stavu bezpečnosti obsahuje řešení a stav BH, KBU, KBI za uplynulé období a návrhy na nápravná opatření.

3.2 Analýza rizik

3.2.1 Popis služby

Služba analýzy rizik spočívá v provádění aktualizací vstupní analýzy rizik v pravidelných intervalech (minimálně 1x ročně nebo při zásadní změně systému) dle zvolené metodiky a s využitím příslušných nástrojů. U takto analyzovaných rizik lze následně sjednat i jejich správu. Součástí služby je pravidelná roční aktualizace analýzy rizik. Analýza rizik prováděná na základě zásadní změny systému není součástí této služby a její realizace bude vykonána na základě dohody smluvních stran.

Obsahem Služby je identifikace a ohodnocení aktiv a rizik pro dosažení souladu prvků KII s požadavky ZoKB.

Součástí dodávky Služby jsou:

- Interview s garanty primárních aktiv a jejich ohodnocení.
- Interview s garanty podpůrných aktiv a jejich ohodnocení.
- Doplnění vazeb mezi podpůrnými a primárními aktivy.
- Upřesnění hrozeb a zranitelností na příslušná podpůrná aktiva.
- Vypracování výstupní dokumentace dle ZoKB (Zpráva o hodnocení aktiv a rizik, Plán zvládání rizik, Prohlášení o aplikovatelnosti).

3.2.2 Proces realizace analýzy rizik

Podrobný popis služby Analýza rizik bude definován jako výstup první fáze Interview, kdy součástí bude určení primárních a podpůrných aktiv v souladu se ZoKB a ISO 27 000. Součástí realizace je Interview s garanty podpůrných aktiv (s rozpadem na nejnižší možný stupeň – IP adresu), včetně fyzického umístění. Výstupem budou dokumenty dle ZoKB.

3.2.2.1 Interview

Jedná se o konzultaci na bázi řízeného rozhovoru, jejíž první část se zaměřuje na identifikování rozsahu služeb a stanovení primárních aktiv (zpravidla služby nebo informace), a zároveň i jejich ohodnocení (důležitost daného aktiva a také jeho důvěrnost, dostupnost a integrita). Druhým důležitým výstupem je identifikování garantů podpůrných aktiv.

Druhá část interview se poté zaměřuje na garanty podpůrných aktiv, s nimiž je veden rozhovor na podobné bázi, jako s garanty primárních aktiv. Cílem je jasný přehled všech podpůrných aktiv (a jejich rozpad až na úroveň IP adresy a jejich fyzického umístění) a ohodnocení z hlediska váhy vlivu na primární aktivum, které je daným podpůrných aktivem ovlivňováno (hodnotí se z hlediska váhy na dostupnost, důvěrnost a integritu primárního aktiva).

Ve třetí fázi se provádí úprava a upřesnění předpřipraveného seznamu hrozeb a zranitelností.

3.2.2.2 Zpracování výstupní dokumentace

Výstupem Služby je zpracovaná dokumentace dle ZoKB, konkrétně se jedná o:

a) Zpráva o hodnocení aktiv a rizik,
b) Plán zvládání rizik,
c) Prohlášení o aplikovatelnosti.

Akceptace výstupní dokumentace probíhá formou akceptačního protokolu.

3.3 Ostatní činnosti v oblasti kybernetické bezpečnosti

Poskytovatel bude vykonávat činnosti v oblasti bezpečnosti pro zajištění řídících a provozních procesů podpory provozu IISSP v souladu s Přílohou č. 1 Část A a Část B.

Rovněž bude Poskytovatel na základě odst. 3.2 a dle postupu stanoveného v odst. 6.1 až 6.7 Smlouvy, poskytovat ostatní činnosti v oblasti kybernetické bezpečnosti, a to zejména:

- příprava a realizace zátěžového a penetračního testování,
- návrh a realizace opatření na základě výstupů analýzy, postupů správy a řízení rizik,
- zpracování návrhu, dopadů a analýz v oblasti bezpečnosti,
- návrh a realizace vzdělávání uživatelů formou e-learning na základě doporučení analýzy rizik nebo v oblasti bezpečnosti,
- analýza procesů a implementace vybraných bezpečnostních nástrojů v prostředí IISSP pro zajištění služeb podpory provozu a pro realizaci bezpečnostních opatření,
- návrh, konfigurace a správa bezpečnostních prvků,
- analýza, návrh, aktualizace a vytvoření vybrané dokumentace IISSP,
- související konzultace v oblasti kybernetické bezpečnosti při změně architektury a úpravách IISSP,
- konzultace, návrh, aktualizace uživatelských a správních procesů a případů užití,
- konzultace v oblasti architektury IISSP v návaznosti na předpisy v oblasti bezpečnosti,
- příprava a realizace požadovaného prostředí pro výkon bezpečnostních doporučení,
- dočasné bezpečné ukládání dat nebo logů sloužící k ověření či bezpečnostnímu auditu IISSP,
- ostatní související konzultace a zpracování odborných analýz v oblasti bezpečnosti.

3.4 Podpora bezpečnostních produktů SAP

3.4.1 Činnosti tvořící službu

Tabulka 1 - Činnosti tvořící službu Podpora bezpečnostní produktů SAP

Oblast či produkt SAP / Činnost	Četnost	Odpovědnost *	
		MF	Poskytovatel
Podpora bezpečnostních produktů SAP			
ETD			
Monitoring stavu (první dvě dlaždice ze sekce Monitoring) a verifikace bezproblémového průběhu monitorování	Průběžně	O	S
Kontrola a validace výstupu Monitoringu stavu a verifikace bezproblémového průběhu monitorování	Průběžně, minimálně 1x týdně	S	O
Řešení problémů při sběru a zpracování logů (Dlaždice Monitoring -> Pattern Executions Last 24 Hours – pokud v sekci failed bude číslo větší než nula)	Průběžně	S	P
Record of Actions – kontrola provedených akcí	Průběžně na měsíční bázi	O	S
Kontrola a validace Record of Actions	Průběžně, minimálně 1x měsíčně	S	O
Zpracování vzniklých upozornění (alerts), případně založení pátrání (investigations)	Průběžně	P	S
Zpracování a vykazovaní založených pátrání (investigations)	Průběžně na týdenní bázi	P	S
Kontrola výjimek Alerts and Investigations à Excemptions (odstranění neopodstatněných výjimek)	Průběžně na měsíční bázi	S	P
Kontrola a identifikace relevantních událostí v nerozpoznaných lozích (kontrola sekce Log Learning à Unrecognized Logs)	Průběžně na měsíční bázi	S	P
Kontrola detailů logů Alerts and Investigations -> Log Events, detailní analýza záznamu logu	Průběžně nebo dle potřeb provozu	S	P
Kontrola detailů logů Log Learning -> Sharelog, detailní analýza záznamu logu podle složitějších kritérií	Průběžně nebo dle potřeb provozu	S	P
Nastavení výjimek pro generování upozornění Alerts and Investigations -> Excemptions	Průběžně nebo dle potřeb provozu	S	P
Kontrola logů na neošetřený potenciální incident, doplnění pravidel pomocí Forensic Lab, případně Anomaly Detection Lab	Průběžně nebo dle potřeb provozu	S	P
Kontrola logů pro sledování landscape, doplnění pravidel pomocí Log Learning a provedení jeho normalizace	Průběžně nebo dle potřeb provozu	S	P

* O = Odpovědnost, S = Součinnost, P = Provádí a odpovídá za svěřené činnosti, poskytuje součinnost

4 Kvalitativní parametry poskytované Služby

4.1 SLA parametry

Poskytovatel je povinen poskytovat Služby kybernetické bezpečnosti dle Smlouvy pro produktivní prostředí IISSP v níže uvedených reakčních časech dle Tabulky č. 2.

Doba reakce úrovně L1 je počítána od zaevidování bezpečnostního hlášení/kybernetické bezpečnostní události/kybernetického bezpečnostního incidentu (BH/KBU/KBI) do aplikace Service Desk. Podpora L1 musí do doby uvedené v tabulce níže přijmout v aplikaci Service Desk BH/KBU/KBI k řešení.

Tabulka 2 - Reakční doby a doby odstranění incidentu

Název Služby:	**Služby kybernetické bezpečnosti**			
SLA parametry				
Služba	Maximální doba zahájení řešení incidentu v pracovní dny 7–19 hod.	Maximální doba zahájení řešení incidentu v mimopracovní dny a v době 19–7 hod.	Doba odstranění incidentu	Maintenance Window každý čtvrtek, vždy 19:00-24:00
Bezpečnostní monitoring	15 minut	30 minut	Po dohodě obou smluvních stran	

5 Smluvní pokuty

Smluvní pokuta za nedodržení stanovených SLA činí 500 Kč za každou minutu, o kterou se prodloužilo zahájení řešení incidentu nad stanovené hodnoty.

6 Požadovaná součinnost

6.1 Součinnost pro zajištění poskytování služby kybernetické bezpečnosti

Objednatel má povinnost spolupracovat s Poskytovatelem při kontrole rozsahu poskytnutých Služeb a informační podpory, zejména formou včasných vyjádření k výstupům Služby a její akceptaci.

Objednatel stanoví Poskytovateli kontaktní osoby včetně komunikační matice pro případ řešení kybernetických bezpečnostních událostí a incidentů (CIRT tým objednatele).

Objednatel stanoví Poskytovateli osoby do rolí, nezbytných pro dodání služby Analýza rizik, zejména příslušné Garanty aktiv.

V případě, že Objednatel využívá třetí strany pro správu, servis, podporu, konfiguraci apod. systému/ů monitorovaného/ných v rámci Služby, bude pro zjištění nebo řešení KBU/KBI zajištěna komunikační matice pro přímou komunikaci mezi Poskytovatelem a touto třetí stranou a to obousměrně. Komunikace bude na straně Poskytovatele zaznamenána a evidována v tiketech v systému Service Desk Poskytovatele. Objednatel bude o této komunikaci dostávat notifikace. Komunikace mezi třetí stranou a Poskytovatelem bude v režimu 24/7. V případě, že třetí strana zjistí KBU/KBI, bude primárně kontaktovat Service Desk Poskytovatele.

Poskytovatel zajistí přístup pro určené osoby Objednatele pro možnost náhledu pro řešení tiketů do systému Service Desk Poskytovatele. Při řešení BH/KBU/KBI je potřeba součinnost se členy CIRT týmu Objednatele.

6.2 Požadovaná součinnost při zpracování výstupů Služby

Objednatel bude spolupracovat s Poskytovatelem při vytváření výstupů služeb zejména:

- nominací kompetentních osob poskytujících součinnost při zpracování výstupů Služeb na straně Objednatele a jejich smluvních partnerů. Zejména se jedná o nominace bezpečnostních rolí a Garantů aktiv do realizačních týmů a stanovení jejich potřebných odpovědností a kompetencí s ohledem na poskytovanou Službu;
- zajištěním potřebné disponibility nominovaných členů realizačních týmů pro poskytnutí součinnosti s ohledem na odsouhlasené termíny;
- poskytnutím všech nezbytných podkladů týkající se obsahu zadaných výstupů Služby.

Poskytovatel prohlašuje, že je připraven v úzké součinnosti s Objednatelem a na základě jeho požadavků optimalizovat parametry poskytované Služby, podílet se na zlepšení celkové bezpečnosti informací v prostředí Objednatele (snížení nepříznivých dopadů na organizaci), zajišťování důkazních prostředků, poskytování vstupních dat pro úpravu politiky bezpečnosti informací a bezpečnostní dokumentace Objednatele.

7 Pojmy a zkratky

Tabulka 3 - Pojmy a zkratky

Zkratka	Význam
BH	Bezpečnostní hlášení – jedná se o hlášení zadané do aplikace Service Desk přímo koncovým uživatelem, který má podezření na KBU nebo KBI
BM	Bezpečnostní monitoring
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CKB	Centrum kybernetické bezpečnosti, organizační útvar SPCSS. Resortní kompetenční centrum poskytující Služby kybernetické bezpečnosti v souladu se ZoKB
CKB – SOC	Centrum kybernetické bezpečnosti – Středisko dohledu kybernetické bezpečnosti (Security Operation Center)
ETD	Enterprise Threat Detection (Detekce hrozeb SAP Enterprise)
KBI	§ 7 odst. 2 ZoKB: Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události
KBU	§ 7 odst. 1 ZoKB: Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo

Zkratka	Význam
	narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
KII	Kritická informační infrastruktura – prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy2) v oblasti kybernetické bezpečnosti
Knowledge Base pro zvládání KBU/KBI	Znalostní báze; součást aplikace Service Desk, která obsahuje popis základních problémů a situací. Obsah Knowledge Base je aktualizován a rozšiřován o řešené situace a Best Practices pro jejich řešení.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA cyklus	Metoda postupného zlepšování například kvality služeb, procesů, aplikací, dat, probíhající formou opakovaného provádění čtyř činností (plan-do-check-act, tedy naplánuj-proveď-ověř-jednej)
RFC	Změnový požadavek (Request for Change)
SIEM	Security Incident and Event Management
SOC	Security Operation Center, organizační část CKB SPCSS zaměřená na dohled bezpečnosti, vyhodnocování a řešení KBI
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti