# **Příloha č. 1**

# **Technická specifikace**

# **„Zajištění služby dohledového centra“**

# Předmět zakázky

Předmětem zakázky je komplexní zajištění služeb dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centrum) k zajištění dohledu a provozu nástrojů pro vyhodnocování kybernetických bezpečnostních událostí ve výpočetních systémech a v komunikačních sítích, které zadavatel využívá nebo provozuje.

V následujících podkapitolách uvádíme soubor všech požadavků na předmětné služby. Tyto požadavky představují kompletní a současně minimální úroveň, kterou musí poskytovatelé služby splnit.

# Předpokládaný harmonogram

Zadavatel požaduje od poskytovatele služby napojení do služby Security Operation Centra do 5 pracovních dnů od účinnosti smlouvy (den jejího uveřejnění dle zákona č.34/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv)při součinnosti zadavatele.

# Ostatní požadavky Zadavatele na plnění zakázky

Zadavatel neumožňuje využití subdodavatelů. Všichni účastníci projektu musí být zaměstnanci poskytovatele služby.

# Součinnost Zadavatele

Zadavatel pro účely poskytování služby zpřístupní poskytovateli služby:

* vlastní bezpečnostní dohledové systémy (Flowmon, SIEM, AddNet, Logmanagement) včetně umožnění potřebné základní konfigurace pro monitoring poskytovatelem služby. **Pozn.:** Zadavatel pro vyloučení všech pochybností uvádí, že ***samu schopnost zálohy a obnovy po výpadku svých systémů nebude hodnotit jako dostatečnou aplikaci opatření zajišťujících vysokou dostupnost služby.***
* propojení VPN typu Site-to-Site s úrovní šifrování, podle aktuálního nařízení NÚKIB.

# Technická specifikace

## Dohledové centrum kybernetické bezpečnosti (SOC)

Předmětem zakázky je komplexní zajištění služeb dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centrum), především:

* formou služby provozovat centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software, tj. nástroje (Flowmon, SIEM, AddNet a Logmanagement). Implementace systému bude provedena v souladu s *§23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.*
* formou služby provozovat centralizovanou správu, ukládání a vyhodnocování komunikačních spojení a výkonnostních parametrů datové sítě, tj. nástroj sběru a vyhodnocení NetFlow. Implementace systému bude provedena v souladu s *§22 Nástroj pro detekci kybernetických bezpečnostních událostí.*

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Poskytovatel služby je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků Zadavatele“ (poskytovatel služby doplní prohlášení ANO nebo NE podle skutečnosti včetně odkazu na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku).

|  |  |  |
| --- | --- | --- |
| **Minimální technické požadavky, které Zadavatel požaduje** | | **Splnění požadavků Zadavatele (ANO/NE)** |
|  | **Požadavky na služby SOC** |  |
| 1. | Zadavatel předpokládá realizaci uvedených úloh prostředky a technologiemi zadavatele, nejméně v rozsahu řešení sběru NetFlow, Addnet, SIEM a Logmanagement, které zadavatel již vlastní. Služba poskytovatele zohlední přítomnost těchto prostředků na straně zadavatele v tom smyslu, že jako primární a rozhodné nástroje dodavatel využije tyto prostředky a celý rozsah služby bude provádět jejich prostřednictvím. |  |
| 2. | Bezpečnostní dohledové centrum poskytovatele služby musí podporovat práci s nástroji zadavatele. |  |
| 3. | Poskytovatel služby navrhne modifikaci relevantních procesů na straně zadavatele, včetně atributů a parametrů procesů potřebných pro doručení služby.  Konfigurační změny a úpravy prostředků zadavatele nutných pro připojení k službě provede poskytovatel služby vlastním nákladem jako součást služby a předá je do vlastnictví zadavatele. |  |
| 4. | Poskytovatel služby navrhne modifikaci konfigurace SIEM řešení na straně zadavatele, včetně atributů a parametrů potřebných pro doručení služby. |  |
| 5. | Služba dostupná v českém jazyce. |  |
| 6. | Služba dohledu je zajišťována z území ČR. |  |
| 7. | V rámci služby bude poskytovatelem služby vytvořeno bezpečné uložiště pro sdílení kompletních materiálů k poskytované službě. |  |
| 8. | **Správa a dohled zdrojů** – zajištění Performance a Capacity management |  |
| 9. | **Síťový dohled** – zajištění Network Performance Monitoring and Diagnostics, zajištění Detection Anomaly. Zajištění Apps Performance Monitoring. |  |
| 10. | **Bezpečnostní dohled –** zajištění správy a provozu nástrojeSIEM. |  |
| 11. | **Incident management** – zajištění Operátorské činnosti, Incident handling, Incident Response. |  |
| 12. | **Analýza incidentů** – zajištění odborné činnosti v detekci a lokalizaci příčin incidentů Analytikem ze strany poskytovatele služby. |  |
| 13. | **Návrhy systematických opatření** – Sestavení opatření v organizační a technické úrovni pro posouzení zadavatelem. |  |
| 14. | **Návrhy řešení incidentů** – zajištění odborné činnosti pro kategorizaci na interní a externí příčiny incidentů a k nim příslušných opatření. |  |
| 15. | **Reporting a analýza stavů, událostí a incidentů** – zajištění odborné činnosti pro doložení úrovně bezpečnosti vůči interním kontrolním procesům nebo pro doložení vůči externím kontrolním autoritám. |  |
| 16. | **Správa informací o aktivech informačních systémů zadavatele** – Zajištění automatizace pro pasportizaci ICT pracovišť manipulujících s klasifikovanými informacemi nebo obsahující privilegované oprávnění k výkonu kritických činností. |  |
| 17. | **Kybernetická bezpečnost** – Personální zajištění služby pracovníky s odbornou způsobilostí vyhovující požadavkům na zajištění kybernetické bezpečnosti kritické infrastruktury v souladu s požadavky *zákona 181/2014Sb. o kybernetické bezpečnosti* v celém průběhu služby a všech jejích procesů a rutin. |  |
| 18. | **Režim Maintenance** – Plánování odstávek poskytované služby se zajištěnou náhradou. |  |
| 19. | **Business Continuity** – Služba (včetně všech komponent, které využívá) musí být odolná proti výpadkům a poruchám. Všechny komponenty služby musí být schopny dlouhodobého provozu bez změny chování a úbytku výkonu. |  |
| 20. | **Zajištění souladu se zákonem ZoKB (Compliance)** - Všechny parametry služby musí zajistit na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Dostupnost, Nepopiratelnost, Autentizaci, Autorizaci. |  |
| 21. | Pokud zadavatel z organizačních důvodů rozhodne pro in-sourcing části procesů nebo workflow (např. Zřízení analytického týmu, útvaru provozu bezpečnostní infrastruktury, Operation centra pro aplikace, systémy, databáze, datovou síť, bezpečnostní komponenty atp.) musí služba poskytovatele umožnit separaci na úrovní procesů, systémů, dat, přístupových oprávnění, včetně transferu historických dat a informací do prostředí zadavatele. Náklady na změnu hradí zadavatel. Požadavek na vydělení části služby do samostatné části, není důvodem k okamžité výpovědi smlouvy. |  |
| 22. | **Adaptace a akceptace sdílených procesů** – Služba zajistí úpravu procesů na straně poskytovatele služby a návrh na jejich integraci s relevantními procesy na straně zadavatele. |  |
| 23. | **SLA procesních vstupů a výstupů** – Služba zajistí monitoring procesů na straně poskytovatele služby a zadavatele. |  |
| 24. | **Vizitace zadavatele v místě výkonu služby** – poskytovatel služby před podpisem smlouvy umožní zadavateli návštěvu vlastního bezpečnostního dohledového centra, aby si mohl ověřit splnění požadavků. Zjištění nedodržení požadavků je důvod pro vyloučení poskytovatele služby. |  |
|  | **Technické požadavky na SOC** |  |
| 25. | Poskytovatel služby provozuje vlastní *Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí*, který umožňuje napojení na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí zadavatele. |  |
| 26. | Rozhodné operace a manipulace jsou prováděny prostředky zadavatele a nástroje poskytovatele služby budou sloužit na jeho straně pro případnou agregaci informací v rámci jeho procesů. Žádný ze způsobů propojení nesmí omezit nebo narušit primární autonomní fungování celého řešení jen prostředky zadavatele. |  |
| 27. | V rámci služby poskytovatel zajistí *provozní monitoring* bezpečnostních nástrojů zadavatele, dle předmětu zakázky, v rozsahu:   * dostupnost a funkčnost bezpečnostních nástrojů, * vytíženost bezpečnostních nástrojů, * detekce vyčerpání kapacitních zdrojů u bezpečnostních nástrojů. |  |
| 28. | V rámci služby poskytovatel zajišťuje *nastavování bezpečnostních nástrojů* zadavatele, dle předmětu zakázky, v rozsahu:   * úprava a optimalizace korelačních pravidel, dle požadavku zadavatele nebo dle best-practice poskytovatele, * přidávání nových zařízení, * vytváření nových scénářů pro detekci, * úprava nastavení nástrojů, dle požadavku zadavatele nebo NÚKIB. |  |
|  | **Požadovaná podpora SOC** |  |
| 29. | **Ticketovací systém** – služba s on-line přístupem pro kompletní správu požadavků, včetně uchování historie požadavků a jejich řešení. |  |
| 30. | Přístup zadavatele k podpoře *provozu systémů* – HotLine |  |
| 31. | Přístup zadavatele k podpoře *Incident Response* – HotLine, telefon/ email na členy CSIRT |  |
| 32. | Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NÚKIB, kooperující CSIRT atd. |  |
| 33. | Přístup *administrátorů zadavatele* ke sledovaným parametrům služby prostřednictvím grafického rozhraní (GUI – dashboard apod.), alespoň v režimu čtení nebo v přístupové roli *Auditor*. |  |
| 34. | **Notifikace/Eskalace** – Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / telefon). |  |
| 35. | **Vulnerability management** – služba kontinuálního skenování aktiv zadavatele definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále vždy 1x měsíčně skeny rozdílové. |  |
| 36. | **Vulnerability management** – Relevance ***zranitelnosti*** – U aktiv musí být ověřena relevantnost incidentů pro dané aktivum vulnerability scannerem. |  |
| 37. | **Reporty – Rozšířený *reporting*** – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu, např. formou videokonference. Prezentace měsíčních reportů v rozsahu min. 30 minut - max. 6 hod. |  |
| 38. | **Reporty** – on***-demand*** – Služba zajistí provádění on-demand spouštění některých pravidel a z výstupu bude vytvářet reporty. |  |
| 39. | **Reporty** – ***Standard*** – poskytovatel v rámci služby zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsáno:   * průběh realizace Plnění služby za uplynulé období; * provedené služby za uplynulé období; * návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a v prevenci eliminace incidentů. |  |
| 40. | **Technologie sběru dat** – Služba zajistí užití nástroje SIEM a nástroje Flowmon v majetku zadavatele jako základního zdroje dat a bude s ním komunikovat průmyslově standardními protokoly.  Navrhované řešení poskytovatele služby:   * zajištuje na straně zadavatele sběr, přenos a uložení logů a jejich vyhodnocování v rámci nástroje SIEM Zadavatele. Případný SIEM poskytovatele služby plní roli Federativní komponenty k výkonu Operátorské činnosti v rámci služby SOC. * zajištuje na straně zadavatele sběr a vyhodnocení NetFlow v rámci nástroje Flowmon zadavatele. * zajištuje na straně zadavatele sběr a vyhodnocení logů v rámci nástroje LOGmanager zadavatele. * Zajišťuje na straně zadavatele viditelnost nových a stávajících síťových prvků v rámci nástroje AddNet * je schopno regulovat zatížení přenosové linky (Bandwidth throttling) podle specifikace zadavatele (minimum 500kbs, maximum 4 Mbs)., jak na vstupu, tak na výstupu VPN/Internetu ze strany zadavatele. * má na své straně služby ve svém komunikačním bodu zařazen VPN akcelerátor. * má na své straně služby ve svém komunikačním bodu Internetu zařazenu komponentu „DDoS pračku“. * má interní storage prostor na konektivitě v propustnosti minimálně 1Gb s využitím VPN v redundantní konfiguraci. * má disponibilně volný interní storage prostor v objemu min. 20TB. * umí detekovat nové nebo dosud neznámé log data či transakční záznamy, a identifikovat jejich relevanci k provozní nebo bezpečnostní kategorii u zadavatele. |  |
| 41. | **Base line analýza** – Služba zajistí porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti. |  |
| 42. | **Členění aktiv** – Aktiva musí:   * být možno rozdělit:   + podle jejich důležitosti v procesech zadavatele;   + podle typu a povahy generování dat:     - Log data na struktuře Syslog přes UDP/TCP ve standardu IETF],     - NetFlow ve standardu IETF.     - SNMP ve standardu IETF.     - Transakční záznamy – SIP, DNS, DHCP, FRAUD ve standardu IETF nebo dle požadavků zákona eIDAS nebo zákona o Spisové službě. * mít uživatelsky definovatelné kategorie a parametry podle požadavků zadavatele. |  |
| 43. | **Kategorizace aktiv** – Služba zajistí jednotnou evidenci a vyhodnocení kategorie aktiv, podle povahy aktiva (viz bod 48.). Podle těchto kategorií bude poskytovatel služby utvářet další pravidla nebo reporty v prostředcích zadavatele. |  |
| 44. | **Manuální parsovací pravidla** – Služba zajistí generování parsovacích pravidel a reportů v prostředcích zadavatele. |  |
| 45. | **Historická korelace** – Služba zajistí ověření nového korelačního pravidla proti historickým datům. |  |
| 46. | **Služba Monitoring Privilegovaných účtů – Sdílené *účty*** – Služba zajistí detekci užití privilegovaných přístupů pro konkrétního uživatele v systémech zadavatele. |  |
| 47. | **Režim Maintenance** – Služba musí být schopna běhu v režimu údržby ohlášenou zadavatelem, kdy se údržbou dotčených zdrojů/aktiv nebudou vyhlašovat alerty. |  |
| 48. | **Služba Monitoringu a detekce**   * Průběžné sledování provozu prostředí zadavatele. * Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. * 2x denně odborné posouzení bezpečnostní situace a provozního stavu. V případě anomálie posouzení její relevance a závažnosti. * Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému zadavatele na analytického specialistu poskytovatele služby. |  |
| 49. | **Služba včasné výstrahy a reakce na nestandardní situace v provozu bezpečnostních systémů**   * Zpracování analytických scénářů na aktuální kybernetické hrozby. * Posouzení eskalovaného problému Zadavatele analytickým specialistou Předkladatele. * Detekce a vyhodnocení závažnosti identifikovaných anomálií. * Posouzení a případná eskalace nestandardní situace v provozu Zadavatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR. |  |
|  | **SLA** |  |
| 50. | Poskytovatel služby musí provozovat vlastní bezpečnostní dohledovou službu v režimu 24x7x365, s minimální dostupností operátorů v pracovní dny od 6:00 do 22:00 hodin a s minimální dostupností Analytiků v pracovní dny od 9:00 do 17:00 hod |  |
| 51. | Pro každý kybernetický incident (dle §7, ZokB) prochází poskytovatel služby následným postupem k určení kategorií kybernetických bezpečnostních incidentů (dle §31, VoKB) podle následků a negativních projevů pro doporučení opatření či součinnosti v následné reakci:  Fáze Detekce   * Monitoring prostředí vymezeného zadavatelem. * Dohledování bezpečnostní situace zadavatele. * Detekce anomálie – rozpoznání odchylky od běžného stavu nebo od zadavatelem normovaného stavu.   Fáze Přiřazení   * Klasifikace anomálie – určení závažnosti ve škále:   + False-Positive Alarm – způsobuje falešný alarm z důvodu:     - chyby v úsudku míry závažnosti anomálie;     - nepřesnosti rozpoznání odchylky vzniklé při dohledování a monitoringu v předchozí fázi Detekce.   + Bezpečnostní událost – anomálie, která může způsobit narušení bezpečnosti:     - informací v informačních systémech zadavatele;     - služeb zadavatele;     - a integrity datových sítí zadavatele.   + Bezpečnostní incident – anomálie, která narušila či narušuje bezpečnost:     - informací v informačních systémech zadavatele;     - služeb zadavatele;     - a integritu datových sítí zadavatele nebo jiných subjektů.   Fáze Analýza   * Vyhodnocení anomálie – vyhodnocení relevance:   + k systémům zadavatele;   + k procesům zadavatele;   + k zákonným normám ČR vztažených na zadavatele. * Klasifikace incidentu – začlenění incidentu do bezpečnostního typu kategorie dle určení zadavatelem nebo dle §30, VoKB:   + Podle příčiny:     - incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb;     - incident způsobený škodlivým kódem;     - incident způsobený překonáním technických opatření;     - incident způsobený porušením organizačních opatření;     - incident spojený s projevem trvale působících hrozeb;     - ostatní incidenty způsobené kybernetickým útokem.   + Podle dopadu:     - incident způsobující narušení důvěrnosti aktiv;     - incident způsobující narušení integrity aktiv;     - incident způsobující narušení dostupnosti aktiv;     - incident způsobující kombinaci výše uvedených dopadů. * Kategorizace incidentu – začlenění incidentu podle významnosti. |  |
| 52. | **Kategorie III** – do 30 minut – velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu, včetně minimalizace vzniklých i potenciálních škod. |  |
| 53. | **Kategorie II** – do 2 hodin – závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod. |  |
| 54. | **Kategorie I** – do 24 hodin – méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. Jedná se o bezpečnostní incidenty, které nespadají do kategorií III a II. |  |