SPRÁVA ŽELEZNIC

— Projekt D – aktivita PAM

— Vyhodnocení 1. kola předběžné tržní konzultace

Kybernetická bezpečnost Správy železnic

— 02.2.2023

Předběžná tržní konzultace PAM (1. kolo)

účastníci	poznámka
účastník 1	bez odpovědi
účastník 2	
účastník 3	
účastník 4	
účastník 5	
účastník 6	
účastník 7	jiná technologie

PTK PAM (1. kolo) – odpovědi

1. Návrh rozdělení fáze :

- **fáze 1: předimplementační analýza**
- **fáze 2: zprovoznění současného PAM s ohledem na změny v infrastruktuře a požadavcích SŽ, doplnění SW licencí a případného specializovaného HW , implementace PAM pro úvodní (jeden nebo více) cílové systémy, ověření pilotním provozem**
- **fáze 3: postupné rozšíření implementace PAM na další definované cílové systémy (SŽT, KB, KII)**
- **fáze 4: technická podpora a rozvoj systému PAM (postupné napojování dalších cílových systémů)**

	Správné rozdělení fází	Komentář
účastník 1	--	bez odpovědi
účastník 2	ČÁST	Nutno přesněji vymezit obsah + přechod F3-F4
účastník 3	ANO	Odpovídá best pactice
účastník 4	ANO	Odpovíldá běžnému členění PAM projektů
účastník 5	ČÁST	Tech. podporu zahájit při předání 1. části do produkce
účastník 6	ANO	Upřesnit z hlediska plnění legislativy
účastník 7	ANO	Pláunují nahradit současné řešení jinou technologií

PTK PAM (1. kolo) – odpovědi

2. Rámcová architektura systému

	HLD architektura	Komentář
účastník 1	--	bez odpovědi
účastník 2	ČÁST	Nutné provést úvodní analýzu
účastník 3	NE	Nedostatek informací
účastník 4	ČÁST	Nutná specifikace parameytrů koncových systémů a rozmístění DC
účastník 5	ČÁST	Nutná úvodní analýza + upřesňující infomace (DR procesy, topologie sítí a DC..)
účastník 6	ČÁST	Nutná znalost strategie ICT a procesů správy priv. účtů
účastník 7	ANO	..avšak nezpracovali.

PTK PAM (1. kolo) – odpovědi

3. Návrh způsobu bezpečného propojení PAM pro primární a podpůrná aktiva

	Oddělené instance PAM	Komentář
účastník 1	--	bez odpovědi
účastník 2	ANO	Řešení je možné implementovat ve dvou kompletně nezávislých instancích (logicky i fyzicky)
účastník 3	NE	Nedostatek informací
účastník 4	ČÁST	Zvážit, zda má smysl oddělené instance vůbec propojovat
účastník 5	ANO	Společný datový trezor (bez využití HSM)
účastník 6	ČÁST	Propojení instancí nahradit HA + procesy DR (propojení je omezující z hlediska vlastností technologie)
účastník 7	ANO	Formou multitenantu

PTK PAM (1. kolo) – odpovědi

4. Možnosti optimalizace licenčního modelu PAM

	Licenční model	Komentář
účastník 1	--	bez odpovědi
účastník 2	ČÁST	Licence: uživatelé PAM - interní admins + externí
účastník 3	NE	Nedostali odpověď od distributora technologie
účastník 4	ČÁST	Nutno znát cílovou architekturu a počty uživatelů PAM
účastník 5	ČÁST	Licence: uživatelé PAM - interní admins + externí "uživatelé"
účastník 6	ČÁST	Licence: uživatelé PAM - admins
účastník 7	ANO	Licence per koncové zařízení

PTK PAM (1. kolo) – odpovědi

5. Odhad předběžné hodnoty a časové náročnosti případné zakázky

	Délka trvání F1+2 cenová indikace	Komentář
účastník 1	--	bez odpovědi
účastník 2	ANO	F1 - 2-3 měsíce, F2 3-4 měsíce služby: 10 mil Kč + 1 mil. ročně podpora licence: 4-4.5 mil. Kč ročně
účastník 3	ČÁST	F1 - 3 měsíce, F2 6 měsíců ceny: nedostali včas informace od CyberArk
účastník 4	ČÁST	F1 - 2-3 měsíce, F2 4-8 měsíců ceny: nedostatek informací
účastník 5	ČÁST	F1 - 2-3 měsíce, F2 4-8 měsíců ceny: nedostatek informací (odhad: licence: 20 mil., HW: 5 mil., služby: 20 mil. Kč)
účastník 6	ČÁST	F1 - 4 měsíce, F2 2 měsíce ceny: ----------
účastník 7	ANO	F1 - 3 měsíce, F2 2 měsíce služby: obch. tajemství licence: 17-25 mil. Kč / 4 roky (900 lic. / 2 VR appliance)

PTK PAM (1. kolo) – odpovědi

6. Rozsah a struktura informací/podkladů potřebných pro zpracování nabídek

	Struktura a rozsah informací pro nabídku	Komentář
účastník 1	--	bez odpovědi
účastník 2	ANO	use-cases, definice řízení priv. účtů současná styruktura priv. účtů autentizace + autorizace PAM politika hesel s ohledem na rotace apod. delegace oprávnění životní cyklus privilegovaných účtů DR a nouzové procesy detailní parametry SLA
účastník 3	ČÁST	Detailnější popis prostředí zadavatele a specifikace jednotlivých typů rozhraní, které si zadavatel přeje monitorovat (RDP, TLS, SQL). Chce zadavatel v rámci nového projektu řešit i část PIM, tedy rotaci hesel.
účastník 4	ČÁST	Detailnější informace o koncovýnch systémech + režim a činnosti podpory nad dodávaným PAM požadavky na proškolení obsluhy (kolik do jaké hloubky) požadavek na strukturu projektové a provozní dokumentace, včetně manuálů pro interní a externí administrátory požadavek a způsob finančního vypořádání na dodatečné služby jako je například integrace dalších systémů pod PAM, či integrace PAM s novými technologiemi, jež nebyly součástí úvodního projektu a analýzy

PTK PAM (1. kolo) – odpovědi

6. Rozsah a struktura informací/podkladů potřebných pro zpracování nabídek

	Struktura a rozsah informací pro nabídku	Komentář
účastník 5	ČÁST	• Cíle projektu a jejich vlastnictví • Konkrétní požadované use-cases • Řízení privilegovaných účtů v řídící dokumentaci • Definice privilegovaného účtu • Využívané způsoby autentizace a autorizace • Politika hesel • Delegace oprávnění • Životní cyklus privilegovaných účtů • Procesy pro nouzový přístup (obálkové účty) • Požadavky na zabezpečení aplikačních a technických privilegovaných účtů a jejich přihlašovacích údajů. Definovat předpokládaný počet aplikací, které si budou vyzvedávat autentizační údaje pro přístup na cílové systémy. • Požadavky na retenci nahrávaných relací privilegovaných uživatelů (sizing úložiště)
účastník 6	ČÁST	1. Korelace reálných uživatelů oproti privilegovaných nepersonifikovaných účtů 2. Definice privilegovaného učtu jak je vnímaná v rámci organizace SŽ. 3. Přesné rozdělení administrátorů pro prvky KB a podpůrných aktiv 4. Specifika technologického stacku a prvků kybernetické bezpečnosti a podpěrných aktiv 5. Požadovaná strategie přístupu externích dodavatelů k účtům v rámci PAM
účastník 7	ANO	Většina údajů z přílohy je dostatečně vypovídající a běžný popis stávajícího HW postačuje. Upřesnění by si zasloužila dislokace jednotlivých řešených destinací z ohledem na přístupy, propojení a případně cestovní náklady.

PTK PAM (1. kolo) – odpovědi

7. Další komentáře k této PTK

Vaše další komentáře k předmětu PTK (účastník 7)
PTK by měl zadavateli dle ÚOHS umožnit zvýšení informovanosti zadavatele o poptávaném plnění veřejné zakázky, popřípadě identifikace jiných způsobů řešení, kterými lze splnit jeho potřeby. Znalost o používaných technologiích získaná z PTK pak zadavateli lépe dá odpověď na otázku, zda jej pro něj přípustná pouze jedna zvolená technologie či varianta řešení, neboť jiné na trhu dostupné technologie. TO umožnit co nejširší zhodnocení požadované budoucí soutěže jak z ohledem na využití stávajících technologií tak z ohledem technologický vývoj na trhu a v neposlední řadě z ohledem na celkové náklady. Pokud bude výsledná vypsaná soutěž technologicky neutrální (vzhledem k nedokončení původních záměru z roku 2019 a nutných dalších investic k případnému dokončení), má možnost zadavatel požadovat „to nejlepší a ověřené na trhu“ a současně mohou celkové náklady pořízení komplexního a uceleného řešení znamenat ve svém důsledku i úsporu celkových prostředku na „Zavedení systému PAM v prostředí SŽ“