|  |  |
| --- | --- |
| Sp. zn.: MZE-35827/2021-11153Č. j.: MZE-68278/2024-12122 | MZE-68278/2024-12122dms_carovy_kodmzedms028355826 |

**Požadavek na změnu (RfC)[[1]](#endnote-1) – Z39724**

**a – věcné zadání**

# Základní informace

|  |  |
| --- | --- |
| **ID PK MZe**[[2]](#endnote-2)**:** | 20 |

|  |  |
| --- | --- |
| **Název změny**[[3]](#endnote-3)**:** | **Zápis ASM blokací do Portálu služeb** |
| **Datum předložení požadavku:** | 16.8.2024 | **Požadované datum nasazení:** | 31.12.2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie změny**[[4]](#endnote-4)**:** | Normální [x]  Urgentní [ ]  | **Priorita**[[5]](#endnote-5)**:** | Vysoká [ ]  Střední [x]  Nízká [ ]  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace [ ]   | **Zkratka**[[6]](#endnote-6)**:**  | Agribus |
| **Typ požadavku:**  | Legislativní [ ]  Zlepšení [x]  Bezpečnost [ ]  |
| Infrastruktura [ ]  | **Typ požadavku:** | Nová komponenta [ ]  Upgrade [x]  Bezpečnost [ ]  Zlepšení [x]  Obnova [ ]  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno**  | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel/  | David Neužil | **MZe/12122** | 221812012 | david.neuzil@mze.gov.cz |
| Technický garant: | Radek Zápotocký | **MZe/12122** | 221813001 | radek.zapotocky@mze.gov.cz |
| Koordinátor změny: | David Neužil | **MZe/12122** | 221812012 | david.neuzil@mze.gov.cz |
| Poskytovatel / dodavatel: | xxx | **GEM** | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[7]](#endnote-7)**:** | *S2020-0081,DMS 1539-2020-11150* | **KL:** | HR-001 |

# Stručný popis a odůvodnění požadavku

## Popis požadavku

Předmětem tohoto požadavku je řešení dostupnosti auditních informací o zamítnutých voláních služeb na IPF AgriBus, které neprošly validací na virtuálním kontextu XMLFW (F5) dle nastavených schválených bezpečnostních pravidel OKB.

Aktuálně jsou tyto zamítnuté požadavky persistovány syslogem z F5 ASM do SIEMu, ze kterého je objednateli generován týdenní souhrnný report.

## Odůvodnění požadované změny (legislativní změny, přínosy))

Důvodem k realizaci tohoto požadavku je potřeba rychlé a snadné dostupnosti těchto informací, zejména pro servisní oddělení MZe, ale i pro dodavatele, kteří zodpovídají za validní požadavky směřované do zdrojových systémů MZe přes integrační platformu AgriBus.

Přínosem bude snazší identifikace problému při volání jednotlivých služeb odchyceného ASM pravidly na F5, jelikož bude docházet ke zpětnému zápisu do DB dohledového centra v Portálu služeb.

## Rizika nerealizace

Informace o zamítnutých voláních ASM pravidly nebudou dostupné v centrálním dohledovém centru Portálu služeb, nebude možné je nijak auditovat, vyhledávat či zpětně s nimi pracovat. Jediným zdrojem informací o těchto voláních pak zůstane týdenní off-line report.

# Podrobný popis požadavku

xxx

# Dopady na IS MZe

(V případě předpokládaných či možných dopadů změny na infrastrukturu nebo na bezpečnost je třeba si vyžádat stanovisko relevantních specialistů, tj. provozního, bezpečnostního garanta, příp. architekta.).

## Na provoz a infrastrukturu

Nejsou.

## Na bezpečnost

Nejsou.

## Na součinnost s dalšími systémy

Nejsou.

## Požadavky na součinnost AgriBus

(Pokud existují požadavky na součinnost Agribus, uveďte specifikaci služby ve formě strukturovaného požadavku (request) a odpovědi (response) s vyznačenou změnou.)

Nejsou.

## Požadavek na podporu provozu naimplementované změny

(Uveďte, zda zařadit změnu do stávající provozní smlouvy, konkrétní požadavky na požadované služby, SLA.)

## Požadavek na úpravu dohledového nástroje

(Uveďte, zda a jakým způsobem je požadována úprava dohledových nástrojů.)

Budou nastaveny nové kontrolní sondy v monitoringu prostředí (Zabbix), jednak na sledování provozu nové utility i na sledování překročení četnosti zápisů do DB (např. na chybné a neřízené, ale autorizované strojové volání služeb). Treshold v monitoringu bude nastaven centrálně pro všechny služby stejně.

# Požadavek na dokumentaci[[8]](#endnote-8)

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Dokument** | **Formát výstupu** (ano/ne) | **Garant[[9]](#endnote-9)** |
| el. úložiště | papír | CD |
|  | Analýza navrhnutého řešení | NE | NE | NE |  |
|  | Dokumentace dle specifikace Závazná metodika návrhu a dokumentace architektury MZe[[10]](#endnote-10) | NE | NE | NE |  |
|  | Testovací scénář, protokol o otestování | ANO | NE | NE |  |
|  | Uživatelská příručka | ANO | NE | NE | Věcný garant |
|  | Provozně technická dokumentace (systémová a bezpečnostní dokumentace) | ANO | NE | NE | OKB, OPPT[[11]](#endnote-11) |
|  | Zdrojový kód a měněné konfigurační soubory | ANO | NE | NE |  |
|  | Webové služby + konzumentské testy | NE | NE | NE |  |
|  | Dohledové scénáře (úprava stávajících/nové scénáře)[[12]](#endnote-12) | ANO | NE | NE |  |

### V připojeném souboru je uveden rozsah vybrané technické dokumentace – otevřete dvojklikem:

Dohledové scénáře jsou požadovány, pokud Dodavatel potvrdí dopad na dohledové scénáře/nástroj.

U dokumentů, které již existují, se má za to, že je požadována jejich aktualizace. Pokud se požaduje zpracování nového dokumentu namísto aktualizace stávajícího, uveďte toto explicitně za názvem daného dokumentu, např. „Uživatelská příručka – nový“.

Provozně-technická dokumentace bude zpracována dle vzorového dokumentu, který je připojen – otevřete dvojklikem:xxx

# Akceptační kritéria

Plnění v rámci požadavku na změnu bude akceptováno, jestliže budou akceptovány dokumenty uvedené v tabulce výše v bodu 5.

# Základní milníky

|  |  |
| --- | --- |
| **Milník** | **Termín** |
| Zahájení plnění | Zveřejněním objednávky v registru smluv |
| Ukončení plnění | 31.12.2024 |

# Přílohy

# Podpisová doložka

|  |  |  |
| --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Datum a podpis** |
| Žadatel | David Neužil |  |
| Technický garant | Radek Zápotocký |  |

**B – nabídkA řešení k požadavku Z39724**

|  |  |
| --- | --- |
| **ID PK MZe**[[13]](#endnote-13)**:** | 20 |

# Návrh konceptu technického řešení

Bude vyvinuta nová samostatná komponenta, která bude vyčítat jednotlivé záznamy ze syslogu, pročistí dodané údaje a uloží je do DB.

S daným záznamem se bude zacházet jako s textem, nikoliv jako s XML – XMLFW vyhodnotil daný záznam jako porušení pravidel a tudíž v příchozím volání může být cokoliv a pokus o zpracování záznamu jako XML by mohlo vést k pádu komponenty.

Komponenta bude pracovat s prerekvizitou, že ukládaný obsah nebude kontrolován a obsah volání může obsahovat nelogické či nesmyslné požadavky.

Komponenta vloží do DB průběh volání odpovídající TCE s tím, že doba zpracování volání služby je rovna nule. Důvodem je vynechání těchto volání ze sledování KPI, jelikož nedochází k samotnému zpracování službou.

Komponenta bude naprogramována v jazyce Python, s využitím knihoven syslog a cx\_oracle.

Komponenta poběží v jediné instanci na jednom ESB serveru (o její běh se bude starat Oracle Clusterware), aby nedošlo k duplicitním záznamům v db. Při zápisu do DB se využije existující API, čímž bude zajištěna konzistence s ukládáním ostatních volání.

Budou připraveny nové kontrolní sondy v monitoringu prostředí (Zabbix) na sledování provozu nové aplikace a na sledování překročení četnosti zápisů do DB (např. na chybné a neřízené, ale autorizované strojové volání služeb) – např. 100 výskytů za 1 minutu. Treshold v monitoringu bude nastaven centrálně pro všechny služby stejně. V případě nedostupnosti komponenty (monitorovacím záznamem) či překročení definovaného tresholdu bude informován a aktivován dohled.

Samotné řešení se skládá z několika samostatných částí:

* Rozšíření syslogu přenášejícího logy z F5 do SIEMu pro zasílání logů také do Agribusu
* Úpravy FW – zajištění prostupů pro syslog do Agribusu
* Konfigurace syslogu na straně Agribusu
* Vývoj komponenty pro čtení dat ze syslogu a zápis do DB
* Nainstalování komponenty do Oracle Clusterware
* Úprava stávající dokumentace

# Uživatelské a licenční zajištění pro Objednatele

Není nutné.

# Tento změnový požadavek neřeší

# Dopady do systémů MZe

# Na provoz a infrastrukturu

(Pozn.: V případě, že má změna dopady na síťovou infrastrukturu, doplňte tabulku v připojeném souboru - otevřete dvojklikem.)

Aktuálně bez dopadu.

# Na bezpečnost

Návrh řešení musí být v souladu se všemi požadavky v aktuální verzi Směrnice systémové bezpečnosti MZe. Upřesnění požadavků směrnice ve vztahu k tomuto RfC:

|  |  |  |
| --- | --- | --- |
| **Č.** | **Oblast požadavku[[14]](#endnote-14)** | **Předpokládaný dopad a navrhované opatření/změny** |
|  | Řízení přístupu 3.1.1. – 3.1.6.[[15]](#footnote-1) | Ne |
|  | Dohledatelnost provedených změn v datech 3.1.7. | Ne |
|  | Centrální logování událostí v systému 3.1.7.[[16]](#footnote-2) | Ne |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. | Ne |
|  | Integrita – constraints, cizí klíče apod. 3.2. | Ne |
|  | Integrita – platnost dat 3.2. | Ne |
|  | Integrita – kontrola na vstupní data formulářů 3.2. | Ne |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. | Ne |
|  | Práce s pamětí 3.4.4. | Ne |
|  | Řízení – konfigurace změn 3.4.5.[[17]](#footnote-3) | Ne |
|  | Ochrana systému 3.4.7. | Ne |
|  | Testování systému 3.4.9. | Ne |
|  | Externí komunikace 3.4.11. | Ne |

Návrh řešení procesních agend maximálně respektuje bezpečnostní pravidla nastavená v Agribus resp. Agribus II a dále pravidla a zvyklosti realizace zabezpečení Portálu MZe.

# Na součinnost s dalšími systémy

Součinnost je očekávána ze strany MZe při vyjasňování detailů specifikace požadavků na zadání v průběhu realizace.

# Na součinnost AgriBus

# Na dohledové nástroje/scénáře[[18]](#endnote-15)

# Ostatní dopady

(Pozn.: Pokud má požadavek dopady do dalších požadavků MZe, uveďte je také v tomto bodu.)

Aktuálně nejsou.

# Požadavky na součinnost Objednatele a třetích stran

|  |  |
| --- | --- |
| **MZe / Třetí strana** | **Popis požadavku na součinnost** |
| MZE / O2ITS | Infrastrukturní konzultace a úpravy konfigurace |
| MZE / CompuNet | Infrastrukturní konzultace a úpravy konfigurace |

(Pozn.: K popisu požadavku uveďte etapu, kdy bude součinnost vyžadována.)

# Harmonogram plnění[[19]](#endnote-16)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Termín objednání = zahájení plnění | 13.09.2024 |
| Vývoj aplikace | 18.10.2024 |
| Nasazení na TEST | 21.10.2024 |
| Nasazení na PROD (pilot) | 20.11.2024 |
| Pilot a zvýšená podpora | 04.12.2024 |
| Dokumentace, akceptace | 11.12.2024 |

Uvedený harmonogram je platný v případě, že Dodavatel obdrží objednávku v rozmezí 11.9.-18.9.2024. V případě pozdějšího data objednání si Dodavatel vyhrazuje právo na úpravu harmonogramu v závislosti na aktuálním vytížení kapacit daného realizačního týmu Dodavatele či stanovení priorit ze strany Objednatele.

# Pracnost a cenová nabídka navrhovaného řešení

včetně vymezení počtu člověkodnů nebo jejich částí, které na provedení poptávaného plnění budou spotřebovány

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[20]](#endnote-17) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH** | **v Kč s DPH** |
|  |  |  |  |  |
| Analytik | Analýza, Konzultace, Podpora testování, Dokumentace | 19 | 119 700 | 144 837 |
| Architekt | Architektura řešení, konzultace | 8 | 50 400 | 60 984 |
| Vývojář | Vývoj dle zadání, Unit Testy, Oprava chyb, Podpora testování | 69 | 434 700 | 525 987 |
| Integrační specialista | Koordinace úprav konfigurace infrastrukturní oblasti | 7 | 44 100 | 53 361 |
| QA | Testování, Testovací scénáře, Kontrola kvality řešení, PM | 15 | 94 500 | 114 345 |
| **Celkem:** | **118** | **743 400** | **899 514** |

(Pozn.: MD – člověkoden, MJ – měrná jednotka, např. počet kusů)

# Přílohy

|  |  |  |
| --- | --- | --- |
| **ID** | **Název přílohy** | **Formát** **(CD, listinná forma)** |
|  |  |  |
|  |  |  |

# Podpisová doložka

|  |  |  |
| --- | --- | --- |
| **Název Dodavatele / Poskytovatele** | **Jméno** **oprávněné osoby**[[21]](#endnote-18) | **Datum a podpis:** |
| GEM System a.s. | xxx |  |

**C – Schválení realizace požadavku Z39724**

|  |  |
| --- | --- |
| **ID PK MZe**[[22]](#endnote-19)**:** | 20 |

# 1 Specifikace plnění

Požadované plnění je specifikováno v části A a B tohoto RfC.

Dle části B bod 3.2 jsou pro realizaci příslušných bezpečnostních opatření požadovány následující změny[[23]](#footnote-4):

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Oblast požadavku** | **Realizovat****(ano** [x]  **/ ne** [ ] **)** | **Upřesnění požadavku** |
|  | Řízení přístupu 3.1.1. – 3.1.6. |[ ]   |
|  | Dohledatelnost provedených změn v datech 3.1.7. |[ ]   |
|  | Centrální logování událostí v systému 3.1.7. |[ ]   |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. |[ ]   |
|  |  Integrita – constraints, cizí klíče apod. 3.2. |[ ]   |
|  | Integrita – platnost dat 3.2. |[ ]   |
|  | Integrita - kontrola na vstupní data formulářů 3.2. |[ ]   |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. |[ ]   |
|  | Práce s pamětí 3.4.4. |[ ]   |
|  | Řízení - konfigurace změn 3.4.5. |[ ]   |
|  | Ochrana systému 3.4.7. |[ ]   |
|  | Testování systému 3.4.9. |[ ]   |
|  | Externí komunikace 3.4.11. |[ ]   |

# 2 Uživatelské a licenční zajištění pro Objednatele (je-li relevantní):

# 3 Požadavek na součinnost

|  |  |  |
| --- | --- | --- |
| **Útvar / Dodavatel** | **Popis požadavku na součinnost** | **Odpovědná osoba** |
| MZe | Ověření funkčnosti |  |
|  |  |  |

(V případě, že má změnový požadavek dopad na napojení na SIEM, PIM nebo Management zranitelnosti dle bodu 1, uveďte také požadovanou součinnost Oddělení kybernetické bezpečnosti.)

# 4 Harmonogram realizace[[24]](#endnote-20)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Zahájení plnění – zveřejněním v registru smluv | T |
| Dokončení plnění | T+90 dní |

# 5 Pracnost a cenová nabídka navrhovaného řešení

včetně vymezení počtu člověkodnů nebo jejich částí, které na provedení poptávaného plnění budou spotřebovány

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[25]](#endnote-21) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  | Cenová nabídka | **118** | **743 400** | **899 514** |
| **Celkem:** | **118** | **743 400** | **899 514** |

(Pozn.: MD – člověkoden, MJ – měrná jednotka, např. počet kusů)

# 6 Posouzení

Bezpečnostní garant, provozní garant a architekt potvrzují svým podpisem za oblast, kterou garantují, správnost specifikace plnění dle bodu 1 a její soulad s předpisy a standardy MZe a doporučují změnu k realizaci.

|  |  |  |
| --- | --- | --- |
| **Role** | **Jméno** | **Datum a podpis:** |
| Bezpečnostní garant | Roman Smetana |  |
| Provozní garant | Aleš Prošek |  |
| Architekt | Lucie Mališová |  |

(Pozn.: RfC se zpravidla předkládá k posouzení Bezpečnostnímu garantovi, Provoznímu garantovi, Architektovi, a to podle předpokládaných dopadů změnového požadavku na bezpečnost, provoz, příp. architekturu. Koordinátor rozhodne, od koho vyžádat posouzení dle konkrétního případu změnového požadavku.)

# 7 Schválení

Věcný garant svým podpisem potvrzuje svůj požadavek na realizaci změny za cenu uvedenou v bodu 0 - Pracnost a cenová nabídka navrhovaného řešení.

|  |  |  |
| --- | --- | --- |
| **Role** | **Jméno** | **Datum a podpis:** |
| Žadatel  | David Neužil |  |
| Technický garant | Radek Zápotocký |  |
| Koordinátor změny | David Neužil |  |
| Oprávněná osoba ve věcech ad hoc služeb | Vladimír Velas |  |
| Ředitel odboru IT | Miroslav Rychtařík |  |

(Pozn.: Oprávněná osoba se uvede v případě, že je uvedena ve smlouvě.)

# Vysvětlivky

1. Formulář RfC je tvořen třemi částmi, A - Věcné zadání, B – Nabídka řešení, C - Potvrzení realizace požadavku. První část (Věcné zadání) je předložena poskytovateli/dodavateli jako pobídka k předložení nabídky řešení. Druhou část, tj. část B použije dodavatel řešení k vypracování nabídky, kterou předloží MZe. Třetí část (Potvrzení realizace požadavku) se po vyplnění přiloží k první a druhé části a předloží se ke schválení osobám uvedeným v části C RfC. Poskytovateli/dodavateli se poté vyplněný formulář RfC předkládá v příloze objednávky na realizaci změnového požadavku. Pouze tato podepsaná objednávka je pokynem pro dodavatele/poskytovatele k realizaci změny. [↑](#endnote-ref-1)
2. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-2)
3. Předmět změny – stručná informace, název požadavku [↑](#endnote-ref-3)
4. Kategorie změny – kategorie urgentní se využije v naléhavých případech, kdy je třeba vyřešit nedostupnost zásadní funkcionality systému vzhledem ke zpracování agendy, pro jejíž podporu systém slouží. [↑](#endnote-ref-4)
5. Priorita – vyjadřuje důležitost zapracování požadavku. Vyplní se v případě volby kategorie „Normální změna“. [↑](#endnote-ref-5)
6. Zkratka – zkratka aplikace (viz „kód služby“ v katalogu služeb) [↑](#endnote-ref-6)
7. Smlouva č. – uvede se, pokud existuje smlouva, v rámci níž se požadavky předkládají, totéž platí pro KL (katalogový list). [↑](#endnote-ref-7)
8. Vyplní Change koordinátor. Uvedený seznam dokumentace je pouze příkladem. [↑](#endnote-ref-8)
9. Garant odpovídá za správnost a úplnost dodané dokumentace a zajišťuje její akceptaci. Např. Provozní dokumentaci posuzuje Oddělení kybernetické bezpečnosti (OKB) a Oddělení provozu a podpory technologií (OPPT). [↑](#endnote-ref-9)
10. Rozsah požadované dokumentace uveďte do tabulky. [↑](#endnote-ref-10)
11. OKB – Oddělení kybernetické bezpečnosti, OPPT – Oddělení provozu a podpory technologií [↑](#endnote-ref-11)
12. Požadováno, pokud Dodavatel potvrdí dopad na dohledové scénáře/nástroje. [↑](#endnote-ref-12)
13. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-13)
14. Jednotlivé oblasti – položky v tabulce korespondují s kapitolami Standardu systémové bezpečnosti. [↑](#endnote-ref-14)
15. Uveďte, zda vznikají servisní účty a budou řízené PIMem nebo v něm budou jen evidované. [↑](#footnote-ref-1)
16. Uveďte, zda a jakým způsobem se mění/vytváří napojení na SIEM. [↑](#footnote-ref-2)
17. Uveďte, zda má RfC vliv na napojení na Management zranitelností (Vulnerability scanner). [↑](#footnote-ref-3)
18. Pokud z vyhodnocení dopadů vyplyne potřeba upravit dohledové scénáře nebo zpracování nového scénáře, pak se má za to, že položka seznamu „Požadavek na dokumentaci“ v b. 5 části A RfC „Dohledové scénáře (úprava stávajících/nové scénáře)“ je vyžadována a bude součástí akceptačního řízení, nebude-li v části C RfC v bodu 1 „Specifikace plnění“ stanoveno jinak. [↑](#endnote-ref-15)
19. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-16)
20. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-17)
21. Oprávněná osoba – smluvně určená osoba oprávněná k předkládání požadavku na předložení nabídky. [↑](#endnote-ref-18)
22. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-19)
23. Potvrzení realizace příslušných opatření/změn vyznačí posuzovatel za Oddělení kybernetické bezpečnosti. [↑](#footnote-ref-4)
24. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-20)
25. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-21)