Metodika realizace penetračních testů

IS KII a VIS

OBSAH

Verze dokumentu

Verze dokumentu	Datum	Autor dokumentu revize / změny	Číslo jednací	Schválil
1	14.7.2021	Ing. Miroslav Starčevič	MF-33092/2019/7001-8	Mgr. Radoslav Bulíř

1 Obecná část

Tento dokument definuje metodiku plánování a provádění penetračních testů, která je specificky určena pro informační systémy kritické informační infrastruktury a významné informační systémy dle definice zákona o kybernetické bezpečnosti.

Metodika popisuje použité standardy, nástroje, organizaci testů, navrhuje harmonogram testů a stanovuje kritéria na kvalitu provedení penetračních testů.

Cílem penetračních testů je identifikovat zranitelnosti testovaných informačních systémů a určit míru jejich závažnosti. Vlastník (garant) systému pracuje s poskytnutými výsledky testování, odstraňuje identifikované nedostatky a realizuje nápravná opatření. Touto činností vlastník eliminuje identifikované hrozby a chrání přístup k informačnímu systému proti neautorizovaným subjektům.

Výsledky penetračního testů popisují stav bezpečnosti systému v daném prostředí a čase. Výsledky testů jsou závislé na množině použitých testů a provozních omezeních. Penetrační testy se plánují s ohledem na významná bezpečnostní rizika. Za účelem ověření účinnosti aplikovaných nápravných opatření, implementovaných na základě identifikovaných zranitelností, jsou penetrační testy opakovány.

1.1 Seznam předpisů

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Vyhláška č. 82/2018Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Směrnice č. 6/2019 ministra financí, Systém řízení bezpečnosti informací Ministerstva financí

1.2 Seznam zkratek a pojmů

1.2.1 Seznam zkratek

ICT – Informační a komunikační technologie

IS – informační systém

KBI – Kybernetický bezpečnostní incident

KBU – Kybernetická bezpečnostní událost

KII – Kritická informační infrastruktura

MF – Ministerstvo financí ČR

SŘBI – Systém řízení bezpečnosti informací

VoKB – vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

VIS – Významný informační systém

ZoKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

1.2.2 Seznam pojmů

Metodika - metodika penetračních testů IS KII a VIS

Prostředí – soubor technických a programových prostředků informačního systému, ve kterém probíhají penetrační testy

Emergency stav – stav informačního systému, kdy vlivem penetračního testování dojde k omezení služeb testovaného prostředí nebo k ohrožení fungování informačního systému

Exploit - krátký program, který umožňuje realizovat existující zranitelnost v softwaru a získat přístup k informačnímu systému nebo jinou výhodu

Exploitace - spuštění exploitu, realizace zranitelnosti

Service Desk (SD) - aplikace v prostředí umožňující správu požadavků mezi poskytovateli služeb a objednatelem.

Směrnice - směrnice č. 6/2019 ministra financí, Systém řízení bezpečnosti informací Ministerstva financí.

Doporučení vedoucí k odstranění nálezů – návrhy k odstranění zjištěných nedostatků při realizaci penetračního testování

Nápravná opatření – nápravná opatření vedoucí k odstranění zjištěných nedostatků vycházející z Doporučení vedoucí k odstranění nálezů

Zadavatel – Ministerstvo financí jako zadavatel veřejné zakázky na realizaci penetračního testování konkrétního informačního systému

Dodavatel – jako externí subjekt, který dodává službu penetračního testování

Simulace kybernetických bezpečnostních událostí (KBU) a incidentů (KBI)- technické a netechnické aktivity dodavatele a jejich přímo řízených subdodavatelů, které jsou svojí povahou podobné kontrolovaným kybernetickým útokům s tím, že se výslovně požaduje, aby tyto aktivity neměly ve vztahu ke sledovanému účelu nepřiměřeně destruktivní charakter.

Test / Penetrační test – časově omezená, věcně zaměřená a cílená činnost při realizaci penetračního testování

Testování / Penetrační testování – komplexní proces sestávající z jednotlivých testů a simulací KBU a KBI

2 Základní rámec penetračního testování

Penetrační testování je proces, při kterém dochází k identifikaci a prověření zranitelností, slabých míst podpůrných aktiv a procesů řízení provozu a bezpečnosti MF minimálně z hlediska důvěrnosti, integrity a dostupnosti nebo vydaných Varování nebo Reaktivních opatření dle §11 odst. 2 písm a) a b) ZoKB.

Identifikace a hodnocení rizik včetně návrhu a aplikace bezpečnostních opatření je základním krokem stanovení rozsahu penetračního testování informačního systému.

2.1 Role a odpovědnosti

Níže uvedené role provádí plánování, realizaci a vyhodnocení penetračních testů. Jednotlivé role a jejich povinnosti jsou definovány v souladu s Přílohou č. 2.2 a 2.3 Směrnice.

U penetračního testování nemusí být všechny role obsazeny nebo mohou být kumulovány.

2.1.1 Složení týmů při realizaci penetračního testování

Provedení penetračního testování je organizováno prostřednictvím dvou týmů:

- Koordinační tým - plánuje, organizuje, řídí a vyhodnocuje jednotlivé penetrační testování
- Realizační tým – realizuje penetrační testy

a) **Koordinační tým**

Vedoucí koordinačního týmu

Členy koordinačního týmu jsou:

- Garant primárního aktiva,
- Garant podpůrných aktiv,
- Projektový manažer informačního systému zadavatele,
- Projektový manažer dodavatele informačního systému,
- Vedoucí týmu dodavatele penetračního testování.

b) **Realizační tým**

Vedoucího týmu dodavatele penetračního testování

Členové realizačního týmu vykonávají činnosti dle požadavků Vedoucího týmu dodavatele penetračního testování. Přímá komunikace mezi členy realizačního týmu a členy koordinačního týmu je možná jen v rozsahu, který byl dohodnut a schválen Vedoucím koordinačního týmu.

Členové realizačního týmu zabezpečují činnosti v oblasti kybernetické bezpečnosti, správy informačního systému a dodávky služeb podpory informačního systému, provozu informačního systému a realizaci penetračního testování.

Kybernetická bezpečnost

- Architekt kybernetické bezpečnosti
- Vedoucí týmu bezpečnostního monitoringu

Správa informačního systému a dodávka služeb podpory informačního systému

- Projektový manažer informačního systému
- Projektový manažer dodavatele informačního systému
- Architekt dodavatele informačního systému

Provoz informačního systému

- Vedoucí týmu provozního monitoringu
- Provozovatel informačního systému

Realizace penetračního testování - povinné role

- Vedoucí týmu dodavatele penetračního testování
- Specialista - tester

2.1.2 Definice odpovědností a pravomocí jednotlivých rolí

a) **Vedoucí koordinačního týmu**

Vedoucím koordinačního týmu může být i Manažer kybernetické bezpečnosti (dále jen „Manažer“) a odpovídá za:

- schválení plánu a časového harmonogramu penetračního testování,
- dodržení plánu a časového harmonogramu penetračního testování,
- poskytnutí všech dostupných podkladů, informací a materiálů zadavatele dle harmonogramu,
- vedení a koordinaci činností koordinačních týmů (provádí pouze Manažer),
- přípravu dílčích zadání pro jednotlivé koordinační týmy (provádí pouze Manažer),
- svolání jednání koordinačního týmu,
- kontrolu vedení dokumentace průběhu penetračního testování,
- zajištění účasti pracovníků zadavatele k zabezpečení plynulého chodu penetračního testování,
- kontrolu dodržování účasti pracovníků zadavatele na penetračním testování,
- zadávání úkolů z koordinačního týmu na Vedoucího týmu dodavatele penetračního testování,
- převzetí a akceptaci protokolů za zadavatele,
- zastavení penetračního testování v případě Emergency stavu informačního systému.

b) **Garant primárního aktiva**

Garant primárního aktiva je odpovědný za:

- poskytnutí všech dostupných podkladů, informací a materiálů za spravované primární aktivum,

- návrh časového harmonogramu penetračního testování,
- návrh na zastavení penetračního testování v případě Emergency stavu informačního systému,
- komunikaci se subjekty, které informační systém využívají,
- návrh nápravných opatření.

c) **Garant podpůrných aktiv**

Garant podpůrných aktiv je odpovědný za:

- poskytnutí všech dostupných podkladů, informací a materiálů za spravované podpůrné aktivum,
- návrh časového harmonogramu penetračního testování,
- návrh na zastavení penetračního testování v případě Emergency stavu informačního systému,
- provozní a bezpečnostní monitoring,
- komunikaci s dodavateli služeb nebo servisních organizací, kteří spravují podpůrná aktiva,
- návrh nápravných opatření.

d) **Projektový manažer informačního systému zadavatele**

Projektový manažer informačního systému zadavatele je odpovědný za:

- poskytnutí všech dostupných podkladů, informací a materiálů za spravovaný informační systém,
- komunikaci s dodavateli informačního systému, kteří poskytují podporu informačního systému.

Projektový manažer informačního systému zadavatele koordinuje kroky s dodavatelem:

- v době realizace testování,
- po realizaci testování.

e) **Projektový manažer dodavatele informačního systému**

Projektový manažer dodavatele informačního systému je odpovědný za:

- poskytnutí všech dostupných podkladů, informací a materiálů za dodávaný informační systém,
- spolupráci na návrhu nápravných opatření.

Projektový manažer dodavatele informačního systému koordinuje kroky s MF:

- v době realizace testování,
- po realizaci testování.

f) **Vedoucí týmu dodavatele penetračního testování**

Vedoucí týmu dodavatele penetračního testování je zároveň Vedoucím realizačního týmu.

Vedoucí týmu dodavatele penetračního testování je odpovědný za:

- návrh plánu a časového harmonogramu penetračního testování,
- poskytnutí všech dostupných podkladů, informací a materiálů dodavatele dle harmonogramu a v souladu s definovaným rozsahem testování,
- vedení penetračních testů a koordinaci činnosti členů realizačního týmu za stranu dodavatele,
- přípravu dílčích zadání pro jednotlivé členy realizačního týmu,
- svolání jednání realizačního týmu,
- zajištění vedení dokumentace průběhu penetračního testování,
- zadávání úkolů stanovených koordinačním týmem členům realizačního týmu dodavatele,
- návrh nápravných opatření,
- podpis předávacích a akceptační protokolů všemi členy realizačního týmu dodavatele.

g) **Architekt kybernetické bezpečnosti**

Architekt kybernetické bezpečnosti je odpovědný za:

- návrh rozsahu testovaných prvků ICT a testovaných částí informačního systému,
- návrh nápravných opatření,

h) **Vedoucí týmu bezpečnostního monitoringu**

Vedoucí týmu bezpečnostního monitoringu je odpovědný za:

- realizaci monitoringu testovaných prvků ICT,
- vypracování informace z bezpečnostního monitoringu o identifikovaném penetračním testování,
- návrh zastavení testování v případě Emergency stavu,
- spolupráci na realizaci Emergency scénáře (viz kapitola 4.3.3)

i) **Architekt dodavatele informačního systému**

Architekt dodavatele informačního systému navrhuje:

- rozsah testovaných částí informačního systému,
- navrhuje nápravná opatření.

j) **Vedoucí týmu provozního monitoringu**

- vypracuje informace z provozního monitoringu o identifikovaném penetračním testování,
- navrhuje zastavení testování v případě Emergency stavu.

k) **Provozovatel informačního systému**

- spolupracuje na realizaci Emergency scénáře,
- zajišťuje provozní monitoring testovaného rozsahu informačního systému.

l) **Specialista – tester**

Počet a zaměření Specialistů testerů je závislý na rozsahu a konkrétních parametrech informačního systému, např. pro:

- platforma - Windows, Linux, Oracle, Solaris, IBM AIX,
- virtuální prostředí - VMware, Hyper-V, RHEVM,
- databáze - Oracle, MS SQL, Sybase, PostgreSQL, MySQL, Informix
- síťové prvky - Cisco IOS, NXOS, Brocade Network OS, Cisco Fabric OS,
- firewall Check Point a proxy SQUID

2.1.3 Změna osob při realizaci penetračního testování

Kterákoliv ze smluvních stran je oprávněna rozhodnout o změně osob, které jmenovala do organizační struktury penetračního testování. O této změně musí v dostatečném předstihu minimálně 7 kalendářních dní informovat druhou smluvní stranu.

2.1.4 Hierarchická matice řízení testování

Koordinační tým				
Vedoucí koordinačního týmu - Manažer kybernetické bezpečnosti				
Garant primárního aktiva	**Garant podpůrných aktiv**	Projektový manažer informačního systému zadavatele	Projektový manažer dodavatele informačního systému	Vedoucí týmu dodavatele penetračního testování

Realizační tým					
Vedoucí týmu dodavatele penetračního testování					
Architekt kybernetické bezpečnosti	**Vedoucí týmu bezpečnostního monitoringu**	**Vedoucí týmu provozního monitoringu**	Projektový manažer informačního systému zadavatele	Specialista – tester	Provozovatel informačního systému

Červeně označené role mají právo v případě Emergency stavu informačního systému **navrhnout** zastavení testování.

Červeno-černě označená role má právo v případě Emergency stavu informačního systému **zastavit** testování.

2.1.5 RACI matice činností a odpovědností

Fáze	Činnosti	Role										
		Vedoucí koordinačního týmu	Architekt	Garant primárního aktiva	Garanti podpůrných aktiv	Projektový manažer informačního systému zadavatele	Projektový manažer dodavatele informačního systému	Vedoucí týmu dodavatele penetračního testování	Vedoucí týmu provozního monitoringu	Vedoucí týmu bezpečnostního monitoringu	Výbor pro řízení kybernetické bezpečnosti MF	Osoba odpovědná za zadávání VZ
Plánování	Vytvoření celkového plánu testování	A	R	R	R	R						
	Schválení plánu penetračního testování	R		R							A	
Definice rozsahu testování	Definice rozsahu testování	A	R	R	R	R	R	R	C	C		I
	Výběr dodavatele penetračního testování	R	R									A
Předání podkladů	Svolání koordinačního týmu	A		I	I		I					
	Definice harmonogramu realizace testu	R	R	C	C	C	C	A	C	C		I
	Souhlas s prováděním penetračních testů a simulací	A	C	C	C	C	C	R	C	C		I
	Kontrola funkčnosti cílových a monitorovacích systémů	A	I	I	R	C	C	I	R	R		
Realizace	Informace o začátku testování	I		I	I	I	I	A	I	I		
	Vedení dokumentace průběhu testování	C	C		C	C		A	C	C		
	Změna v průběhu testování	A	C	R	R	R	R	R				I
	Návrh na spuštění Emergency scénáře	A		R	R	I	I	R	R	R		
	Rozhodnutí o spuštění Emergency scénáře	A		C	C	I	I	R	C	C		I

Vyhodnocení a akceptace	Sumarizace podkladů a vytvoření Návrhu zprávy z penetračního testování	I	C	C	R	C	C	A	R	R		
	Připomínky k návrhu zprávy	A	C	R	R	R	R	R	R	R		I
	Vypořádání a Akceptace	R	I	R	R	R	I	A	C	C		R
	Seznam doporučení vedoucí k odstranění nálezů	A	R	R	R	R	R		C	C	I	
	Kontrola nápravných opatření	A	R	C	C	C	C					

- **R** - Responsible - kdo je odpovědný za vykonání dílčí činnosti svěřeného úkolu
- **A** - Accountable (někdy též Approver) - kdo je odpovědný za realizaci celého úkolu, je odpovědný za to, co je vykonáno – výsledek
- **C** - Consulted - kdo může poskytnout cennou radu či konzultaci k úkolu
- **I** - Informed - kdo má být informován o průběhu úkolu

2.2 Metodiky a frameworky

2.2.1 NIST SP 800-115

Norma NIST SP 800-115 zahrnuje pokyny, jak provádět sebehodnocení, podrobnosti o řízení rizik v dodavatelském řetězci, pokyny, jak komunikovat se zúčastněnými stranami dodavatelského řetězce a podporuje proces zveřejňování zranitelností.

2.2.2 OWASP

Open Web Application Security Project (dále jen „OWASP“) pokrývá testování webových aplikací včetně infrastruktury webových aplikací a částečně konfiguraci webových serverů, které spadají do oblasti konfiguračních testů.

2.2.3 ISECOM - OSSTMM

Standard Open Source Security Testing Methodology Manual (dále jen „OSSTMM“) je zastřešen institutem ISECOM (Institute for Security and Open Methodologies) a klade důraz na přípravu a formální ohodnocení penetračního testování.

2.2.4 OSINT

Open-Source INTelligence (dále jen „OSINT“) je framework pro shromažďování dat z veřejně dostupných zdrojů, která mají být použita pro penetrační testování.

2.3 Časový rámec testování

2.3.1 Dlouhodobý plán penetračního testování IS MF

- Celkový plán testování – časový rámec pro realizaci všech penetračních testování u všech informačních systémů.
- Penetrační testování KII – doba opakování penetračních testování v celém rozsahu jednoho IS – KII. Je doporučeno 1x za 3 roky.
- Penetrační testování VIS – doba opakování penetračních testování v celém rozsahu jednoho IS – VIS. Je doporučeno 1x za 5 let.
- Penetrační testování provozních IS – doba opakování penetračních testování v celém rozsahu jednoho provozního IS. Je doporučeno 1x za 5 let.

2.3.2 Časové úseky realizace jednotlivého penetračního testování IS

- Stanovení členů jednotlivých týmů (Příloha č. 1).
- Stanovení komunikační matice včetně Emergency matice (Příloha č. 2).
- Definice rozsahu testování – seznámení se s relevantní zákonnou a smluvní povinností zadavatele a stanovení cíle testování, jeho rozsahu a Emergency scénářů (Příloha č. 3).
- Převzetí podkladů – zadavatel dodavateli odevzdá všechny vyžádané podklady včetně Souhlasu s provedením penetračního testování (Příloha č. 4).
- Stanovení harmonogramu penetračního testování (Příloha č. 5).
- Realizace testování
    - Testy – doba, kdy jsou realizovány vlastní testy.
    - Vyhodnocení výstupů z testů – doba, kdy dochází k auditní sumarizaci všech postupů, nálezů. Následně je zadavateli předán Návrh zprávy z penetračního testování (Příloha č. 6).
- Vypořádání a akceptace nálezů – doba do odevzdání konečné Zprávy z penetračního testování a návrhu na bezpečnostní opatření.
- Uzavření testování a opatření – přijetí bezpečnostních opatření ze zjištěných nálezů.

2.4 Identifikace rozsahu infrastruktury a informačního systému

Níže uvedené prvky ICT definují rozsah infrastruktury a informační systém, který má být předmětem penetračního testování. Při plánování a definici penetračního testování jsou definovány jednotlivé oblasti, které se mají otestovat. Je to soubor fyzických, hardwarových a softwarových prvků realizující informační systém.

Veškeré informace jsou součástí provozní popř. bezpečnostní dokumentace jednotlivých prvků ICT.

2.4.1 Identifikace prostředí a rozsahu jednotlivých vrstev pro testování

a) **Základní oblast**

- budovy, kde jsou umístěny prvky ICT informačního systému
- technologické místnosti a serverovny
- elektřina a UPS
- fyzické zabezpečení technologických místností a serverovny
- regulace teploty a protipožární systém

b) **Fyzická oblast**

- metalická infrastruktura uvnitř technologických místností, serveroven nebo objektů
- optická infrastruktura uvnitř technologických místností, serveroven nebo objektů
- vstupy/výstupy komunikačních linek providerů nebo pronajatých linek
- bezdrátová infrastruktura uvnitř nebo vně objektů

c) **Linková oblast**

- převodníky a čidla (non IT)
- L2 switche
- media convertory
- bezdrátové přijímače/vysílače

d) **Síťová oblast**

- DDoS protectory
- firewally
- L3 switche / core
- routery
- VLANy

e) **Transportní oblast**

- loadbalancery
- prostředky HA/Geocluster
- aplikační firewally
- použití nešifrovaných a šifrovaných protokolů
- použití nestandartních a standartních portů

f) **Relační oblast**

- dedikované fyzické servery
- virtualizační hardwarové servery
- virtualizační softwarová platforma
- dedikovaná disková pole
- SAN včetně diskových polí
- podpůrné servery (DHCP/DNS/AD)
- HSM moduly

g) **Prezentační oblast**

- operační systémy umístěné na hardwarovém prostředí
- databázové systémy umístěné na hardwarovém prostředí
- file systémy umístěné na hardwarovém prostředí
- operační systémy umístěné ve virtuálním prostředí
- databázové systémy umístěné ve virtuálním prostředí
- file systémy umístěné ve virtuálním prostředí

h) **Aplikační oblast**

- aplikační servery
- prezentační servery
- ověření uživatelů a identity management

i) **Datová oblast**

- ekonomická data
- agendová data
- osobní data
- data uživatelských účtů
- provozní a bezpečnostní data a logy

j) **Bezpečnostní oblast**

- provozní dokumentace
- bezpečnostní dokumentace
- dokumentace veřejné zakázky a smlouvy
- konfigurační databáze
- definice rolí a odpovědností provozu a rozvoje IS
- provozní monitoring
- bezpečnostní monitoring
- zálohování a DRP

2.4.2 Adresní rozsahy

a) **Externí adresní rozsahy**

- veřejné IP adresy
- neveřejné IP adresy na externím DMZ perimetru
- komunikační protokoly určené pro externí komunikaci
- komunikační porty určené pro externí komunikaci
- dodavatelé externí konektivity

b) **Interní adresní rozsahy jednotlivých prvků ICT**

- interní IP adresy na vstupu

- interní IP adresy na výstupu
- komunikační protokoly určené pro interní komunikaci
- komunikační porty určené pro interní komunikaci
- správci interní konektivity

2.4.3 Identifikace platforem

Výčet všech platforem nelze taxativně určit, vychází se zejména z konkrétních aplikovaných prvků ICT v oblastech:

- webové služby
- operační systémy - Windows, Linux, Oracle, Solaris, IBM AIX
- virtuální prostředí - VMware, Hyper-V, RHEVM
- databáze - Oracle, MS SQL, Sybase, PostgreSQL, MySQL, Informix
- síťové prvky - Cisco IOS, NXOS, Brocade Network OS, Cisco Fabric OS
- firewall Check Point a proxy SQUID

2.4.4 Dopady na propojené informační systémy

V rámci stanovení rozsahu IS je vytvořen soupis informačních systémů a prvků ICT, na které může mít penetrační testování vliv. V tomto soupisu jsou uvedena propojení na další IS, se kterými testovaný systém komunikuje. Soupis je vytvořen v případě selhání testovaného systému a zabezpečení následného chodu IS. Jedná se především o:

- soupis propojených informačních systémů,
- soupis kontaktů na správce propojených informačních systémů,
- podmínky propojení informačních systémů,
- podmínky provozu testovaného informačního systému,
- podmínky poskytování služeb informačního pro veřejnost,
- definice časových omezení realizace penetračního testování,
- napojení na provozní monitoring,
- napojení na bezpečnostní monitoring.

2.5 Požadavky na smluvní podmínky

V případě uzavření smlouvy s dodavatelem služby penetračního testování musí být definovány příslušné požadavky, které budou předmětem zadání veřejné zakázky.

2.5.1 Požadavky na Dohodu o mlčenlivosti

Základní požadavky na Dohodu o mlčenlivosti (dále jen „NDA“) jsou:

- požadavky na rozsah a formu předání a použití podkladů,
- požadavky na rozsah a formu předání výstupů,
- požadavky na likvidaci předaných podkladů a odevzdaných výstupů.

2.5.2 Požadavky na Úroveň poskytovaných služeb

Požadavky na úroveň poskytovaných služeb (dále jen „SLA“) se upřesňují při definici jednotlivých penetračních testování konkrétního informačního systému.

2.5.3 Požadavky na komunikaci v průběhu testování

Základní požadavky na komunikaci v průběhu testování jsou:

- komunikační matice koordinačního týmu,
- komunikační matice realizačního týmu,
- nastavení komunikace při Emergency scénářích.

2.5.4 Odbornost zástupců dodavatele v koordinačním a v realizačním týmu

Základní požadavky na zástupce dodavatele v koordinačním a realizačním týmu musí být neoddělitelnou součástí smluvního ujednání.

2.5.5 Požadavky na sankce

Neoddělitelnou součástí smluvního ujednání jsou v minimálním rozsahu sankce za:

- nedodržení harmonogramu penetračního testování,
- nedodání výstupů v požadovaném termínu a kvalitě,
- neoprávněné nakládání s předanou dokumentací,
- nedodržení komunikace při řešení Emergency stavů.

2.6 Identifikace účelu

2.6.1 Identifikace požadovaného účelu testování

Účel testování vychází z VoKB. Jedná se zejména o:

- testování při uvedení informačního systému do provozu,
- testování při změně prvku ICT, který je podpůrným aktivem informačního systému,
- testování při pravidelném ověřování nápravných nebo technických opatření.

2.6.2 Identifikace míry bezpečnosti na procesy organizace

Před vlastním zadáním penetračního testování musí být definováno především:

- nastavení rozsahu testování
    - zaměřenost - rozsah je určen konkrétně vymezenou částí prvků ICT,
    - omezenost - omezen na vybrané systémy, definicí části informačního systému, nebo může být vymezen i na více systémů uskupené do logického celku,
    - úplnost - test pokrývá všechny vymezené a dostupné systémy, včetně částí, které jsou záměrně vyjmuty z testování,
- nastavení informovanosti
    - provozního monitoringu,

  - bezpečnostního monitoringu,
- nastavení míry, kdy je přerušeno testování z důvodu nadměrného zatížení prvku ICT
- nastavení doby nebo časového úseku, kdy jsou realizovány zálohy nastavení nebo dat každého prvku ICT,
- nastavení informovanosti správců propojených informačních systémů,
- nastavení omezení služeb pro uživatele a systémy,
- nastavení nakládání s citlivými informacemi,
- nastavení požadavku na uchování důkazů.

2.7 Podmínky testování

2.7.1 Stanovení členů jednotlivých týmů a komunikační matice

Stanovení členů jednotlivých týmů a komunikační matice musí být vytvořeno při zadání penetračního testování. Jedná se o všechny úrovně a to jak organizační a testovací, tak tzv. informační a Emergency. S těmito kontakty je nutné nastavit frekvence realizace jednotlivých komunikací včetně formy. Jedná se především o:

- obsazení jednotlivých rolí v průběhu testování,
- Emergency kontakty pro spuštění Emergency scénáře (Příloha č. 2),
- report incidentů jednotlivých prvků ICT a informačního systému,
- definice zabezpečení komunikace
  - telefon,
  - e-mail,
  - ServiceDesk,
- plán a řízení schůzek a pravidelné informování zadavatele o realizovaném penetračním testování.

2.7.2 Work Breakdown Structure a pravidla testování

Pro naplánování každého penetračního testování musí být vytvořeno:

- rozložení testování na jednotlivé činnosti,
- definice harmonogramu a milníků testování,
- odpovědnosti za jednotlivé činnosti,
- povolené a vyloučené doby testování,
- výkonové omezení nebo omezení zátěže jednotlivých prvků ICT.

2.7.3 Definice součinnosti zadavatele a dodavatele

Pro vlastní realizaci testování je nutné definovat součinnostní kroky, které především obsahují:

- rozsah a přístupová oprávnění pro testery,
- fyzický přístup k jednotlivým prvkům ICT,
- přístup do prostor zadavatele nebo provozovatelů informačních systémů zadavatele,

- zdrojové IP adresy testerů.

2.7.4 Agresivita testování

Agresivita testování udává úroveň narušení testovaného systému:

- striktně pasivní - minimální úroveň narušení testovaného systému, kdy tester nevytváří s testovaným systémem žádné interakce a jen pozoruje chování systému nebo odposlouchává jeho síťový provoz; v tomto režimu nelze ověřit zranitelnost;
- opatrná - úroveň narušení testovaného systému představuje ověření zranitelností jen v těch případech, kdy tester usoudí, že realizace zranitelnosti nezpůsobí žádnou škodu, například jde o pokus autentizace s implicitním heslem nebo přístup k adresáři na webovém serveru;
- cílená - úroveň narušení testovaného systému umožňuje cíleně ověřit vybrané zranitelnosti za předpokladu, že exploit je podle dostupných informací funkční pro cílovou verzi zranitelného softwaru a pravděpodobnost úspěšné exploitace je vysoká a bez vážných následků poškození;
- úplná penetrace - tester se snaží exploitovat všechny potencionální zranitelnosti a to i v případě, kdy přesné verze softwaru na cílových systémech nejsou známy.

2.8 Použití testovacích nástrojů

2.8.1 Automatické nástroje

Během testování prostředí IS je dovoleno testovat pouze automatizovanými nástroji maximálně do objemu 50% všech testů.
Použití automatizovaných nástrojů jako doplněk k ověření výsledků manuálního testování je dovoleno.

2.8.2 Nepovolené nástroje

Je zakázáno použití jakékoli funkcionality nástrojů, které odesílají data mimo prostředí IS (např. odesílání dat k analýze na externí servery dodavatele). V případě, že nástroje tuto funkcionalitu mají, musí se funkcionalita odeslání dat zakázat a toto nastavení musí být ověřeno v celém průběhu penetračního testování. Nelze-li funkcionalitu odesílání dat zakázat, není použití takového nástroje přípustné.

2.8.3 Seznam povolených testovacích nástrojů

Seznam povolených testovacích nástrojů je uveden v Příloze č. 7

2.9 Kontrola funkčnosti testovaných a monitorovacích systémů

Před realizací penetračního testování je provedena kontrola funkčnosti testovaných informačních systémů a provozních a bezpečnostních monitorovacích systémů. Za každou

kontrolu odpovídají jednotlivé role v koordinačním a realizačním týmu v rámci jejich standardních pracovních činností.

Před vlastním penetračním testování musí být realizovány následující kontroly:

- kontrola funkčnosti jednotlivých testovaných prvků ICT,
- kontrola nástrojů a procesů ochrany prvků ICT,
- kontrola nástrojů provozního monitoringu a realizace provozních incidentů,
- kontrola nástrojů bezpečnostního monitoringu a realizace KBU a KBI,
- kontrola realizace a aktuálnosti záloh, obnovy a archivace,
- kontrola nastavení přístupových oprávnění,
- kontrola specifických opatření ochrany.

2.10 Definice cílů a základních podmínek realizace penetračního testování

Zadavatel definuje cíle a základní podmínky realizace penetračního testování. Penetrační testování a realizace jednotlivých testů má za cíl simulovat napadení informačního systému útočníkem.

Definice dílčích cílů Zadavatelem se prování za účelem upřesnění způsobů a podmínek realizace simulovaného útoku tak, aby celý proces penetračního testování byl řízen.

2.10.1 Role uživatelských účtů

Cílem je kompromitace, převzetí nebo vytvoření jednotlivých druhů uživatelských rolí. Základní rozdělení druhů těchto rolí je:

- privilegované role – cílem je kompromitace privilegovaných nebo administrátorských účtů s nejvyššími oprávněními a jejich další využití v penetračních testech,
- specifické role – cílem je kompromitace specifických uživatelských účtů, které mají vyšší nebo schvalovací oprávnění v informačním systému,
- uživatelské role - cílem je kompromitace běžných uživatelských účtů.

2.10.2 Způsob penetračního testování

Cílem je stanovení způsobu nebo kombinace způsobů provedení penetračního testování. Základní způsoby realizace jsou:

- elektronické – cílem je využití elektronických nástrojů a různých komunikačních prostředků pro realizaci testování,
- fyzické - cílem je provedení testování fyzických prostor na místě,
- sociální inženýrství – cílem je využití sociálního inženýrství nebo komunikace s lidmi k získání potřebných informací.

2.10.3 Viditelnost testování

Cílem je stanovení, jakým způsobem penetrační tester skryje svou identitu a kroky při realizaci jednotlivých testů. Pro Zadavatele je toto stanovení důležité k ověření, jak reagují monitorovací systémy včetně eskalačních procedur. Způsoby testování jsou:

- skryté - v testu se používají metody, které nejsou jednoznačně identifikovatelné jako útok,
- otevřené - test je vykonáván bez snahy skrýt aktivitu.

2.10.4 Vstupní bod

Cílem je stanovení vstupního bodu, který určuje počátek realizace penetračního testování nebo připojení penetračního testera do sítě a rozlišuje se:

- externí - test probíhá z veřejné sítě,
- interní - test probíhá z vnitřní sítě.

2.10.5 Informační báze

Informační báze specifikuje, jakou má tester počáteční znalost o informačním systému, který je předmětem testování.

- black box - tester nemá žádnou počáteční znalost o testovaném informačním systému a tento způsob provedení testu simuluje reálný útok,
- white box - tester má úplnou znalost prostředí IS včetně architektury sítě, funkcionality aplikace nebo přístupu ke zdrojovému kódu aplikace, a tento způsob provedení testu má za cíl ověřit veškeré možné zranitelnosti informačního systému,
- gray box - tester má částečnou znalost nebo omezený přístup do systému. Jedná se o kombinaci obou předchozích přístupů.

2.11 Souhlas s prováděním penetračních testů a simulací

Před vlastní realizací penetračního testování je dodavateli penetračního testování udělen souhlas s prováděním penetračních testů a simulací. Tento souhlas uděluje Manažer. Vzor souhlasu je v Příloze č. 4.

Souhlas obsahuje vždy:

- identifikaci osoby, která uděluje souhlas,
- identifikaci subjektu (dodavatele), kterému je souhlas udělován,
- informace o čísle smlouvy, kterou je penetrační testování realizováno,
- definici cílů nebo předmětu penetračního testování,
- definici účelu penetračního testování ,
- datum a čas začátku a konce realizace penetračního testování,
- podpisy obou stran.

3 Celkový plán penetračního testování

3.1 Návrh celkového plánu penetračního testování

Na začátku kalendářního roku Manažer ve spolupráci se všemi garanty primárních a podpůrných aktiv zpracuje návrh celkového plánu penetračního testování pro aktuální kalendářní rok.

Garanti primárních aktiv poskytují podporu při plánování jednotlivých termínů penetračních testování tak, aby nedocházelo k souběhu u důležitých činností a v agendách, které informační systém podporuje.

Manažer navržené termíny přenese do celkového plánu penetračního testování na příslušný rok a předkládá ho ke schválení Výboru pro řízení kybernetické bezpečnosti MF.

3.2 Schválení celkového plánu penetračního testování

Výbor pro řízení kybernetické bezpečnosti MF na svém jednání schválí celkový plán penetračního testování na příslušný rok, popřípadě dá podnět k jeho změně. Tato změna musí být projednána s příslušnými garanty primárních aktiv.

3.3 Změna schváleného celkového plánu penetračního testování

Pokud je v aktuálním roce potřeba změny nebo realizace dalšího penetračního testování mimo schválený celkový plán penetračního testování navrhne Manažer Výboru pro řízení kybernetické bezpečnosti MF tuto změnu. Tato změna musí být projednána s příslušnými garanty primárních aktiv. Výbor pro řízení kybernetické bezpečnosti MF na svém nejbližším jednání tuto změnu schválí do celkového plánu penetračního testování pro aktuální rok.

4 Průběh jednotlivého penetračního testování

4.1 Fáze a organizace průběhu jednotlivého testování

4.1.1 Definice rozsahu testování

Manažer ve spolupráci s Architektem a garanty primárních a podpůrných aktiv definuje požadavky, které slouží jako podklad pro zadání veřejné zakázky. Z definice cílů a základních podmínek realizace penetračního testování (dle kapitoly 2.10) Manažer zpracuje dokument Definice rozsahu testování (Příloha č. 3) a předá jej útvaru odpovědnému za přípravu veřejné zakázky.

Mezi základní údaje v Definici rozsahu testování patří:

a) Identifikace rozsahu testovaného informačního systému pro stanovení pracnosti, a to minimálně v rozsahu dle jednotlivých scénářů, které se mohou lišit dle jednotlivých frameworků. Rozsah testovaného informačního systému je v souladu s kapitolou 2 této metodiky.
b) Časový rámec penetračního testování.
c) Definice komunikace na straně zadavatele:
    a. Emergency kontakty (Příloha č. 2)
    b. incident reporting procesy (identifikace incidentu, vyhodnocovací míra dopadu)
    c. frekvence status reportů
    d. způsoby zabezpečení komunikace
    e. pravidla výměny dat ve vztahu ke třetím stranám a k NDA
    f. pravidla status schůzek (plán, identifikace postupu)
    g. eskalační pravidla.
d) Pravidla realizace testování:
    a. návrh harmonogramu za zadavatele
    b. odpovědnost za jednotlivé testy
    c. pravidla pro přerušení, zastavení a Emergency stav při testování a break-stop (povolené nebo vyloučené doby testování, výkonová omezení nebo omezení zátěže)
    d. testované prostředí IS a lokality
    e. přístup k fyzické infrastruktuře
    f. dálkový přístup
    g. řízení exploatace.
e) Požadavky na dodavatele:
    a. požadavky na nakládání s citlivými informacemi - NDA
    b. požadavky na uchování důkazů
    c. požadavky na úroveň poskytnutých služeb – SLA.
f) Definice součinnosti zadavatele a dodavatele:
    a. přístupová oprávnění pro dodavatele
    b. přístup k infrastruktuře pro dodavatele
    c. přístup do prostor zadavatele popřípadě do prostor provozovatele testovaného IS
    d. přístup k prvkům ICT informačního systému zadavatele a popřípadě provozovatele testovaného IS.
g) Požadavky na získávání informací:
    a. pravidla výběru cílů testování
        i. privilegovaní uživatelé (např. administrátoři a správci sítí, vedoucí zaměstnanci)
        ii. uživatelé specifických rolí (např. dodavatel testovaného IS, sekretářky, personalisti, účetní apod.)

iii. běžní uživatelé
b. sociotechnické testování (např. phishing, pharming)
c. vytěžování informací z veřejně dostupných zdrojů (OSINT)
i. o ministerstvu
ii. o zaměstnancích včetně osobních údajů.

h) Pravidla hodnocení výstupů z penetračního testování

4.1.2 Zadávání jednotlivých veřejných zakázek penetračního testování

Zadávání jednotlivých veřejných zakázek je v souladu se schváleným celkovým plánem penetračního testování dle kapitoly 3.2.

Útvar odpovědný za přípravu veřejné zakázky spolupracuje s Architektem na zadávání jednotlivých veřejných zakázek a výběru dodavatele.

4.1.3 První svolání koordinačního týmu

Vedoucí koordinačního týmu svolá po výběru dodavatele koordinační tým, na kterém předá Vedoucímu týmu dodavatele penetračního testování Definici rozsahu penetračního testování (viz Příloha č. 3). Ze strany dodavatele může dojít k požadavku na doplnění rozsahu předaných informací.

Na jednání koordinačního týmu jsou vzájemně dohodnuty konkrétní komunikační matice, návrh harmonogramu a technické prostředky potřebné k realizaci penetračního testování.

Na základě jednání koordinačního týmu Vedoucí týmu dodavatele penetračního testování ve spolupráci s Vedoucím koordinačního týmu a Architektem vytvoří finální harmonogram realizace penetračního testování, který je součástí zápisu z jednání koordinačního týmu.

Vedoucí koordinačního týmu Vedoucímu týmu dodavatele penetračního testování předá souhlas s provedením testu (viz Příloha č. 4).

Vedoucí koordinačního týmu vyzve všechny garanty podpůrných aktiv a monitorovacích systémů, aby před testováním provedli kontrolu funkčnosti testovaných IS a monitorovacích systémů (v souladu se kapitolou 2.9 této metodiky).

Od stanoveného termínu a v souladu se schváleným harmonogramem musí Vedoucí týmu dodavatele penetračního testování zajistit realizaci penetračního testování.

4.1.4 Realizace

Vedoucí týmu dodavatele penetračního testování informuje všechny členy koordinačního týmu o začátku testování.

Vedoucí koordinačního týmu informuje Emergency kontakty o počátku testování.

Vedoucí týmu dodavatele penetračního testování zajišťuje provedení penetračního testování a zejména:

a) dodržuje harmonogram průběhu testování,

b) dodržuje definici rozsahu a cíle testování,
c) průběžně informuje Vedoucí koordinačního týmu o stavu testování,
d) v případě, že dojde vlivem testování k omezení služeb testovaného prostředí IS (Emergency stav), podá ihned Vedoucí koordinačního týmu návrh k přerušení testování.

4.1.5 Ukončení

Vedoucí týmu dodavatele penetračního testování informuje všechny členy koordinačního týmu o ukončení testování.

Vedoucí koordinačního týmu informuje Emergency kontakty o ukončení testování.

Vedoucí týmu dodavatele penetračního testování vyžádá od jednotlivých členů realizačního týmu dokumentaci průběhu testování a zapracuje do Návrhu zprávy z penetračního testování (Příloha č. 6)

4.2 Dokumentace průběhu testování

V průběhu testování Vedoucí týmu dodavatele penetračního testování odpovídá za vedení příslušné dokumentace.

Všichni členové realizačního týmu dávají Vedoucímu týmu dodavatele penetračního testování podklady pro tvorbu dokumentace. Rozsah dokumentace vedené v průběhu testování obsahuje minimálně:

a) popis použitých testovacích metod,
b) popis vstupních bodů a zdrojových adres testování,
c) popis jednotlivých cílů testování včetně topologie testované sítě,
d) popis rozsahu testování,
e) popis realizace testování
    a. identifikace cílů,
    b. průběh řešení,
    c. seznam použitých nástrojů u konkrétního penetračního testu,
f) popis neshod a výstupy z testování
    a. index nálezů,
    b. zjištění včetně popisu důkazů a příloh z použitých nástrojů,
    c. návrh doporučení vedoucí k odstranění nálezu,
g) popis komunikace realizačního a koordinačního týmu,
h) popis použití Emergency scénáře a přerušení testování,
i) popis provozního a bezpečnostního monitoringu.

4.3 Změny v průběhu testování

4.3.1 Organizační změny

Organizační změny, které mohou nastat v průběhu testování, jsou vždy hlášeny od všech členů obou týmů Vedoucímu koordinačního týmu.

Změna je definována jako:

a) změna rozsahu testování,
b) změna harmonogramu,
c) změna zvoleného scénáře,
d) změna požadovaného účelu testování,
e) změna členů týmů,
f) změna způsobu komunikace,
g) změna komunikační matice,
h) změna incident reporting procesů (identifikace incidentu, vyhodnocovací míra dopadu),
i) změna frekvence statusu a reportů,
j) změna způsobu zabezpečení komunikace,
k) změna pravidel nebo statusu schůzek (plán, identifikace postupu),
l) změna eskalačních pravidel,
m) změna Emergency kontaktů,
n) další změny ovlivňující realizaci testu.

4.3.2 Schválení změny

Veškeré změny v průběhu testování musí být schváleny Koordinačním týmem.

Nelze schválit změny, které mají vliv na předmět nebo realizaci veřejné zakázky.

Vedoucí koordinačního týmu následně informuje Vedoucího týmu dodavatele penetračního testování, který tuto změnu uvede do dokumentace testování.

4.3.3 Emergency scénář

V případě, že dojde vlivem penetračního testování k omezení služeb testovaného prostředí IS, jedná se o tzv. Emergency stav.

Každá role, která zjistí Emergency stav, bez prodlení informuje Vedoucího koordinačního týmu, který dá pokyn k ukončení testování.

Role, které mají oprávnění navrhnout zastavení testování:

a) Manažer kybernetické bezpečnosti,
b) Garant primárního aktiva,
c) Garant podpůrného aktiva,
d) Vedoucí týmu provozního monitoringu,
e) Vedoucí týmu bezpečnostního monitoringu,
f) Vedoucí týmu dodavatele penetračního testování.

Všechny role komunikují na základě určené Emergency komunikační matice.

Pokud dojde k rozhodnutí o Emergency stavu, Vedoucí týmu dodavatele penetračního testování je odpovědný za okamžité zastavení veškerých činností spojených s realizací testování. Vedoucí koordinačního týmu ve spolupráci s Vedoucím týmu dodavatele penetračního testování, Vedoucím týmu provozního monitoringu a Vedoucím týmu bezpečnostního monitoringu zabezpečí, aby testovaný informační systém, byl uveden do stavu jako před testováním.

Vedoucí týmu dodavatele penetračního testování ve spolupráci s Vedoucím týmu provozního monitoringu, Vedoucím týmu bezpečnostního monitoringu a Vedoucím koordinačního týmu vede veškerou dokumentaci průběhu Emergency stavu, včetně jeho příčin, následků a komunikace.

V případě opakování penetračního testování Vedoucí týmu dodavatele penetračního testování vydá takové pokyny Realizačnímu týmu, aby nedošlo k opakovanému Emergency stavu. O změně parametrů realizovaných testů jsou vedeny příslušné záznamy v dokumentaci.

4.3.4 Přerušení penetračního testování

Role, které mají oprávnění navrhnout přerušení testování:

a) Manažer kybernetické bezpečnosti,
b) Garant primárního aktiva,
c) Garant podpůrného aktiva,
d) Vedoucí týmu provozního monitoringu,
e) Vedoucí týmu bezpečnostního monitoringu,
f) Vedoucí týmu dodavatele penetračního testování.

O návrhu na přerušení penetračního testování je informován Vedoucí koordinačního týmu. Vedoucí koordinačního týmu svolá jednání koordinačního týmu, kde navrhovatel přerušení sdělí informace o:

- příčinách přerušení penetračního testování,
- návrhu činností pro dokončení realizace penetračního testování,
- návrhu na změnu cílů nebo parametrů penetračního testování,
- návrhu na změnu harmonogramu penetračního testování.

Vedoucí koordinačního týmu rozhodne o návrzích vedoucích k pokračování v realizaci penetračního testování.

Přerušení je detailně vedeno v dokumentaci penetračního testování.

4.3.5 Zastavení penetračního testování

V případě, že z Emergency stavu nebo z přerušení penetračního testování vyplyne, že není možné dále pokračovat v realizaci penetračního testování, Vedoucí koordinačního týmu, svolá

jednání koordinačního týmu. Na tomto jednání jsou projednány aspekty zastavení penetračního testování v minimálním rozsahu:

- příčiny zastavení penetračního testování,
- rozsah již provedených a realizovaných testů,
- vliv na harmonogram penetračního testování,
- vliv na průběh veřejné zakázky a plnění uzavřenou smlouvu,
- způsob předání dokumentace z již provedených a realizovaných testů.

Po rozhodnutí o zastavení penetračního testování Vedoucí týmu provozního monitoringu a Vedoucí týmu bezpečnostního monitoringu ověří, že testovaný informační systém je uveden do stavu jako před testováním.

Zastavení penetračního testování je detailně vedeno v dokumentaci penetračního testování.

5 Vyhodnocení a akceptace

5.1 Vyhodnocení penetračního testování

Po skončení penetračního testování Vedoucí týmu dodavatele penetračního testování shromáždí všechny postupy, nálezy a důkazy od ostatních členů realizačního týmu a zaznamená je do Návrhu zprávy z penetračního testování (viz Příloha č. 6). Výstupy musí být v souladu s rozsahem a požadovanými cíli penetračního testování.

Součástí Návrhu zprávy z penetračního testování jsou návrhy na nápravná opatření k jednotlivým nálezům.

Návrh zprávy z penetračního testování odešle Vedoucí týmu dodavatele penetračního testování v harmonogramem stanoveném termínu a ve struktuře dle Přílohy č. 6 všem členům Koordinačního týmu.

V Návrhu zprávy z penetračního testování jsou nálezy rozděleny do jednotlivých kategorií podle závažnosti:

a) Kategorie A – Kritické – kdy útočníci mohou získat kontrolu nad zařízením nebo serverem nebo mohou unikat vysoce citlivé informace, včetně přístupu ke všem souborům, jejich modifikaci, přístupu k seznamu uživatelů na zařízení, spuštění příkazů a instalaci zadní vrátek (backdoor).
b) Kategorie B – Závažné – kdy útočníci mohou získat přístup ke specifickým informačním zdrojům, které obsahují bezpečnostní nastavení, včetně přístupu ke konkrétním souborům, prohlížení obsahu adresářů nebo neoprávněné využití služeb, jako například mail-relaying.

c) Kategorie C – Upozornění – kdy útočníci mohou shromažďovat informace o zařízení (otevřené porty, služby atd.), případně používat tyto informace k vyhledání dalších zranitelností.

5.2 Připomínky k Návrhu zprávy z penetračního testování

Vedoucí koordinačního týmu určí členům Koordinačního týmu termín a způsob pro uplatnění připomínek k Návrhu zprávy z penetračního testování. Tyto připomínky uplatňují u Vedoucího týmu dodavatele penetračního testování, v kopii na ostatní členy Koordinačního týmu.

Vedoucí koordinačního týmu určí termíny projednání a vypořádání připomínek k Návrhu zprávy z penetračního testování. Tohoto jednání se účastní členové Koordinačního týmu a členové Realizačního týmu za dodavatele.

5.3 Vypořádání a akceptace

Cílem projednání je vypořádat všechny připomínky členů Koordinačního týmu a posoudit návrhy na doporučení vedoucí k odstranění nálezů.

Z jednání je vyhotoven zápis, který je součástí Zprávy z penetračního testování.

Vedoucí týmu dodavatele penetračního testování po projednání připomínek k Návrhu zprávy z penetračního testování a návrhů na doporučení vedoucí k odstranění nálezů k jednotlivým nálezům zpracuje konečné znění Zprávy z penetračního testování.

Vedoucí týmu dodavatele penetračního testování zašle konečné znění Zprávy z penetračního testování členům Koordinačního týmu k akceptaci.

Vedoucí koordinačního týmu svolá jednání Koordinačního týmu, na kterém je Zpráva z penetračního testování akceptována.

Vedoucí koordinačního týmu udělí pokyn k zakončení realizace veřejné zakázky na penetrační testování.

Vedoucí koordinačního týmu předá doporučení vedoucí k odstranění nálezů z penetračního testování Manažerovi.

5.4 Seznam doporučení vedoucí k odstranění nálezů

Manažer zašle doporučení vedoucí k odstranění nálezů z penetračního testování garantu primárního aktiva testovaného IS a příslušným garantům podpůrných aktiv k návrhu konkrétních nápravných opatření.

Konkrétní nápravná opatření jsou následně schválena Manažerem.

Odsouhlasená nápravná opatření Manažer uvede v Plánu zvládání rizik informačního systému se stanovením vlastníků, termínů a způsobu řešení u jednotlivých nálezů.

5.5 Realizace nápravných opatření

Garant primárních nebo podpůrných aktiv realizuje všechna schválená nápravná opatření z Plánu zvládání rizik informačního systému.

5.6 Kontrola nápravných opatření

Manažer pravidelně kontroluje provádění všech odsouhlasených nápravných opatření v Plánu zvládání rizik informačního systému a po jejich realizaci ukončí sledování konkrétního nápravného opatření.

6 Následný plán a ověření výsledků penetračního testování

Na základě Zprávy z penetračního testování naplánuje Manažer další penetrační testování dle kapitoly 2.3.1 této metodiky za účelem ověření, zda realizovaná nápravná opatření měla vliv na zvýšení bezpečnosti testovaného informačního systému.

Příloha 1 – Stanovení členů týmů

Koordinační tým		
role člena týmu	titul, jméno a příjmení	organizace
Vedoucí koordinačního týmu		MF
Garant primárního aktiva		MF
Garant podpůrných aktiv		MF
Projektový manažer informačního systému zadavatele		MF
Projektový manažer dodavatele informačního systému		
Vedoucí týmu dodavatele penetračního testování		

Realizační tým		
role člena týmu	titul, jméno a příjmení	organizace
Oblast kybernetická bezpečnost IS		
Architekt kybernetické bezpečnosti		MF
Vedoucí týmu bezpečnostního monitoringu		
Oblast správy a provozu IS		
Zástupce garanta podpůrných aktiv		MF
Zástupce garanta primárního aktiva		MF
Vedoucí týmu provozního monitoringu		
Projektový manažer informačního systému zadavatele		MF
Provozovatel informačního systému		
Oblast dodavatele IS		
Architekt informačního systému		
Oblast dodavatele penetračního testování		
Specialista tester – 1		
Specialista tester – 2		
Specialista tester – 3		
Specialista tester – …		

Příloha 2 – Komunikační a Emergency matice

Koordinační tým			
role člena týmu	e-mail	telefon	Emergency
Vedoucí koordinačního týmu			ANO

Garant primárního aktiva			ANO
Garant podpůrných aktiv			ANO
Projektový manažer informačního systému zadavatele			
Projektový manažer informačního systému dodavatele			
Vedoucí týmu dodavatele penetračního testování			ANO

Realizační tým			
role člena týmu	e-mail	telefon	Emergency
Oblast kybernetická bezpečnost IS			
Architekt kybernetické bezpečnosti			
Vedoucí týmu bezpečnostního monitoringu			ANO
Oblast správy a provozu IS			
Zástupce garanta podpůrných aktiv			
Zástupce garanta primárního aktiva			
Vedoucí týmu provozního monitoringu			ANO
Projektový manažer informačního systému zadavatele			
Provozovatel informačního systému			
Oblast dodavatele IS			
Architekt informačního systému			
Oblast dodavatele penetračního testování			
Specialista tester – 1			
Specialista tester – 2			
Specialista tester – 3			
Specialista tester – …			

Příloha 3 – Definice rozsahu testování

Oddíl / činnost / podklady	Příklad
Definice testování	
nastavení rozsahu testování	zaměřený / omezený / úplný
nastavení informovanosti	žádný / provozního monitoringu / bezpečnostního monitoringu
nastavení míry, kdy je přerušeno testování dochází k omezení služeb testovaného prostředí IS	max. % vytíženosti prostředí IS
nastavení doby nebo časového úseku, kdy jsou realizovány zálohy nastavení nebo dat každého prvku ICT	6 / 12 / 24 hodin
nastavení informovanosti správců propojených informačních systémů	informace podána / nepodána
nastavení omezení služeb pro uživatele a propojené informační systémy	omezení se plánuje / neplánuje
nastavení nakládání s citlivými informacemi	definice NDA a rozsahu zpřístupněných informací
nastavení požadavku na uchování důkazů	místo a oprávnění pro uchování důkazů
nastavení metodiky a frameworku testování	NIST SP 800-115, OWASP, OSSTMM, OISNT
nastavení Koordinačního týmu	Ano
nastavení Realizačního týmu	Ano
nastavení Emergency kontaktů	Ano
Identifikace prostředí a rozsahu jednotlivých vrstev pro testování	
Základní oblast	
budovy, kde jsou umístěny prvky ICT informačního systému	informace o prvku ICT
technologické místnosti a serverovny	informace o prvku ICT
elektřina a UPS	informace o prvku ICT
fyzické zabezpečení technologických místností a serverovny	informace o prvku ICT
regulace teploty a protipožární systém	informace o prvku ICT
Fyzická oblast	
metalická infrastruktura uvnitř technologických místností, serveroven nebo objektů	informace o prvku ICT
optická infrastruktura uvnitř technologických místností, serveroven nebo objektů	informace o prvku ICT
vstupy/výstupy komunikačních linky providerů nebo pronajatých linek	informace o prvku ICT
bezdrátová infrastruktura uvnitř nebo vně objektů	informace o prvku ICT
Linková oblast	
převodníky a čidla (non IT)	informace o prvku ICT
L2 switche	informace o prvku ICT
media convertory	informace o prvku ICT

bezdrátové přijímače/vysílače	informace o prvku ICT
Síťová oblast	
DDoS protectory	informace o prvku ICT
firewally	informace o prvku ICT
L3 switche / core	informace o prvku ICT
routery	informace o prvku ICT
VLANy	informace o prvku ICT
Transportní oblast	
loadbalancery	informace o prvku ICT
prostředky HA/Geocluster	informace o prvku ICT
aplikační firewall	informace o prvku ICT
použití nešifrovaných a šifrovaných protokolů	informace o prvku ICT
použití nestandartních a standartních portů	informace o prvku ICT
Relační oblast	
dedikované fyzické servery	informace o prvku ICT
virtualizační hardwarové servery	informace o prvku ICT
virtualizační softwarová platforma	informace o prvku ICT
dedikovaná disková pole	informace o prvku ICT
SAN včetně diskových polí	informace o prvku ICT
podpůrné servery (DHCP/DNS/AD)	informace o prvku ICT
HSM moduly	informace o prvku ICT
Prezentační oblast	
operační systémy umístěné na hardwarovém prostředí	informace o prvku ICT
databázové systémy umístěné na hardwarovém prostředí	informace o prvku ICT
file systémy umístěné na hardwarovém prostředí	informace o prvku ICT
operační systémy umístěné ve virtuálním prostředí	informace o prvku ICT
databázové systémy umístěné ve virtuálním prostředí	informace o prvku ICT
file systémy umístěné ve virtuálním prostředí	informace o prvku ICT
Aplikační oblast	
aplikační servery	informace o prvku ICT
prezentační servery	informace o prvku ICT
ověření uživatelů a identity management	informace o prvku ICT
Datová oblast	
ekonomická data	umístění dat
agendová data	umístění dat
osobní data	umístění dat
data uživatelských účtů	umístění dat
provozní a bezpečnostní data a logy	umístění dat
Bezpečnostní oblast	
provozní dokumentace	umístění dokumentů
bezpečnostní dokumentace	umístění dokumentů

dokumentace veřejné zakázky a smlouvy	umístění dokumentů
konfigurační databáze	umístění dokumentů
definice rolí a odpovědností provozu a rozvoje IS	umístění dokumentů
provozní monitoring	umístění dokumentů
bezpečnostní monitoring	umístění dokumentů
zálohování a DRP	umístění dokumentů
Adresní rozsahy	
Externí adresní rozsahy	
veřejné IP adresy	informace o konfiguraci
neveřejné IP adresy na externím DMZ perimetru	informace o konfiguraci
komunikační protokoly určené pro externí komunikaci	informace o konfiguraci
komunikační porty určené pro externí komunikaci	informace o konfiguraci
dodavatelé externí konektivity	informace o dodavateli
Interní adresní rozsahy jednotlivých prvků ICT	
interní IP adresy na vstupu	informace o konfiguraci
interní IP adresy na výstupu	informace o konfiguraci
komunikační protokoly určené pro interní komunikaci	informace o konfiguraci
komunikační porty určené pro interní komunikaci	informace o konfiguraci
správci interní konektivity	informace o správci
Identifikace platforem	
webové služby	IIS, Apache
operační systémy	Windows, Linux, Oracle, Solaris, IBM AIX,
virtuální prostředí	VMware, Hyper-V, RHEVM,
databáze	Oracle, MS SQL, Sybase, PostgreSQL, MySQL,
síťové prvky	Cisco IOS, NXOS, Brocade Network OS, Cisco Fabric OS,
firewall a proxy	Check Point, SQUID
Dopady na propojené informační systémy	
soupis propojených informačních systémů	informace o systému
soupis kontaktů na správce propojených informačních systémů	informace o správci
podmínky propojení informačních systémů	definice propojení
podmínky provozu testovaného informačního systému	definice provozu
podmínky poskytování služeb informačního systému pro veřejnost	rozsah služby
definice časových omezení realizace penetračního testování	rozsah omezení
napojení na provozní monitoring	Ano / Ne
napojení na bezpečnostní monitoring	Ano / Ne

Příloha 4 – Souhlas s prováděním penetračních testů a simulací

Souhlas s prováděním penetračních testů a simulací

Česká republika – Ministerstvo financí

Letenská 525/15,

118 10 Praha 1 - Malá Strana

prostřednictvím Manažera kybernetické bezpečnosti Mgr. Josefa Nováka a na základě uzavřené smlouvy č. MF-123456/20XX

uděluje souhlas

společnosti ABC s.r.o.

Ulice 123/45,

111 50 Praha

IČ 123 456 789 (a jejím přímo řízeným subdodavatelům k předmětné zakázce)

s prováděním bezpečnostních testů a simulací informačního systému ISKB včetně dále uvedených cílů:

a) Cíl 1
b) Cíl 2
c) ..

a to v termínu:

od DD.MM.RRRR, HH:MM hod. do DD.MM.RRRR, HH:MM hod.

Účelem realizace penetračního testování a simulací kybernetických bezpečnostních událostí a incidentů je kontrola a monitorování účinnosti organizačních a technických opatření v oblasti zajištění kybernetické bezpečnosti identifikovaných cílů.

Simulací kybernetických bezpečnostních událostí a incidentů se pro účely tohoto souhlasu rozumí takové technické a netechnické aktivity společnosti ABC s.r.o. a jejich přímo řízených subdodavatelů, které jsou svojí povahou podobné kontrolovaným kybernetickým útokům na shora uvedené cíle s tím, že se výslovně požaduje, aby tyto aktivity neměly ve vztahu ke sledovanému účelu nepřiměřeně destruktivní charakter.

Ministerstvo financí pro vyloučení všech pochybností výslovně uvádí, že je oprávněno k vydání tohoto souhlasu.

----------	----------
souhlas udělil	souhlas obdržel
(podpis zadavatele)	(podpis dodavatele)

Příloha 5 – Harmonogram realizace penetračního testu

Harmonogram realizace penetračního testování v souladu s kapitolou 2.3.2 má následující fáze:

1. Stanovení členů jednotlivých týmů
2. Stanovení komunikační matice včetně Emergency kontaktní matice
3. Definice rozsahu testování
4. Převzetí podkladů
5. Souhlas s provedením penetračního testování
6. Stanovení harmonogramu penetračního testování (Příloha č. 5).
7. Realizace penetračního testování
   7.1. Realizace jednotlivých tesů
   7.2. Vyhodnocení výstupů z testů
8. Zaslání Návrhu zprávy z penetračního testování
9. Projednání Návrhu zprávy z penetračního testování
10. Zaslání Zprávy z penetračního testování
11. Akceptace Zprávy z penetračního testování

Příloha 6 – Návrh zprávy a Zpráva z penetračního testování

Tato příloha definuje strukturu dokumentu Návrh zprávy z penetračního testování resp. Zprávy z penetračního testování.

Hlavička a obsah dokumentu

1. Manažerské shrnutí
   1.1. Souhrnné doporučení
2. Identifikace cílů - bezpečnostní testování
   2.1. Specifikace cílů pro testování:
      2.1.1. cíl 1 …
      2.1.2. cíl 2 …
      2.1.3. cíl 3 …
   2.2. Dokumentace k testovaným cílům
   2.3. Účel testování
      2.3.1. Identifikace požadovaného účelu testování
      2.3.2. Identifikace míry bezpečnosti na procesy zadavatele
   2.4. Definice testování
      2.4.1. Metodika testování
      2.4.2. Výběr rolí testování
      2.4.3. Orientační postup
      2.4.4. Způsob sociotechnické testování
      2.4.5. Viditelnost testování
      2.4.6. Vstupní bod
      2.4.7. Informační báze
      2.4.8. Rozsah a přístupová oprávnění pro testery
      2.4.9. Fyzický přístup k jednotlivým prvkům ICT
      2.4.10. Přístup do fyzických prostor
      2.4.11. Zdrojové adresy testerů
      2.4.12. Agresivita testování
3. Realizace penetračního testování
   3.1. Cíle penetračního testování
      3.1.1. Stanovení cíle penetračního testování
      3.1.2. Harmonogram penetračního testování
   3.2. Rozsah penetračního testování
      3.2.1. Dokumentace penetračního testování
      3.2.2. Výstupy penetračního testování
      3.2.3. Akceptační kritéria
      3.2.4. Plánované činnosti v průběhu penetračního testování
   3.3. Organizace penetračního testování
      3.3.1. Vedoucí koordinačního týmu
      3.3.2. Realizační tým

Příloha 7 – Seznam povolených testovacích nástrojů

- **Nmap** - síťový skener pro detekci portů, síťových služeb a jejich verzí (opensource),
- **Unicornscan** - síťový skener podobný nástroji Nmap,
- **BurpSuite** - nástroj pro hledání zranitelností webových aplikací, dostupný jako freeware a v komerční edici s plnou funkcionalitou,
- **Acunetix** - nástroj pro hledání zranitelností webových aplikací,
- **Nikto** – webový skener detekující různé aplikace a jejich verze a doplňující moduly včetně nastavení web serveru (opensource),
- **w3af** - webový skener (Web Application Attack & Audit Framework) umožňující testovat zranitelnosti webových aplikací (opensource),
- **DirBuster** – nástroj pro odhalování existujících adresářů a souborů na web server (opensource),
- **SQLmap** – nástroj pro testování a exploitaci zranitelností typu SQL injection (opensource),
- **THC Hydra, Medusa** – nástroje pro lámání hesel online (opensource),
- **HashCat, John the Ripper** – nástroje pro lámání hesel offline (freeware, opensource),
- **Metasploit framework** – nástroj pro penetrační testování se skenovacími a exploitačními moduly včetně platformy pro vývoj dalších modulů (volně k použití),
- **Core Impact Pro** – komplexní nástroj pro penetrační testery obsahující detekční skenovací moduly a připravené exploity (komerční nástroj),
- **netcat** – nástroj pro demonstraci zadních vrátek, lze jej používat k testování dostupností síťových portů (volně k použití),
- **BeEF** – nástroj pro exploitaci zranitelností webového prohlížeče (volně k použití),
- **Firefox** – webový prohlížeč doplněný o moduly usnadňující práci se čtením zdrojového kódu HTML stránky a sledováním HTTP požadavků (volně k použití),
- **Nessus** – síťový a bezpečnostní skener, umožňuje pouze detekovat zranitelnosti (komerční nástroj),
- **SIUX** – nástroj pro ověřování konfigurací UNIX/Linux systémů (komerční interní nástroj),
- **WinAudit** – nástroj pro ověřování konfigurací MS Windows (komerční nástroj).