

1.1 Zátěžové testování

Předpokladem pro toto stádium testování je ukončení funkčních testů a „zamražení“ systému pro zátěžové testování. Toto stádium testování má podpořit systémové testování a poukázat na slabá místa systému, která nelze odhalit funkčními a integračními testy.

V rámci tohoto testování jsou realizovány výkonnostní testy a stress testy.

Role	<ul style="list-style-type: none">• Vedoucí testování Zhotovitele – zodpovídá za organizaci a řízení testů na straně Zhotovitele• Vedoucí projektu Zhotovitele – zodpovídá za zajištění zdrojů na straně Zhotovitele
Vstupy	<ul style="list-style-type: none">• Projektová dokumentace• Plán testů• Analýza pro zátěžové testování• Testovací data• Testovací scénáře• Protokol o provedení systémových testů
Výstupy	<ul style="list-style-type: none">• Výsledky zátěžového testování• Zpráva o zátěžovém testování

Tabulka 1 Přehled vstupů a výstupů ze stádia Zátěžové testování

1.1.1 Výkonnostní testy

Tyto testy mají prověřit výkonnost systému při očekávaném zatížení, které by mělo odpovídat běžnému provozu včetně prognózované pracovní špičky. Cílem je zaměřit se na chování systému hlavně v oblasti uživatelské odezvy systému, tj. ověřit výkonové parametry systému v souladu se smlouvou.

1.1.2 Stress testy

Tyto testy mají prověřit stabilitu systému a jeho schopnost zachovat se podle definovaných pravidel při simulaci extrémních situací, jako např.:

- schopnost systému zachovat si své funkce i během vygenerované maximální zátěže nad hranicí „bodu zlomu“, tj. v situaci kdy dochází k výkonovému přetížení systému, které není předpokládané při standardním provozu,
- schopnost systému zachovat se dle definovaných pravidel při simulovaném výpadku vybraných komponent systému (např.: jeden z aplikačních serverů, load balancer, databáze, síťová komunikace,...).

1.1.2.1 Vyhodnocení zátěžových testů a následný postup

Po každém běhu zátěžových testů vypracuje testovací tým výslednou zprávu o běhu testu, ve které vyhodnotí provedení běhu, případně navrhne úpravy aplikace, které mají zlepšit výkonnost systému. Po provedení všech naplánovaných běhů uvedených v harmonogramu zpracuje testovací tým výslednou Zprávu o zátěžových testech, kde je shrnut, vyhodnocen celý proces zátěžového testování a navrhnout následný postup.

Výsledná zpráva poskytuje informace o provedených zátěžových testech, o chování systému během testů díky naměřeným hodnotám a slouží jako podklad pro návrh dalšího postupu při odstraňování nedostatků a slabých

míst systému, které nebylo možné objevit funkčním testováním. Následný způsob řešení objevených nedostatků systému nebo optimalizace testovaného systému bude stanoven na základě dohody Zhotovitele s MPSV.

1.2 Bezpečnostní testování

Testování bezpečnosti systému bude prováděno podle relevantních oblastí metodiky OSSTMM (Open Source Security Testing Methodology Manual). Testování bude rozděleno do dvou hlavních částí. První část obsahuje otestování zranitelnosti systému z pohledu nepřátelského prostředí. Ve druhé části bude provedeno ověření implementace opatření požadovaných MPSV v rámci definice požadavků na dodávaný systém.

Role	<ul style="list-style-type: none"> Vedoucí testování Zhotovitele – zodpovídá za organizaci a řízení testů na straně Zhotovitele (funkční, testy výjimek, integrace z pozice Zhotovitele) Koordinátor testování MPSV – zodpovídá za organizaci a řízení testů na straně MPSV (integrační testy) Vedoucí projektu Zhotovitele – zodpovídá za zajištění zdrojů na straně Zhotovitele Vedoucí projektu MPSV - zodpovídá za zajištění zdrojů na straně MPSV Specialista na bezpečnostní testy – zodpovídá za provedení testů
Vstupy	<ul style="list-style-type: none"> Návrh architektury testování Plán testů Testovací scénáře a testovací případy
Výstupy	<ul style="list-style-type: none"> Zpráva o bezpečnostních testech Záznam výsledků testů

Tabulka 2 Přehled zodpovědných rolí, vstupů a výstupů pro Bezpečnostní testování

1.2.1 OSSTMM

Účelem použití testování bezpečnosti pomocí metodologie OSSTMM je zajištění důkladného otestování relevantních částí systému. Respektováním pravidel metodologie bude zajištěno minimalizování škod na testovaném systému.

Z metodologie OSSTMM jsou vybrány následující oblasti jako relevantní pro účely bezpečnostních testů: Internet Technology Security Testing (význam slova Internet bude pro testovaný systém představovat celé vnější prostředí z pohledu vlastního testovaného systému (např. Internet, WAN MPSV, WAN ČSSZ a pod.), nikoli pouze Internet, tak jak je standardně chápán)

1.2.2 Testy zranitelnosti

Cílem těchto testů je odhalení slabin realizovaného systému. Odhalení zranitelností systému bude provedeno zjištěním dostupných služeb, identifikováním zranitelnosti dostupných služeb, kontrolou konfigurace, pokusy o neautorizované přístupy a předkládáním neočekávaných vstupů.

Za součást identifikování slabin systému lze pokládat i testy simulující nesprávné chování uživatele. Tyto testy jsou součástí interní, funkční a akceptační fáze. Bližší informace jsou uvedeny v předchozích kapitolách.

Výsledkem testování bude podrobný přehled nalezených slabin systému a návrh nápravných opatření na odstranění těchto slabin. Testování bude provedeno na produkčním i testovacím prostředí, případně na dalších prostředích, budou-li v rámci konkrétního projektu realizována (školicí, zkušební, integrační, ...).

1.2.3 Soulad s požadavky

Cílem tohoto testu bude ověření implementace bezpečnostních požadavků. Výsledkem testování bude zdokumentování zjištěných rozporů a souladu s požadavky, včetně návrhu na změny.

Ověření souladu s požadavky bude provedeno na produkčním, záložním i testovacím prostředí.

1.2.4 Podmínky pro zahájení testů

Pro zahájení bezpečnostních testů je nutné, aby aplikace a systémy v testovaném prostředí byly po dobu bezpečnostních testů „zmrazeny“ a nebyly na nich vykonávány žádné změny nebo jiné než bezpečnostní testování.

Před zahájením testů musí být připraven dokument *Plán testů* včetně testovacích scénářů a testovacích případů.

1.2.5 Vyhodnocení a ukončení bezpečnostních testů

Ukončení bezpečnostních testů je podmíněno provedením všech naplánovaných testů a odstraněním všech kritických chyb.

Výsledky bezpečnostních testů budou shrnuty v závěrečném dokumentu *Zpráva o bezpečnostních testech*. Vlastní průběh testování bude zaznamenán v dokumentu *Záznam výsledků testů*.

1.2.6 Definice závažnosti bezpečnostní chyby

Pouze pro účely vyhodnocení bezpečnostních testů byly definice tříd neshody v kapitole 2.6 *Definice závažnosti funkčních chyb* upraveny následovně:

- **Kritická (Critical)** – systém neprovádí kontrolu, která byla definována v analýze; systém obsahuje chybu, která je zneužitelná vzdáleně; neprovádění kontroly má za následek získání neoprávněného přístupu; existuje snadná možnost obejít kontrolu, takže kontrola není provedena
- **Střední (Medium)** – systém kontrolu provádí pouze částečně; kontrola není prováděna vždy, kdy je to požadováno; systém obsahuje chybu, která je zneužitelná lokálně; existuje možnost obejít kontrolu, ale pouze při splnění jedné velmi specifické podmínky
- **Malá (Low)** – systém kontrolu provádí, nicméně existuje možnost jak kontrolu obejít; obejít kontrolu je náročné a vyžaduje splnění několika velmi specifických podmínek

Odstraňování nalezených neshod bude prováděno podle pravidel definovaných v kapitole 2.7 *Pravidla odstraňování chyb*.

1.3 Akceptační testování

Cílem akceptačního testování je ověřit správnou a bezchybnou funkčnost aplikace, která odpovídá schválenému zadání. Toto stádium testování slouží jako potvrzení, že předávaný systém odpovídá požadavkům a akceptačním kritériím podle zadání MPSV.

V tomto stádiu testování budou prováděny funkční testy, testy výjimek a integrační testy. V tomto stadiu budou dále provedeny další testy na kterých se shodnou strany Zhotovitele a MPSV.

Role	<ul style="list-style-type: none"> • Koordinátor testování MPSV – zodpovídá za organizaci a řízení testů na straně MPSV • Vedoucí projektu MPSV – zodpovídá za zajištění zdrojů na straně MPSV
------	--



Vstupy	<ul style="list-style-type: none">• Plán testů• Protokol o provedení systémových testů• Testovací scénáře, testovací případy• Data ze systémových testů
Výstupy	<ul style="list-style-type: none">• Záznam výsledků testů• Akceptační protokol za testování

Tabulka 3 Přehled vstupů a výstupů ze stádia Akceptační testování

1.3.1 Funkční testy

Bude ověřena funkčnost systému dle specifikovaných požadavků a testy budou probíhat na základě schválené testovací dokumentace (testovací případy, testovací scénáře, testovací data). Akceptační testování bude probíhat v testovacím prostředí MPSV.

1.3.2 Testy výjimek

Testování výjimek je simulace nesprávného chování uživatele.

1.3.3 Integroční testy

Tento typ testů má za úkol ověřit integraci subsystému dodávaného Zhotovitelem s okolními spolupracujícími systémy.

1.3.4 Podmínky pro akceptační testy

Akceptační testování je prováděno podle testovací dokumentace (testovací případy a testovací scénáře), která je vytvořena testovacím týmem Zhotovitele. Vytvořená testovací dokumentace je předložena ke schválení MPSV. Na akceptačním testování se podílí pracovníci Zhotovitele a MPSV. Testy provádějí pracovníci MPSV, pracovníci Zhotovitele jsou k dispozici pro konzultace.

1.3.4.1 Testovací prostředí pro akceptační testy

Testovací prostředí pro akceptační testy musí odpovídat konfiguraci pro dané prostředí.

1.3.4.2 Testovací data pro akceptační testy

Testovací data, která budou použita, musí být připravena v předem definované struktuře a rozsahu.

1.3.4.3 Vstupní podmínky pro začátek akceptačních testů

- Ukončení interních a systémových testů v požadovaném rozsahu (dokladováno protokolem),
- v případě integračních testů musí být tým informován o připravenosti spolupracujících aplikací a systémů,
- Zhotovitel dodá verzi aplikace a specifické dokumenty, které dokladují připravenost k zahájení testování.

1.3.4.4 Předpoklady pro ukončení akceptačních testů

V dokumentu *Plán testů* budou definovány podmínky pro ukončení akceptačního testování jako např.:

- byly provedeny všechny typy testů požadované ze strany MPSV pro dané stádium testování,
- aplikace neobsahuje žádné chyby se závažností Kritická a Velká,
- aplikace obsahuje maximálně 10 chyb závažnosti Střední a 20 chyb závažnosti Malá,
- je vyplněn Akceptační protokol za testování.

Výše uvedené body jsou pouze jako příklad akceptačních kritérií, definitivní znění akceptačních kritérií musí být stanoveno v dokumentu *Plán testů*, který musí schválit odpovědný pracovník MPSV a po schválení budou tato kritéria závazná.

V případě, že jsou splněna výše uvedená kritéria a účastníci schůzky se dohodnou na ukončení akceptačních testů, vyplní Koordinátor testování MPSV příslušné části Akceptačního protokolu za testování a přiloží k němu přílohy.

Výsledky o průběhu každého testu budou zaznamenány do dokumentu Záznam výsledků testů.

1.4 Definice závažnosti funkčních neshod aplikace

Při provádění jednotlivých testovacích scénářů dochází k porovnání skutečné reakce systému s reakcí očekávanou podle daného scénáře (v případě pevně definovaných testů) nebo očekávanou subjektivně (v případě volných testů). Pokud se skutečná reakce systému od očekávané reakce liší, je tento fakt označen jako **Neshoda**. Dalšími možnými důvody nesprávné očekávané reakce nebo nesprávné skutečné reakce systému jsou neshody vyplývající z chyby testovacího scénáře, chyby testovacích dat, chyby v nastavení prostředí, atd.

Klasifikaci neshody provádí a zaznamenává Tester při evidenci neshody. Její klasifikaci schvaluje ve stádiu Interních testů či Systémových testů Vedoucí testování Zhotovitele, ve stádiu Akceptačních testů Koordinátor testování MPSV a Vedoucí projektu MPSV a Zhotovitele. Při neshodné klasifikaci řeší problém Vedoucí projektu Zhotovitele a Vedoucí projektu MPSV.

Podle charakteru a závažnosti jsou neshody klasifikovány do jednotlivých tříd následujícím způsobem: (níže uvedené definice jednotlivých tříd neshod aplikace jsou stejné pro všechna stadia testů, tj. pro Interní, Systémové, Akceptační testy. Uvedené definice jsou popsány obecně, konkrétní specifikace musí být uvedena v dokumentu *Plán testů*.)

- **Změna** – Detekovaná neshoda není funkční chybou systému, systém reaguje vzhledem k zadání správně, nesprávná je v tomto případě očekávaná reakce. Hlavním důvodem nesprávné očekávané reakce je nepřesná znalost zadání ze strany hodnotitele nebo skutečná změna požadavků na systém oproti zadání např. zjištění chybějící nebo nevhodně navržené funkčnosti. Neshoda této třídy může vyústit v požadavek na změnu.
- **Chyba** – Neshoda je funkční chybou systému (očekávaná reakce systému je správná a skutečná reakce systému se od ní liší). Podle projevu a dopadů na systém jako celek se tato třída neshod dále dělí podle tzv. Závažnosti na:
 - **Kritická** - Neshoda má významný dopad na realizaci testu - testovací činnosti nemohou pokračovat bez opravy neshody. Neshoda výrazně ovlivňuje několik nebo všechny významné funkce systému, nelze pokračovat v procesech systému bez odstranění neshody.
 - **Velká** - Neshoda má nižší závažnost než „Kritická“ chyba. Neshoda způsobuje zakrytí některé dílčí funkčnosti, která nemůže být prověřena. Neshoda znemožňuje plně využít požadovanou funkčnost systému a má významný dopad na proces podporovaný funkcí systému. Neshoda se vyskytuje v omezeném rozsahu.
 - **Střední** - Neshoda se vyskytuje v kritickém procesu, ale je možné jej obejít využitím jiné funkce systému. Neshoda se může také vyskytovat v nekritickém procesu.
 - **Malá** - Neshoda má zanedbatelný dopad na procesy testovaného systému, většinou způsobuje odchylku požadovaného uživatelského rozhraní (jiný text, diakritika, odlišná informativní hlášení, poloha tlačítek atd.)

Chyby procesu testování jsou pouze přechodné (po jejich opravě je znovu proveden příslušný test vč. vyhodnocení a klasifikace výsledku). Odstranění chyb procesu testování probíhá zejména ve stádiu interních a systémových testů.

1.5 Pravidla pro odstraňování neshod

Odstraňování neshod se řídí níže uvedenými pravidly (která mohou být upřesněna v *Plánu testů*):

- **Kritické chyby** musí být opraveny a přetestovány ve stejném testovacím cyklu.



- **Velké a Střední chyby** musí být opraveny a ověřeny do konce daného stádia testů.
- **Malé chyby** musí být odstraněny podle dohody zúčastněných stran testování. Rozhodování o odstranění chyb této závažnosti je v kompetenci Vedoucího projektu. Do konce daného stádia testování musí být definován termín pro jejich odstranění.
- **Změnové neshody** jsou postoupeny jako vstup do změnového řízení.



Příloha A - Vzor popisu testovacího scénáře

Název testu

IDENTIFIKACE TESTU

IDTestu	
Předmět	
Autor	
Datum vytvoření	
Typ testu	
Testovací data	
Podmínky	

POPIS TESTU

.

POSTUP

Krok	Popis	Očekávaný výsledek
1		
2		
3		
4		
5		

OČEKÁVANÝ VÝSLEDEK



Příloha B - Vzor protokolu testování

Test (identifikátor, název)	<i>Komponenta A</i>	<i>Komponenta B</i>	<i>Komponenta C</i>	<i>Komponenta D</i>	<i>Komponenta E</i>

Komentář k výsledku testů

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Datum:

Testy provedl:

Potvrzení průběhu a výsledku testů za Zhotovitele:

Potvrzení průběhu a výsledku testů za MPSV:

