**Příloha č. 1 servisní smlouvy Kyberbezpečnost v MMN a.s.**

**VYMEZENÍ ROZSAHU**

Servisní a technická podpora bude poskytována na všechny části díla dodaného jako předmět plnění Smlouvy o dílo z veřejné zakázky „Kyberbezpečnost v MMN a.s.“, a to na dobu 5 let od ukončení realizace předmětu plnění dle výše uvedené smlouvy o dílo. Jedná se o služby technické a servisní podpory, služby podpory kybernetického zabezpečení a související služby (dále jen Technická podpora), a to pro všechna zařízení, systémy, aplikace a služby dodané v rámci samostatné smlouvy o dílo na dodávku a implementaci, tedy o prvky specifikované v přílohách:

1. Svazek 3a – Obchodní podmínky – Příloha č.1 – Technická specifikace prvků aktivní bezpečnosti
2. Svazek 3a – Obchodní podmínky – Příloha č.2 – Technická specifikace prvků pasivní bezpečnosti
3. CENA
   1. Cena za služby servisní a technické a služby podpory kybernetického zabezpečení a související služby je uvedena v servisní smlouvě.
4. TECHNICKÁ PODPORA
   1. Součinnost při průběžném provádění inovace technologií a systémů implementovaných v rámci projektu „Kyberbezpečnost v MMN a.s.“ (dále také jako Projekt) a jeho jednotlivých technologických částí.
   2. Součinnost při provádění obecných změn technologií a systémů v rámci Projektu v důsledku vývoje HW a SW prostředků.
   3. Součinnost při distribuci nových verzí produktu a bezpečnostních a funkčních oprav (patchů), včetně aktuální dokumentace a popisu změn zpřístupněním pokynů k jeho elektronickému stažení Objednatelem z datového úložiště určeného Poskytovatelem.
   4. Služba Helpdesk formou webového portálu pro oprávněné osoby Objednatele jako primární prostředek pro hlášení závad a požadavků na Technickou podporu.
   5. Služba Hotline formou telefonické podpory pro oprávněné osoby Objednatele jako záložní prostředek pro hlášení požadavků na Technickou podporu.
5. SERVISNÍ PODPORA
   1. Služby odstraňování vad. Proces odstraňování vad produktu bude probíhat v těchto režimech:
      1. Kategorie závažnosti vady „**vysoká**“

Jedná se o vady zcela zabraňující provozu, produkt není použitelný ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující činnost systému. Tento stav může ohrozit běžný provoz Objednatele a nelze jej dočasně řešit organizačním opatřením.

Nejpozději do 8 pracovních hodin po nahlášení vady provede Poskytovatel zjištění příčin, které vadu způsobují. Jde-li o vadu způsobenou důvody na straně Poskytovatele (oprávněná reklamace) bezodkladně zahájí práce na odstranění vady a zajistí odstranění této vady ve lhůtě do 48 pracovních hodin od nahlášení vady, a to i způsobem dočasného provizorního řešení, umožňujícího provoz produktu. Vada bude odstraněna v nejkratší možné lhůtě s ohledem na její povahu a dopad na činnost Objednatele.

Jde-li o vadu způsobenou důvody na straně Objednatele, dohodne Poskytovatel s Objednatelem další postup.

* + 1. Kategorie závažnosti vady „**střední**“

Jedná se o vady omezující provoz, funkčnost systémů je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz Objednatele. Jedná se také o vady způsobující problémy při užívání a provozování produktu nebo jeho části, ale umožňující provoz, jimiž způsobené problémy lze dočasně řešit organizačními opatřeními.

Nejpozději do 16 pracovních hodin po nahlášení vady provede Poskytovatel zjištění příčin, které vadu způsobují. Jde-li o vadu způsobenou důvody na straně Poskytovatele (oprávněná reklamace) bezodkladně zahájí práce na odstranění vady a zajistí odstranění této vady ve lhůtě do 10 pracovních dnů od nahlášení vady. Vada bude odstraněna v nejkratší možné lhůtě s ohledem na její povahu a dopad na činnost Objednatele.

Jde-li o vadu způsobenou důvody na straně Objednatele, dohodne Poskytovatel s Objednatelem další postup.

* + 1. Kategorie závažnosti vady „**nízká**“

Jedná se o vady neomezující provoz, drobné vady, které nespadají do kategorií „vysoká“ nebo „střední“. Nejpozději do 2 pracovních dnů po nahlášení vady provede Poskytovatel zjištění příčin, které vadu způsobují. Jde-li o vadu způsobenou důvody na straně Poskytovatele (oprávněná reklamace) bezodkladně zahájí práce na odstranění vady a zajistí odstranění této vady ve lhůtě do 20 pracovních dnů od nahlášení vady.

Jde-li o vadu způsobenou důvody na straně Objednatele, dohodne Poskytovatel s Objednatelem další postup.

* 1. Zařazení vady do jednotlivých kategorií určuje Objednatel (návrhem při prvotním kontaktu s Helpdesk nebo Hotline Poskytovatele) ve spolupráci s Poskytovatelem.
  2. Poskytnutí součinnosti při řešení provozních problémů jednotlivých aplikačních částí díla vzniklých při jejich užití Objednatelem.
  3. Poskytnutí součinnosti při řešení provozních problémů vzniklých při užití díla na pracovišti Objednatele.
  4. Poskytování služby Helpdesk pro hlášení závad a požadavků na servis, metodickou podporu, poradenství a konzultace a jejich řešení pro oprávněné osoby Objednatele.
  5. Poskytování služby Hotline, jako záložní komunikační řešení pro hlášení závad a požadavků na servis, metodickou podporu, poradenství a konzultace a jejich řešení pro oprávněné osoby Objednatele nebo pro řešení závažných naléhavých situací.

1. KYBERNETICKÁ BEZPEČNOSTNÍ PODPORA
   1. Služby spojené s kybernetickým dohledem a zabezpečením systémů Objednatele. Proces bude zahrnovat, že níže definované požadavky budou pravidelně ze strany Poskytovatele vyhodnocovány a data o jejich plnění budou k dispozici oprávněným zástupcům Objednatele. Reakce na zjištěnou kybernetickou bezpečnostní událost (dále jen Incident) bude v režimu aktivního dohledu a dle kategorizace očekávaného kybernetického bezpečnostního incidentu v režimech:
      1. Kategorie závažnosti Incidentu „**vysoká**“

Jedná se o velmi závažné narušení kybernetické bezpečnosti, které významně a přímo ohrožuje bezpečnost poskytovaných služeb nebo dat a vyžaduje neprodlený zásah odpovědných osob daného systému pro zabránění dalšího šíření hrozby, minimalizaci škod a poskytnutí hlášení na NÚKIB. Tento stav může ohrozit běžný provoz a data Objednatele a nelze jej dočasně řešit organizačním opatřením.

Nejpozději do 3 hodin provede Poskytovatel hlášení o potencionálním incidentu. Následně nejpozději do 6 hodin provede Poskytovatel výsledky vstupní analýzy a navrhne další kroky k postupu**.**

* + 1. Kategorie závažnosti Incidentu „**střední**“

Jedná se o závažné narušení kybernetické bezpečnosti poskytovaných služeb nebo dat vyžadující rychlý zásah odpovědných osob. Tento stav může ohrozit běžný provoz Objednatele, ale lze jej dočasně řešit organizačním opatřením.

Nejpozději do 6 hodin provede Poskytovatel hlášení o potencionálním incidentu. Následně nejpozději do 8 hodin provede Poskytovatel výsledky vstupní analýzy a navrhne další kroky k postupu**.**

* + 1. Kategorie závažnosti Incidentu „**nízká**“

Jedná se o méně závažné narušení kybernetické bezpečnosti poskytovaných služeb nebo dat, které nevyžaduje okamžitý zásah odpovědných osob a které nespadají do kategorií „vysoká“ nebo „střední“. Nejpozději do konce následujícího pracovního dne provede Poskytovatel hlášení o potencionálním incidentu včetně vstupní analýzy a návrhu kroků dalšího postupu.

* 1. Zařazení Incidentu do jednotlivých kategorií určuje Poskytovatel ve spolupráci s Objednatelem (návrhem při prvotním kontaktu s Objednatelem) na základě zjištění informací z dohledového centra a odborných znalostí.
  2. Hlášení o potenciálním incidentu se rozumí oznámení o podezření na Incident a základní informace o zasaženém aktivu (monitorovaném zdroji Objednatele).
  3. Výsledkem úvodní analýzy se rozumí aktuální informace o rozsahu incidentu, specifikace zasažených aktiv, potenciálních příčin a dopadů, indikace způsobu řešení a návrh opatření k okamžité ochraně aktiv.
  4. Poskytovatel se zavazuje spolupracovat v začlenění procesů dohledového centra do tzv. Businness Continuity Managementu Objednatele – primárně poskytováním konzultací. Kapacity pro tyto konzultace budou Objednateli poskytnuty bezodkladně, zahájení konzultací maximálně do 5 pracovních dní od zadání požadavku.
  5. Aktivní dohled centra v rozsahu přítomnosti operátorů provádějících L1 triáž a L2 analytika, je zajišťován v pracovních dnech dle stanovených SLA parametrů pro řešení kybernetických bezpečnostních incidentů.
  6. Dostupnost automatizovaných detekčních a dohledových nástrojů je zajišťována v režimu 365x7x24h.
  7. V rámci dohledového centra bude Poskytovatel zajišťovat organizačně a technicky službu CSIRT. Proces využití této služby bude spouštěn na základě požadavku Objednatele.
  8. Poskytovatel bude Objednateli poskytovat výstupy s přehledem o plnění sledovaných indikátorů nastavených v rámci požadavků na dostupnost a úroveň služeb.
  9. Objednatel má přístup k informacím ve všech částech nebo technologiích minimálně v rozsahu pro čtení. Přidělení vyšších přístupů Objednateli může být dohodnuto v rámci vzájemné písemné dohody.
  10. Poskytovatel se zavazuje spolupracovat v začlenění procesů kybernetického bezpečnostního dohledového centra do Businness Continuity Managementu zadavatele formou poskytováním konzultací.
  11. Poskytovatel bude spolupracovat na pravidelném hodnocení dodavatelů z pohledu kybernetické bezpečnosti dodavatelského řetězce dle legislativních požadavků.
  12. Poskytovatel bude zajišťovat potřebné kapacity specialistů kybernetického bezpečnostního dohledu v rozsahu úrovní podpory L1, L2 a L3.
  13. Poskytovatel bude zajišťovat potřebné kapacity kvalifikovaných specialistů pro kybernetický bezpečnostní dohled v rozsahu kvalifikací minimálně:
      1. **Vedoucí týmu kybernetické bezpečnosti**
* Praxe v oboru kybernetické bezpečnosti minimálně 5 let.
* Zkušenosti s vedením alespoň 3 zakázek obdobného charakteru, jejichž předmět zahrnoval nebo zahrnuje dodávku, implementaci, podporu a napojení do bezpečnostního dohledového centra.
* Je držitelem certifikátu z oblasti projektového řízení např. Prince2 Foundation a vyšší, IPMA nebo obdobný.
  + 1. **Architekt pro kybernetickou bezpečnost**
* Praxe v oboru kybernetické bezpečnosti minimálně 5 let.
* Zkušenosti s realizací alespoň 2 zakázek obdobného charakteru splňující významné zakázky.
* Je držitelem certifikátu architekta na úrovni TOGAF Enterprise Architecture Foundation a vyšší, ITIL Foundation a vyšší nebo Architekt KB dle ZoKB.
  + 1. **Auditor pro kybernetickou bezpečnost**
* Praxe v oboru kybernetické bezpečnosti minimálně 5 let.
* Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje organizační opatření a plán continuity.
  + 1. **Technický specialista pro datové toky (Flows)**
* Praxe v oboru ICT minimálně 5 let.
* Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje analýzu datových toků v síti na základě monitoringu založeném na analýze NetFlow/IPFIX či obdobné.
* Je držitelem certifikátu na nabízené technologie, a to minimálně v rozsahu certifikace pro techniky, ne obchodní.
  + 1. **Technický specialista pro zranitelnosti**
* Praxe v oboru ICT minimálně 5 let.
* Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje správu a management zranitelností.
* Je držitelem certifikátu na nabízené technologie, a to minimálně v rozsahu certifikace pro techniky, ne obchodní.
  + 1. **Technický specialista log managementu a SIEM**
* Praxe v oboru ICT minimálně 5 let.
* Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje Log Management a SIEM.
* Je držitelem certifikátu na nabízené technologie, a to minimálně v rozsahu certifikace pro techniky, ne obchodní.