

Klasifikace: Veřejný dokument



Testování systému IdM

Příloha č. 12 Zadávací dokumentace veřejné zakázky s názvem
„Nasazení systému IdM v prostředí Správy železnic“

1 Obsah

1	Úvod	2
2	Testování systému IdM v kontextu akceptačního řízení	2
1.1	Typy testů	2
1.1.1	Ověřování testovatelnosti	2
1.1.2	Systémové testy	2
1.1.3	Funkční uživatelské testy	2
1.1.4	Integrační testy	3
1.1.5	Výkonnostní testy	3
1.1.6	DRP	3
1.1.7	Bezpečnostní testy	4
1.2	Typy testů použitých v projektu	5
1.3	Podoba testovacích scénářů	6

1 Úvod

Cílem tohoto dokumentu je definovat základní rozsah testování dodávky systému IdM v prostředí SŽ.

2 Testování systému IdM v kontextu akceptačního řízení

Projekt Nasazení systému IdM v prostředí SŽ bude ze strany Zadavatele akceptován průběžně v souladu s definovanými fázemi projektu a platebními milníky.

Veškeré závažné a kritické problémy vyplývající z penetračních testů musí být bezodkladně odstraněny ještě před uvedením IdM nástroje do produkčního provozu.

Pro potřeby testování poskytne Dodavatel Zadavateli nástroj, kam bude možné zaznamenávat veškeré identifikované vady a nedostatky. Tento nástroj musí dovolovat export statistik pro účely sledování procesu odstraňování identifikovaných nálezů.

1.1 Typy testů

V rámci testování budou použity statické i dynamické typy testů. Scénáře testů budou připraveny ke schválení SŽ Dodavatelem jako součást F1.1 Implementační analýzy. SŽ si je vědoma, že v rámci Implementační analýzy nebudou k dispozici detailně rozpracované testovací scénáře (use case), ty budou detailně rozpracovány Dodavatelem v průběhu implementace.

1.1.1 Ověřování testovatelnosti

Bude prováděno statické posouzení vytvářených dokumentů (příruček, konfigurační dokumentace, use-casů, testovacích scénářů), v rámci kterého, bude ověřen soulad a konzistence dokumentů a jejich návaznost na skutečný stav/podobu implementace IdM nástroje (řešení) v prostředí SŽ.

1.1.2 Systémové testy

Cílem Systémových testů (ST) bude ověřit chování jednoho systému včetně rozhraní, nezávisle na okolních systémech.

1.1.3 Funkční uživatelské testy

Funkčními testy bude ověřeno, že dodaný systém IdM splňuje požadavky a funkčnost podle Technické specifikace, případně zpřesněného návrhu v Implementační analýze. Tyto testy ověřují splnění funkčnosti v jednotlivých

krocích procesů, tak jak jej popisuje funkční specifikace a správnost technického řešení těchto kroků popsaných v návrhu řešení (Implementační analýze).

Funkční testy budou prováděny na základě odsouhlaseného harmonogramu testování, který bude upřesněn Implementační analýzou v dohodnutém testovacím/produkčním prostředí podle úrovně testů. Za formální akceptaci funkčních testů odpovídá Zadavatel.

V oblasti funkčních testů budou provedeny primárně následující typy testů:

Testy funkčnosti

Ověřují, zda jednotlivé funkčnosti řešení odpovídají definovaným požadavkům a funkční specifikaci.

Negativní testy

Ověřují chování systému v případě nekorektního jednání uživatelů (např. zadávání nepovolených hodnot apod.).

Testy procesů

Ověřují chování systému jako celku na základě definovaných procesů, tzv. "End-to-end" testů.

Testy přístupů a oprávnění

Ověřují správnost chování IdM nástroje nebo administrace uživatelských účtů z pohledu řízení životního uživatelských cyklu uživatelských nebo systémových identit, jejich rolí a příslušných oprávnění.

1.1.4 Integrační testy

Integrační testy se zaměří na komplexní otestování vazeb mezi nástrojem IdM a externími aplikacemi integrovanými na nástroj. Probíhat budou na integrovaném testovacím prostředí podle dohodnuté míry integrace.

Odpovědnost za otestování integračních vazeb mezi IdM nástrojem a zapojovanými systémy nese Dodavatel IdM nástroje, který bude současně odpovědný za zajištění funkčnosti těchto vazeb mezi systémy.

1.1.5 Výkonnostní testy

Performance (výkonnostní) testy ověřují, že aplikace dosahuje očekávaných výsledků v oblasti výkonnosti v souladu s požadavkem Zadavatele. Výkonnostní parametry budou zpřesněny v rámci Implementační analýzy zpracované Dodavatelem IdM nástroje.

1.1.6 DRP

V rámci testování systému bude provedeno otestování disaster recovery scénáře, včetně obnovy ze zálohy, případně testu odolnosti systému na požadovanou úroveň redundance. Výstupem bude zdokumentovaný optimální postup oživení systému včetně nutných předpokladů a dosažitelné hodnoty RTO/RPO.

1.1.7 Bezpečnostní testy

Zaměření penetračních testů na důležitá aktiva

Penetrační testování, které Zadavatel nebo jím vybraný třetí strana zrealizuje před uvedením systému do provozu, zohlední především bezpečnostní požadavky na aktiva s vyšším hodnocením z hlediska důvěrnosti, dostupnosti a integrity.

Popis provedení testů

Penetrační testy mohou probíhat ve dvou režimech (interní a externí penetrační testy).

Externí testy budou spočívat v simulaci útoku, při němž se útočník pokouší o průnik z internetu, nemá předběžné znalosti o IT infrastruktuře a nemá přístupové údaje k IT službám publikovaným do internetu. Testy budou probíhat v souladu s relevantními standardy a metodikami a např. OWASP, NIST SP 800-115, OSSTMM apod. Externí penetrační testování bude spočívat v simulaci napadení komponent systému útočníkem z vnějšího prostředí. Cílem testování bude zjistit, jaké informace lze získat z dostupných komponent, detekce zranitelností, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům a navrhnout doporučení k jejich odstranění. Skenování zranitelností je jen dílčím krokem v celkovém penetračním testování systému a jeho provedení nenaplnuje cíle penetračního testování. Testování se musí snažit i o nalezení a zneužití dalších, skenem zranitelností neidentifikovaných, součástí systému. Simulace také prověří systém z pohledu spolehlivosti, zajištění integrity a důvěrnosti dat. Testy jsou zaměřeny také na identifikaci bezpečnostních slabín, které se mohou vyskytovat v rámci instalace, konfigurace a procesů zpracování dat aplikace.

Interní testy se zaměří na prověření bezpečnosti systému v rámci jeho provozního prostředí. Simuluje počínání potenciálního útočníka, který se pokouší o napadení systému z počítače umístěného uvnitř interní sítě. Testy budou zaměřeny na:

- získání informací, identifikaci funkčních systémů,
- všeobecné testy zranitelnosti,
- charakteristiky infrastruktury systému,
- spolehlivost konfigurace,
- existenci backdoors,
- autentizaci a schémata pro kontrolu přístupu,
- kontrolu operačních systémů,
- aplikační chyby a vady v systému,
- nedostatečné provozní zabezpečení,
- slabá místa zahrnující body selhání, s cílem způsobit odmítnutí služeb webových aplikací,
- odposlechy komunikace se systémem,
- odchytení a přesměrování komunikace,
- zneužití odchytených informací a komunikace směrem k aplikačním službám (serverům),
- potencionální útoky na uživatele systému prostřednictvím tohoto systému.

Penetrační testy budou provedeny v souladu s požadavky aktuálních norem a platné legislativy, konkrétně jde o:

- Zákon o kybernetické bezpečnosti č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
- Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.
- Zákon č. 110/2019 o zpracování osobních údajů a Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (GDPR).
- Dodržení ČSN ISO 31000, ISO/IEC 27000, ISO/IEC 20000-1.

Veškeré testy budou prováděny bez destruktivních zásahů a nebude při jejich realizaci docházet k žádným změnám, které, by poškodily prověřovaný nástroj. Testy budou probíhat nad testovacími daty a v testovacím prostředí. Externí testy budou provedeny také v produkčním prostředí po uvedení nástroje do testovacího provozu.

Pro upřesnění uvádíme, že všechna ustanovení, uvedená v dokumentu "Zvláštní obchodní podmínky pro Zakázky v oblasti ICT", která se týkají penetračního testování jsou platná.

1.2 Typy testů použitých v projektu

Zodpovědnost za řízení a realizaci testů:

Typ testů	Prostředí	Řídí	Provádí	Součinnost	Výstupy
Systémové testy	Testovací prostředí Zadavatele	Dodavatel	Dodavatel	Zadavatel	Plány testování Protokoly z testování
Funkční uživatelské akceptační testy	Testovací prostředí Zadavatele	Zadavatel	Zadavatel	Dodavatel, třetí strany	Plány testování Akceptační testovací scénáře Protokoly z testování Akceptační protokoly
Integrační testy	Testovací prostředí Zadavatele, Produkční prostředí Zadavatele	Dodavatel	Dodavatel	Dodavatel, třetí strany, Zadavatel	Plány testování Akceptační testovací scénáře Protokoly z testování Akceptační protokoly
Nefunkční testy (Výkonnostní testy)	Produkční prostředí Zadavatele	Dodavatel	Dodavatel	Zadavatel	Plány testování Výstup z testování Akceptační protokoly
Bezpečnostní testy	Testovací/ produkční prostředí Zadavatele	Zadavatel	Zadavatel nebo jím určená třetí strana	Dodavatele	Plány testování Výstup z testování Akceptační protokoly

Tabulka 1 - Zodpovědnosti za řízení a realizaci testů

1.3 Podoba testovacích scénářů

Testovací scénáře budou vytvořeny ve formě dokumentu nebo dokumentů, které budou popisovat specifické kroky, datové vstupy a očekávané výstupy pro provedení testů IdM nástroje. Budou součástí Implementační analýzy. Obsah testovacích scénářů by měl být strukturovaný a podrobný, aby umožňoval opakovatelné a důkladné testování. Následující prvky musí být obsaženy v testovacích scénářích:

- **Název a identifikátor:** Každý testovací scénář by měl mít jedinečný název a identifikátor, který umožňuje snadnou identifikaci a sledování testů.
- **Popis scénáře:** Scénář by měl být popsán dostatečně jasně a srozumitelně, aby tester porozuměl cíli a účelu testu. Popis by měl zahrnovat informace o funkčnosti nebo části systému, která se testuje.
- **Předpoklady:** Předpoklady specifikují podmínky nebo nastavení, které musí být splněny před provedením testu. Mohou zahrnovat přítomnost určitého prostředí, dat nebo konfigurace.
- **Kroky testu:** Kroky testu popisují jednotlivé kroky, které musí tester provést, aby provedl test. Každý krok by měl být popsán dostatečně podrobně, včetně požadovaného vstupu, akce provedené testovatelem a očekávaného výstupu.
- **Vstupy:** Testovací scénáře by měly specifikovat vstupy, které se používají pro testování. Může se jednat o konkrétní data, hodnoty, soubory nebo jiné prvky potřebné pro provedení testu. Při stanovování vstupů bude Dodavatel vycházet z dat dostupných v současném řešení pro jednotlivé moduly.
- **Očekávané výstupy:** Scénář by měl popisovat očekávané výstupy nebo výsledky testu. Tyto výstupy slouží jako reference pro porovnání s výsledky skutečného testování.
- **Případné předpokládané chyby nebo problémy:** Testovací scénáře by měly také zahrnovat seznam možných chyb nebo problémů, které mohou nastat během provedení testu. To pomáhá testerovi připravit se na potenciální problémy a reagovat na ně adekvátně.
- **Předpokládaný výsledek:** Každý testovací scénář by měl mít jasně definovaný předpokládaný výsledek testu, který umožňuje porovnání s výsledky skutečného testování.
- **Testovací scénáře by měly být vytvořeny tak, aby pokrývaly různé aspekty systému a testovaly různé scénáře použití. Měly by být konzistentní, srozumitelné a důkladně otestované, aby zajistily správné fungování softwaru a splnění požadavků uživatelů.**

Testovací scénáře musí být vytvořeny, tak aby pokryly celý rozsah definovaných funkčních požadavků Zadávací dokumentací a současně musí být klíčové funkcionality nástroje IdM otestovány pro všechny zapojované systémy.