**Číslo Smlouvy MF**
**23/906/0003**
*Toto číslo uvádějte při fakturaci*

# SMLOUVA O POSKYTOVÁNÍ SLUŽEB PENETRAČNÍHO TESTOVÁNÍ

uzavřená v souladu s ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „Občanský zákoník"), v souladu s ust. § 122 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ"), jejímž předmětem je plnění veřejné zakázky s názvem

**„Služby penetračního testování Informačního systému Evidence dotací MF – CEDR MF – EHP/NF"**

č. j.: MF-3054/2023/6602

***Evidenční číslo smlouvy: 9006/003/2023***

**ČESKÁ REPUBLIKA – MINISTERSTVO FINANCÍ**
se sídlem: Letenská 15, 118 10 Praha 1
jejímž jménem jedná: xxx
IČO: 00006947
DIČ: CZ00006947
Bankovní spojení: ČNB,
číslo účtu 3328001/0710
ID datové schránky: xzeaauv
(dále jen „**Objednatel**")
a

**BELCOM Digital a.s.**
se sídlem: Generála Šišky 2375/6, Modřany, 143 00 Praha 4
zapsaná v obchodním rejstříku pod spisovou značkou B 4080 vedenou u Městského soudu v Praze
zastoupena: xxx
IČO: 25056646
DIČ: CZ25056646
Bankovní spojení: Raiffeisenbank, a.s.,
číslo účtu: 465434001/5500
ID datové schránky: p43c3pq
(dále jen „**Dodavatel**")

Objednatel a Dodavatel spolu dále jen „**Smluvní strany**".

spolu uzavírají tuto smlouvu za účelem zabezpečení služby penetračního testování a identifikace zranitelností (dále také „Předmět smlouvy") u významného informačního systému (dále jen „VIS") v prostředí Objednatele (dále jen „Smlouva")

## PREAMBULE

Smlouva je uzavírána na základě výsledku zadávacího postupu na veřejnou zakázku Dynamický nákupní systém - Služby penetračního testování – Výzva 4-2023 (dále také jako „Zadávací postup"). Výše uvedený dynamický nákupní systém je uveřejněn ve Věstníku veřejných zakázek pod evidenčním číslem Z2020-046552. Dodavatel prohlašuje, že není

ve střetu zájmů při plnění této Smlouvy, ve vztahu k jejímu cíli dle v čl. I odst. 2 ani ve vztahu ke skutečnosti, že v návaznosti na výsledek Předmětu smlouvy mohou být odpovědným dodavatelům Objednatele stanoveny nové povinnosti, mohou po nich být vymáhány smluvní sankce, popřípadě náhrada škody (dále jen „Definovaný střet zájmů Dodavatele“).

## Článek I
## Předmět Smlouvy

1) Předmětem této Smlouvy je na straně jedné závazek Dodavatele provést penetrační test informačního systému Objednatele „Evidence dotací MF – CEDR MF – EHP/NF“ (dále jen „CEDR MF - EHP/NF“ nebo „Informační systém“), jehož specifikace a definice rozsahu plnění je uvedena v Příloze č. 1 této Smlouvy, a na straně druhé pak závazek Objednatele převzít řádně a včas poskytnuté Plnění a uhradit jejich sjednanou cenu dle čl. II této Smlouvy.
2) Předmětem plnění (dále jen „Plnění“) je provedení penetračního testování s cílem:
    a) ověřit zranitelnost webové aplikace a služeb uvedeného Informačního systému,
    b) ověřit bezpečnost webové aplikace a služeb uvedeného Informačního systému,
    c) poskytnout komplexní zprávu o provedeném testování včetně návrhu opatření:
        - aplikace pravidel a technických opatření nezbytných k ochraně citlivých informací v daném Informačním systému,
        - zvýšení účinnosti zabezpečení daného Informačního systému.
3) Postupy, vstupy i výstupy penetračního testování budou probíhat na základě Objednatelem zpracované „Metodiky provádění penetračních testů“, která je Přílohou č. 4 této Smlouvy. Tato metodika vychází z obecně platných standardů, doporučení a metodik pro provádění penetračních testů.
4) Dodavatel prohlašuje a podpisem této Smlouvy potvrzuje, že předmět Smlouvy bude plnit realizační tým Dodavatele, který disponuje veškerými potřebnými oprávněními, odbornými znalostmi a praktickými zkušenostmi k řádnému splnění této Smlouvy a tyto skutečnosti dokládá v Příloze č. 2 této Smlouvy**.** Dodavatel prohlašuje, že bez předchozího a nenárokového souhlasu Objednatele se na plnění této Smlouvy nebudou podílet žádní poddodavatelé, kromě těch, kteří mají svého zástupce v Koordinačním nebo v Realizačním týmu a jejichž prostřednictvím Dodavatel při zavádění dynamického nákupního systému prokazoval svoji kvalifikaci. V případě, že se v průběhu plnění této Smlouvy prokáže, že Dodavatel nesplňuje doložené skutečnosti nebo uvedl nepravdivé údaje, či zatajil poddodavatele na plnění této Smlouvy, bude toto jednání považováno za podstatné porušení této Smlouvy s právem Objednatele odstoupit od podepsané Smlouvy v souladu s čl. XI odst. 2. Při odstoupení od této Smlouvy z výše uvedeného důvodu má Objednatel právo uplatnit vůči Dodavateli smluvní pokutu dle čl. X odst. 3.
5) Dodavatel dále prohlašuje, že na jeho majetek nebyl prohlášen konkurz, nebylo proti němu zahájeno konkurzní ani vyrovnávací řízení, nebyl zamítnut konkurz pro nedostatek majetku, není v likvidaci a nemá v evidenci daní zachyceny daňové nedoplatky. Dále Dodavatel prohlašuje, že není osobou, která by v době posledních tří let byla disciplinárně potrestána nebo pravomocně odsouzena pro trestný čin hospodářský, proti majetku nebo pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání Dodavatele.
6) Objednatel se zavazuje poskytnout Dodavateli veškerou součinnost, nezbytnou pro řádné splnění této Smlouvy.
7) Objednatel je oprávněn rozhodnout o provedení kontrolního dne, a to i opakovaně. Neurčí-li Objednatel jinak, musí se za Dodavatele na kontrolní den dostavit Vedoucí týmu dodavatele penetračního testování a alespoň jeden tester dle výběru Objednatele (dále též „Povinné osoby za Dodavatele“, a osoby, které určil Objednatel).

8) Na kontrolním dni je Dodavatel povinen prezentovat aktuální stav Plnění, způsob provádění Plnění, použité podklady a další informace související s Předmětem smlouvy podle potřeb Objednatele. Objednatel je na kontrolním dni oprávněn vytýkat vady Plnění, pokud již realizované plnění neodpovídá požadavkům dle této Smlouvy, jejích příloh, či obecně závazným předpisům – zejména avšak nikoli pouze požadavkům zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů a jeho prováděcích předpisů.
9) O provádění kontrolního dne se sepíše protokol, pro jeho náležitosti se použije přiměřeně ustanovení čl. III. odst. 5 této Smlouvy, navíc se vždy uvede seznam osob přítomných na kontrolním dnu a to, zda Objednatel vytýkal vady Plnění.
10) Objednatel stanoví přiměřenou lhůtu pro odstranění vad Plnění a způsob kontroly jejího odstranění, například se může jednat o provedení nového kontrolního dne či o předání písemných dokumentů. Přiměřenost lhůty se stanoví i s přihlédnutím k termínu plnění dle čl. III odst. 1 této Smlouvy.
11) Pokud se na kontrolní den nedostaví všechny povinné osoby za Dodavatele nebo pokud nejsou odstraněny vady vytknuté Objednatelem ve stanovené lhůtě, bude toto jednání považováno za podstatné porušení této Smlouvy s právem Objednatele odstoupit od podepsané Smlouvy v souladu s čl. XI odst. 2.

## Článek II
## Cena

1) Smluvní strany si ujednaly, za řádné a včasné poskytnutí Plnění Smluvní cenu (dále jen „Cena“), která činí částku **73 000,- Kč bez DPH** zvýšenou o částku odpovídající dani z přidané hodnoty ve výši 15 330,- Kč platné ke dni uskutečnění zdanitelného plnění.
2) Výše uvedená Cena je sjednána dohodou Smluvních stran podle zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, a je cenou maximální a nepřekročitelnou, která zahrnuje veškeré náklady spojené s poskytnutím Plnění, včetně nákladů na dopravu do sídla Objednatele a dalších nákladů v této Smlouvě výslovně neuvedených, které souvisejí s poskytnutým Plněním.

## Článek III
## Termín a místo plnění, dodací podmínky

1) Dodavatel se zavazuje poskytnout Plnění **do 30 dnů** ode dne počátku běhu lhůty, kdy budou předány Dodavatelem Objednateli písemné výstupy z Plnění (dále jen „Výstupy z Plnění“), a to dle jejich specifikace uvedené v Příloze č. 1. Dodavatel se zavazuje poskytnout Plnění dle této Smlouvy jako celek, tj. částečné Plnění je vyloučené. Lhůta počíná plynout 16. dnem účinnosti této Smlouvy, pokud se Smluvní strany nedohodnou na dřívějším dni; na takovou dohodu ovšem nemá ani jedna ze Smluvních stran právní nárok.
2) Dodavatel se zavazuje, že Plnění bude provedeno pod vedením Vedoucího týmu dodavatele penetračního testování a členy týmu splňujících požadované odborné požadavky ve smyslu Přílohy č. 2 této Smlouvy. Dodavatel je oprávněn předložit Objednateli k odsouhlasení pouze takovou změnu týmu Dodavatele, aby i nadále byly splněny požadavky dle Přílohy č. 2 této smlouvy. Odpovídá-li navrhovaná změna požadavkům dle předchozí věty, Objednatel neodmítne souhlas se změnou. Návrh změny týmu nesmí sloužit k obcházení smluvní povinnosti Dodavatele dle čl. I odst. 7 věta druhá této Smlouvy. Je-li Objednatelem již oznámeno konání kontrolního dne, je Objednatel oprávněn vyčkat s udělením souhlasu až po jeho konání.
3) Výstupy z Plnění je Dodavatel povinen předat Objednateli v sídle Objednatele: Letenská 525/15, 118 10 Praha 1 (dále jen „Místo Plnění“).

4) Plnění dle této Smlouvy bude považováno za splněné převzetím Plnění Oprávněnou osobou Objednatele uvedenou v čl. XII odst. 2 této Smlouvy a podpisem akceptačního protokolu oběma stranami této Smlouvy (dále jen „Akceptační protokol“) v sídle Objednatele. Akceptační protokol bude vyhotoven elektronicky.
5) Dodavatel je povinen uvést v Akceptačním protokolu totožné identifikační údaje, které jsou uvedeny v této Smlouvě včetně základních údajů o Objednateli, zejména:
   a) identifikační údaje Objednatele a Dodavatele,
   b) jméno a příjmení oprávněné osoby Objednatele, příp. pověřené osoby Objednatele, kterou může být osoba písemně pověřená xxx,
   c) číslo této Smlouvy,
   d) adresu sídla Objednatele,
   e) datum provedení Plnění,
6) Převezme-li oprávněná osoba Objednatele, příp. pověřená osoba Objednatele, Výstupy z Plnění bez výhrad, má se za to, že poskytnuté Plnění nemá žádné zjevné vady. Převezme-li oprávněná osoba Objednatele, příp. pověřená osoba Objednatele, Výstupy z Plnění s výhradami, je povinen tyto výhrady uvést do Akceptačního protokolu. Oprávněná osoba Objednatele, příp. pověřená osoba Objednatele i Dodavatele, je povinna stvrdit obsah Akceptačního protokolu svým jménem a podpisem. V případě, že Akceptační protokol obsahuje výhrady oprávněné osoby Objednatele, příp. pověřené osoby Objednatele, zavazuje se Dodavatel odstranit výhrady ve lhůtě a způsobem uvedeným oprávněnou osobou Objednatele, příp. pověřenou osobou Objednatele v Akceptačním protokolu. Po odstranění výhrad oprávněná osoba Objednatele, příp. pověřená osoba Objednatele a Dodavatele sepíší nový Akceptační protokol bez výhrad.
7) Nastane-li stav Plnění dle bodu 4.3.3 Přílohy č. 4 této Smlouvy, termín Plnění uvedený v odstavci 1 tohoto článku se prodlužuje o dobu stavu Plnění. Dodavatel je za stavu Plnění dle bodu 4.3.3. Přílohy č. 4 této smlouvy povinen vykonat činnosti definované Přílohou č. 4.
8) Dojde-li k přerušení Plnění dle bodu 4.3.4 Přílohy č. 4 této Smlouvy, termín Plnění uvedený v odstavci 1 tohoto článku se prodlužuje o dobu přerušení Plnění.
9) Dojde-li k zastavení Plnění dle bodu 4.3.5 Přílohy č. 4 této Smlouvy, předá Dodavatel Objednateli veškeré Výstupy z Plnění k okamžiku zastavení Plnění.

## Článek IV
## Náhrada škody a práva třetích osob

1) Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu vzniklou porušením platných právních předpisů a této Smlouvy.
2) Dodavatel odpovídá mimo jiné za veškerou škodu, která vznikne v důsledku vadného poskytování Plnění nebo v důsledku porušení jiné právní povinnosti Dodavatele.
3) Za škodu se přitom považuje i škoda vzniklá Objednateli porušením jeho vlastní povinnosti vůči některému jeho smluvnímu partnerovi, včetně sankce vyplacené smluvním partnerům Objednatele, a jakákoliv sankce veřejnoprávní povahy uvalená na Objednatele, pokud Objednatel takové porušení své právní povinnosti nemohl z důvodu porušení povinnosti Dodavatele zabránit.
4) Škodu hradí škůdce v penězích, nežádá-li poškozený uvedení do předešlého stavu.
5) Náhrada škody je splatná ve lhůtě 7 (sedmi) dnů od doručení písemné výzvy oprávněné smluvní strany smluvní straně povinné z náhrady škody.
6) Dodavatel prohlašuje, že provedení Plnění vč. výstupů budou bez právních vad, zejména nebudou zatíženy žádnými právy třetích osob, z nichž by pro Objednatele vyplynul finanční nebo jakýkoliv jiný závazek ve prospěch třetí strany nebo která by jakkoliv

omezovala užívání výsledků penetračních testování. V případě porušení tohoto závazku je Dodavatel v plném rozsahu odpovědný za případné následky takového porušení, přičemž právo Objednatele na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.

7) Dodavatel se zavazuje, že při Plnění této Smlouvy bude postupovat tak, aby nedošlo k neoprávněnému zásahu do práv třetích osob. V případě porušení tohoto závazku je Dodavatel v plném rozsahu odpovědný za případné následky takového porušení, přičemž právo Objednatele na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.
8) Dodavatel se zavazuje, že bude mít po celou dobu účinnosti této Smlouvy sjednánu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě s limitem pojistného plnění minimálně ve výši 20 mil. Kč (slovy: dvaceti milionů korun českých). Dodavatel je povinen předat kopii pojistného certifikátu (pojistné smlouvy) Objednateli před podpisem této Smlouvy a současně kdykoliv na vyžádání Objednatele a to bez zbytečného odkladu, nejpozději však do 5 (pěti) pracovních dnů od doručení písemné žádosti Objednatele.
9) Smluvní strany prohlašují, že je jim ke dni podpisu Smlouvy známa existence epidemie koronaviru označovaného jako SARS CoV-2 (způsobujícího nemoc COVID-19) a s ní související krizová opatření, jiná opatření, předpisy, správní akty či jiné zásahy orgánů veřejné moci České republiky či jiných států, jakož i skutečností, že v budoucnu se tato krizová opatření apod. mohou vyvíjet nebo opakovat, s řadou přímých či nepřímých dopadů na ekonomickou či politickou situaci, zejména dodavatelské řetězce (např. nedostatky v plnění Poddodavatelů), nedostatek pracovních sil či materiálů, nedostatek finanční likvidity či dalších dopadů. Tyto dopady koronaviru se nepovažují za nepředvídatelné, a tedy za okolnost vylučující povinnost k náhradě škody dle tohoto článku.

## Článek V
## Odpovědnost za vady a záruka

1) Dodavatel se zavazuje, že poskytnuté Plnění, včetně jeho výstupů, nebude mít při předání žádné vady.
2) Dodavatel je povinen provést Plnění v souladu s požadavky definovanými touto Smlouvou, podle technických vlastností specifikovaných v Příloze č. 1 a při dodržení povinností sjednaných v této Smlouvě. Objednatel je povinen řádně a včas dodané a akceptované výstupy z Plnění převzít a zaplatit za ně smluvenou cenu.
3) Poruší-li Dodavatel povinnosti stanovené v odst. 1 tohoto článku, jedná se o vady Plnění.
4) Zjistí-li Objednatel vady týkající se Plnění a výstupů z tohoto Plnění, je oprávněn odmítnout jejich převzetí. O takovém odmítnutí bude proveden zápis do Akceptačního protokolu podepsaného Objednatelem nebo jím Pověřenou osobou a Dodavatelem s uvedením důvodu odmítnutí převzetí.
5) Nestanoví-li tato Smlouva jinak, řídí se odpovědnost za vady ust. § 2099 a násl. Občanského zákoníku o právech z vadného Plnění a záruce za jakost.
6) V případě prodlení Dodavatele s plněním práv Objednatele z vad Díla je Dodavatel povinen uhradit Objednateli smluvní pokutu uvedenou v čl. X odst. 1 této Smlouvy.

## Článek VI
## Platební podmínky

1) Platba za Plnění řádně poskytnuté Dodavatelem Objednateli dle této Smlouvy bude provedena Objednatelem jednorázově bezhotovostním platebním převodem na základě faktury vystavené Dodavatelem Objednateli nejpozději do 14 (čtrnácti) kalendářních dnů

ode dne podpisu Akceptačního protokolu bez výhrad oběma stranami této Smlouvy (příp. Dodavatelem a Oprávněnou osobou Objednatele nebo Pověřenou osobou Objednatele). Přílohou faktury bude kopie příslušného Akceptačního protokolu bez výhrad podepsané Objednatelem, příp. Oprávněnou osobou Objednatele nebo Pověřenou osobou Objednatele a Dodavatelem a splňující všechny náležitosti dle této Smlouvy.

2) Faktura musí obsahovat zejména:
   a) číslo této Smlouvy, uvedené v záhlaví v rámečku,
   b) uvedení názvu Veřejné zakázky,
   c) specifikaci Plnění a jeho cenu; celková cena nesmí být vyšší než Maximální cena, kterou Dodavatel nabídl v nabídce, na jejímž základě byla uzavřena tato Smlouva,
   d) úplné bankovní spojení Dodavatele s tím, že číslo účtu musí odpovídat číslu účtu uvedenému v záhlaví této Smlouvy nebo číslu účtu v registru plátců DPH,
   e) označení Objednatele,
   f) veškeré náležitosti dle ust. § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a
   g) údaje uvedené v ust. § 435 odst. 1 Občanského zákoníku.
3) Faktury jsou splatné do 30 (třiceti) kalendářních dnů ode dne jejich prokazatelného elektronického doručení prostřednictvím datové schránky Objednateli na adresu Objednatele uvedenou v identifikaci Objednatele v záhlaví této Smlouvy. Dodavatel se zavazuje doručovat faktury ve formátu PDF nebo ve formátu, který je v souladu s evropským standardem elektronické faktury nebo ve formátu popsaném vyhláškou č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění pozdějších předpisů.
4) Faktura je považována za uhrazenou okamžikem odepsání příslušné finanční částky z účtu Objednatele ve prospěch účtu Dodavatele.
5) Objednatel je oprávněn před uplynutím lhůty splatnosti fakturu vrátit Dodavateli, aniž by došlo k prodlení s její úhradou, obsahuje-li nesprávné náležitosti nebo údaje, chybí-li na faktuře některá z náležitostí nebo údajů nebo chybí-li některá z příloh. Dodavatel je povinen v případě vrácení faktury fakturu opravit nebo vyhotovit fakturu novou. Ode dne doručení opravené, příp. nové faktury běží Objednateli nová lhůta splatnosti v délce 30 kalendářních dnů.
6) Platby budou probíhat výhradně v korunách českých a rovněž veškeré cenové údaje budou uvedeny v této měně.
7) Dodavatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Dodavatel je nespolehlivým plátcem ve smyslu ust. § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „Nespolehlivý plátce“). V případě, že správce daně rozhodne o tom, že Dodavatel je Nespolehlivým plátcem, zavazuje se Dodavatel o tomto informovat Objednatele do 3 pracovních dnů od vydání takového rozhodnutí. Stane-li se Dodavatel Nespolehlivým plátcem, je Objednatel oprávněn provést zajišťovací úhradu daně z přidané hodnoty ve smyslu ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, na účet příslušného správce daně.
8) Dodavatel bere na vědomí, že Objednatel neposkytuje zálohové platby.

## Článek VII
## Práva a povinnosti Smluvních stran

1) Dodavatel a Objednatel jsou povinni si poskytovat součinnost a vzájemně se informovat o všech okolnostech důležitých pro řádné a včasné Plnění této Smlouvy. Objednatel se zavazuje poskytnout Dodavateli řádně a včas veškeré informace a podklady k testovanému Informačnímu systému, bez čehož by Dodavatel nemohl v souladu s touto

Smlouvou plnit své povinnosti a poskytovat Plnění dle této Smlouvy.

2) Dodavatel se zavazuje poskytnout Plnění dle této Smlouvy v souladu se zájmy Objednatele a při veškeré své činnosti dbát jeho dobrého jména a nedopustit se jednání, které by mohlo dobré jméno Objednatele jakkoliv ohrozit nebo poškodit. Dodavatel je povinen oznámit Objednateli všechny okolnosti, které zjistí a které mohou mít vliv na činnost Objednatele nebo na kvalitu a včasnost Plnění dle této Smlouvy.
3) Dodavatel je povinen realizovat Plnění dle této Smlouvy na své náklady a na své nebezpečí. Dodavatel je za účelem Plnění dle této Smlouvy oprávněn využít pouze toho poddodavatele, který byl Dodavatelem uveden při žádosti o zavedení do DNS. Za plnění poddodavatele, který byl uveden při žádosti o zavedení DNS, odpovídá Dodavatel tak, jako by plnil sám. V ostatních případech není Plnění prostřednictvím poddodavatele přípustné a porušení této povinnosti se považuje za podstatné porušení této Smlouvy.
4) Dodavatel se zavazuje provádět Plnění řádně a včas, s potřebnou odbornou péčí, podle pokynů Objednatele a v souladu se zájmy Objednatele, jakož i právními předpisy. Má-li Dodavatel pochybnost, zda zamýšlený úkon je či již není ve prospěch Objednatele, je povinen o této skutečnosti (pochybnosti) Objednatele neprodleně informovat a vyžádat si jeho písemné stanovisko, jak v dané záležitosti dále postupovat. V případě, že pokyny Objednatel budou v rozporu s obecně závaznými právními předpisy, bude Dodavatel na tuto skutečnost povinen Objednatele upozornit. Bude-li Objednatel na takovém pokynu trvat, bude Dodavatel oprávněn splnění pokynu odmítnout.
5) Dodavatel se zavazuje provádět Plnění v souladu s touto Smlouvou, jakož i dokumenty Zadávacího postupu. V případě rozporu vyjmenovaných podkladů mají přednost ustanovení této Smlouvy (vč. příloh).
6) Dodavatel bere na vědomí, že je povinen umožnit osobám oprávněným k výkonu kontroly např. podle zákona č. 218/2000 Sb., o rozpočtových pravidlech, ve znění pozdějších předpisů, provést kontrolu dokladů souvisejících s plněním Veřejné zakázky, a to v rozsahu jejich oprávnění a po dobu danou právními předpisy České republiky k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů). Dále bere Dodavatel na vědomí, že je podle ust. § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou služeb z veřejných výdajů. Dodavatel je povinen zajistit, že všichni poddodavatelé poskytnou subjektům provádějícím audit a kontrolu, zejména kontrolním orgánům dle zákona č. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů, nezbytné informace týkající se jejich činnosti a Plnění, které v rámci této Smlouvy vykonávají pro Dodavatele.
7) Dodavatel se zavazuje, že s kontrolními orgány podle předchozího odstavce tohoto článku bude na výzvu spolupracovat a poskytne jim odpovídající součinnost.
8) Dodavatel je povinen řádně uchovávat veškerou dokumentaci související s Plněním, včetně účetních dokladů, minimálně po dobu stanovenou v českých a bezprostředně aplikovatelných evropských právních předpisech.
9) Objednatel bez objektivních důvodů nepřipouští změnu členů realizačního týmu na straně Dodavatele. Dojde-li z objektivních důvodů ke změně člena realizačního týmu, podléhá tato změna předchozímu souhlasu Objednatele. O navrhované změně člena realizačního týmu je Dodavatel povinen, minimálně 7 kalendářních dní předem písemně informovat Objednavatele. Nový člen realizačního týmu musí splnit veškeré požadavky plynoucí dle Přílohy č. 2 této Smlouvy.
10) Dodavatel se zavazuje nakládat se všemi věcmi, dokumenty a jinými písemnostmi, které mu byly Objednatelem svěřeny pro účely provádění Plnění, s péčí řádného hospodáře a chránit je před poškozením a zneužitím. Objednatel zůstává vlastníkem takových podkladů

poskytnutých Dodavateli za účelem plnění této Smlouvy. Dodavatel je oprávněn s podklady nakládat pouze v souladu s podmínkami této Smlouvy. Dodavatel není oprávněn k jinému nakládání a užití podkladů bez předchozího souhlasu Objednatele. Všechny písemnosti a jiné nosiče informací, včetně případných kopií, je povinen chránit před nepovolanými osobami. Dodavatel plně odpovídá za škodu způsobenou ztrátou a zneužitím svěřených hodnot dle tohoto odstavce. Dodavatel se zavazuje na základě písemné výzvy Objednatele nebo po ukončení platnosti této Smlouvy veškeré věci, dokumenty a jiné písemnosti, které mu byly Objednatelem svěřeny pro účely Plnění této Smlouvy znehodnotit tak, aby nemohly být nadále jakkoliv využitelné, a to nejpozději do 5 (pěti) dnů od skončení této Smlouvy.

## Článek VIII
## Kybernetická bezpečnost a související povinnosti Dodavatele

1) Dodavatel se zavazuje při plnění této Smlouvy postupovat v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále též „ZoKB“), jakož i v souladu se souvisejícími prováděcími předpisy a dodržovat bezpečnostní politiky a vnitřní předpisy.
2) Dodavatel bere na vědomí, že Předmět plnění dle této Smlouvy má přímou souvislost s provozem IS VIS (významný informační systém) ve smyslu ZoKB.
3) Dodavatel se zavazuje v průběhu plnění této Smlouvy písemně upozornit Objednatele na případný zjištěný nesoulad Plnění dle článku I této Smlouvy s povinnostmi definovanými ZoKB a s případnými nedostatky zjištěnými auditem kybernetické bezpečnosti.
4) Dodavatel akceptuje, že veškeré náklady, které mu v průběhu plnění dle této Smlouvy vzniknou v souvislosti se zavedením a plněním požadavků dle ZoKB, s provedeným auditem kybernetické bezpečnosti, či užitím definovaných bezpečnostních v rozsahu Předmětu Plnění dle této Smlouvy, jsou plně k jeho tíži.
5) Seznam vyžadovaných bezpečnostních opatření se může měnit v návaznosti na povinnosti Objednatele vyplývající z § 11 ZoKB. Pokud Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) Objednateli uloží povinnost zavést či užívat určité bezpečnostní opatření a dotýká–li se toto jakkoliv povahy či rozsahu plnění dle této Smlouvy, má Dodavatel povinnost toto bezpečnostní opatření zavést či užívat nebo Objednateli poskytnout nutnou součinnost k zajištění uložených povinností.

## Článek IX
## Mlčenlivost

1) Dodavatel a Objednatel se zavazují udržovat v tajnosti, podniknout všechny nezbytné kroky k zabezpečení a nezpřístupnit třetím osobám informace, které jsou nuceni v zájmu realizace této Smlouvy zpřístupnit druhé Smluvní straně a které považují za důvěrné, neveřejné a mají na jejich ochraně zájem (dále jen „Neveřejné informace“). Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena. Za Neveřejné informace se považují veškeré následující informace:
   a) veškeré informace poskytnuté Dodavateli Objednatelem v souvislosti s Plněním této Smlouvy, a to zejména veškeré informace týkající se Informačního systému a všech dat v něm obsažených, poskytnuté v jakékoliv podobě, ať písemně, ústně či jiným způsobem (pokud nejsou výslovně obsaženy ve znění této Smlouvy), včetně informací

které byly do data uzavření této Smlouvy chráněny dle DOHODY O ZACHOVÁNÍ MLČENLIVOSTI A OCHRANĚ NEVEŘEJNÝCH INFORMACÍ (číslo Smlouvy MF 9006/003/2023), pokud ji Smluvní strany uzavřely,
   b) informace, na která se vztahuje zákonem uložená povinnost mlčenlivosti,
   c) veškeré další informace, které budou Objednatelem označeny jako Neveřejné informace.
2) Povinnost zachovávat mlčenlivost, uvedená v předchozím článku, se nevztahuje na informace:
   a) které je Objednatel povinen poskytnout třetím osobám podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,
   b) jejichž sdělení vyžaduje jiný právní předpis,
   c) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak než porušením právních povinností ze strany některé ze Smluvních stran,
   d) u nichž je Dodavatel schopen prokázat, že mu byly známy ještě před přijetím těchto informací od Objednatele, avšak pouze za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů,
   e) které budou Dodavateli po uzavření této Smlouvy sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k těmto informacím nijak vázána.
3) Jako s Neveřejnými informacemi musí být nakládáno také s informacemi, které splňují podmínky uvedené v odst. 1 tohoto článku, i když byly získané náhodně nebo bez vědomí Objednatele, a dále s veškerými informacemi získanými od jakékoliv třetí strany, pokud se týkají Objednatele či plnění této Smlouvy.
4) Dodavatel se zavazuje, že Neveřejné informace užije pouze za účelem Plnění této Smlouvy. K jinému použití je třeba předchozí písemné svolení Objednatele.
5) Dodavatel je povinen svého případného, Objednatelem předem schváleného poddodavatele zavázat povinností mlčenlivosti a respektováním práv Objednatele nejméně ve stejném rozsahu, v jakém je zavázán sám touto Smlouvou.
6) Veškeré Neveřejné informace včetně jejich kopií musí být vráceny či prokazatelně zničeny nejpozději do 5 (pěti) pracovních dnů od ukončení poskytovaného Plnění a/nebo v případě požadavku zpřístupňující Smluvní strany. Dodavatel je oprávněn si ponechat jen takové Neveřejné informace, které jsou nezbytné pro účely splnění požadavků vyplývajících z platných právních předpisů.
7) Povinnost zachování mlčenlivosti trvá po dobu neurčitou bez ohledu na zánik ostatních závazků z této Smlouvy.
8) Závazky vyplývající z tohoto článku není žádná ze Smluvních stran oprávněna vypovědět ani jiným způsobem jednostranně ukončit.
9) Smluvní strany jsou si vědomy, že v případě porušení svých povinností týkajících se ochrany Neveřejných informací dle této Smlouvy, ponesou veškerou odpovědnost spojenou s náhradou vzniklé škody.
10) Ustanovení tohoto článku jsou v plném rozsahu uvedeny v Příloze č. 3 této Smlouvy.

## Článek X
## Sankce

1) V případě prodlení Dodavatele s poskytnutím Plnění ve lhůtě dle čl. III odst. 1 této Smlouvy, má Objednatel právo uplatnit vůči Dodavateli smluvní pokutu ve výši 0,5 % z Ceny, a to za každý, byť i započatý den prodlení. V případě prodlení Dodavatele se lhůtou pro odstranění vad Plnění dle čl. I odst. 10 této Smlouvy, má Objednatel právo uplatnit vůči Dodavateli smluvní pokutu ve výši 0,5 % z Ceny, a to za každý, byť i započatý den prodlení.

2) V případě prodlení Dodavatele s dodržením lhůty pro odstranění výhrad (vad Plnění) stanovené v Akceptačním protokolu dle čl. III odst. 6 této Smlouvy, má Objednatel právo uplatnit smluvní pokutu ve výši 15.000 Kč (patnáct tisíc korun českých) za každou neodstraněnou vadu a to za každý, byť i započatý den prodlení.
3) V případě porušení některé z povinností Dodavatele stanovené v čl. I odst. 4 (splnění odborných předpokladů, zákaz poddodavatele), čl. IV odst. 6 (právní vady Plnění), čl. VII odst. 2 (informační povinnost Dodavatele o závažných okolnostech) nebo čl. VII odst. 3 (nepřípustné plnění poddodavatelem), čl. VIII odst. 5 (kybernetická bezpečnost) či v případě Definovaného střetu zájmů Dodavatele, má Objednatel právo uplatnit vůči Dodavateli smluvní pokutu ve výši 100.000 Kč (sto tisíc korun českých), a to za každý jednotlivý případ porušení.
4) V případě, že Dodavatel poruší smluvní povinnost dle čl. XI odst. 7, tj. nesplní informační povinnost o skutečnostech uvedených v čl. XI odst. 6, má Objednatel právo uplatnit vůči Dodavateli smluvní pokutu ve výši 100.000 Kč (sto tisíc korun českých), a to za každý jednotlivý případ porušení.
5) V případě, že Dodavatel poruší některou z povinností mlčenlivosti dle čl. IX, má Objednatel právo uplatnit vůči Dodavateli smluvní pokutu ve výši 1.000.000 Kč (jeden milion korun českých), a to za každý jednotlivý případ porušení.
6) V případě, že Dodavatel poruší smluvní povinnost dle čl. I odst. 7 věta druhá této Smlouvy (nedostaví se všechny Povinné osoby za Dodavatele), má Objednatel právo uplatnit vůči Dodavateli smluvní pokutu ve výši 3.000 Kč za každou Povinnou osobu Dodavatele, která se byla povinna dostavit na kontrolní den, ale neučinila tak.
7) V případě pokuty ze strany dozorového orgánu (NÚKIB) uplatněná vůči Objednateli za zjištěná porušení povinností Dodavatelem, bude Objednateli uhrazena Dodavatelem tato pokuta v plné výši.
8) V případě prodlení Objednatele s úhradou řádně vystavené a doručené faktury je Dodavatel oprávněn požadovat úrok z prodlení ve výši stanovené platnými právními předpisy.
9) Smluvní pokuta je splatná ve lhůtě 7 (sedmi) dnů od doručení písemné výzvy oprávněné Smluvní strany Smluvní straně povinné ze smluvní pokuty.
10) Ujednáním o smluvní pokutě není dotčeno právo poškozené smluvní strany domáhat se náhrady škody v plné výši.
11) Zaplacení smluvní pokuty nezbavuje Dodavatele povinnosti splnit závazek utvrzený smluvní pokutou.

## Článek XI
## Doba trvání a ukončení Smlouvy

1) Tato Smlouva se uzavírá na dobu určitou ode dne její účinnosti, tj. na dobu ode dne jejího zveřejnění v Registru smluv, do okamžiku splnění všech závazků obou Smluvních stran touto Smlouvou stanovených.
2) Tato Smlouva může zaniknout odstoupením příslušné Smluvní strany, nastanou-li okolnosti předvídané ust. § 2002 Občanského zákoníku či okolnosti pro odstoupení, stanovené touto Smlouvou.
3) Odstoupením se závazek touto Smlouvou založený zrušuje ohledně nesplněného zbytku plnění (tj. ex nunc).

4) Objednatel může od Smlouvy odstoupit také ohledně celého Plnění a to v případě, kdy Dodavatel nesplní odborné požadavky dle čl. I odst. 4 této Smlouvy nebo poruší ustanovení čl. VII odst. 3 týkající se zákazu plnění prostřednictvím poddodavatele, který nebyl uveden při zavedení DNS. V takovém případě se závazek založený touto Smlouvou ruší od počátku (tj. ex tunc). Smluvní strany si jsou povinny vyrovnat dosavadní vzájemné závazky z této Smlouvy, a to bez zbytečného odkladu, nejpozději však do 30 (třiceti) dnů od doručení oznámení Smluvní strany o odstoupení od této Smlouvy.
5) Za podstatné porušení této Smlouvy Dodavatelem se považuje zejména jednání, kdy:
   a) Dodavatel neprovede Plnění ani do 10 (deseti) pracovních dnů ode dne uplynutí smluveného termínu Plnění dle čl. III odst. 1 za podmínky, že důvody prodlení nejsou na straně Objednatele,
   b) Dodavatel neodstraní vady Plnění ani do 10 (deseti) pracovních dnů ode dne uplynutí lhůty stanovené v Akceptačním protokolu dle čl. III odst. 6 této Smlouvy,
   c) Dodavatel nedoloží skutečnosti požadované dle čl. I odst. 4 této Smlouvy.
6) Objednatel je dále oprávněn odstoupit od této Smlouvy v případě, že:
   a) v insolvenčním řízení bude zjištěn úpadek Dodavatele nebo insolvenční návrh bude zamítnut pro nedostatek majetku Dodavatele v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů;
   b) proti Dodavateli je zahájeno trestní stíhání pro trestný čin podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů;
   c) Dodavatel se stane Nespolehlivým plátcem dle čl. VI odst. 8 této Smlouvy.
7) Nastane-li některý z případů uvedených v odst. 6 písm. a) až c) tohoto článku, je Dodavatel povinen písemně informovat o této skutečnosti Objednatele písemně do 2 (dvou) dnů od jejího vzniku, společně s informací o tom, o kterou ze skutečností jde, a s uvedením bližších údajů, které by Objednatel mohl v této souvislosti potřebovat pro své rozhodnutí o odstoupení od této Smlouvy. Nedodržení této povinnosti je podstatným porušením této Smlouvy.
8) Odstoupení od této Smlouvy musí být učiněno písemně, jinak nemá právní účinky. Odstoupení je účinné ode dne, kdy bylo doručeno druhé smluvní straně. V pochybnostech se má za to, že odstoupení od této Smlouvy bylo doručeno 5 (pátým) kalendářním dnem od jeho odeslání oprávněnou stranou doporučenou poštovní zásilkou nebo doručením do datové schránky druhé Smluvní strany při odeslání datovou zprávou.
9) Ukončením této Smlouvy není dotčen nárok na zaplacení smluvní pokuty nebo úroku z prodlení, pokud již dospěl, právo na náhradu škody vzniklé porušením smluvní povinnosti, povinnost mlčenlivosti, práva z odpovědnosti za vady a záruky ani ujednání, které má vzhledem ke své povaze zavazovat Smluvní strany i po ukončení této Smlouvy.

## Článek XII
## Závěrečná ustanovení

1) Smluvní strany se dohodly na určení Oprávněné osoby za Objednatele a Dodavatele (dále jen „Oprávněná osoba“). Oprávněné osoby jsou oprávněné ke všem jednáním týkajícím se této Smlouvy, není-li v této Smlouvě stanoveno jinak, s výjimkou změn nebo ukončení této Smlouvy nebo změny bankovních údajů. V případě, že strana má více Oprávněných osob, zasílají se veškeré e-mailové zprávy na adresy všech Oprávněných osob současně.
2) Oprávněnou osobou Objednatele je:
   a) ve věcech smluvních:
      Jméno: xxx
      e-mail: xxx
      tel.: xxx

b) ve věcech technických:
Jméno: xxx
e-mail: xxx
tel.: xxx

3) Oznámení nebo jiná sdělení podle této Smlouvy musí být učiněna písemně v českém jazyce. Jakékoliv úkony směřující ke skončení této Smlouvy a oznámení o změně bankovních údajů musí být doručeny druhé smluvní straně datovou schránkou nebo formou doporučeného dopisu. Oznámení nebo jiná sdělení podle této Smlouvy se budou považovat za řádně učiněná, pokud budou doručena osobně, poštou, prostřednictvím datové schránky či kurýrem na adresy uvedené v tomto odstavci (včetně označení jménem příslušné Oprávněné osoby) nebo na jinou adresu, kterou příslušná Smluvní strana v předstihu písemně oznámí adresátovi, není-li v konkrétním případě stanoveno jinak.
   a) Objednatel:
   Název: Ministerstvo financí
   Adresa: Letenská 15, Praha 1, PSČ 118 10
   K rukám: Oprávněná osoba Objednatele
   b) Dodavatel:
   Název: BELCOM Digital a.s.
   Adresa: Generála Šišky 2375/6, Modřany, 143 00 Praha 4
   K rukám: xxx
   Datová schránka: p43c3pq
4) Účinnost oznámení nastává v pracovní den následující po dni doručení tohoto oznámení Objednateli nebo Dodavateli, není-li v této Smlouvě dohodnuto jinak.
5) Tato Smlouva nabývá platnosti dnem podpisu Smluvními stranami a účinná okamžikem zveřejnění v Registru smluv v souladu se zákonem č. 340/2015 Sb., zákon o registru smluv, ve znění pozdějších předpisů.
6) Oprávněné osoby nejsou oprávněny doplňovat, měnit nebo ukončovat tuto Smlouvu či měnit bankovní údaje. K takovým úkonům je za Objednatele v úvodu této Smlouvy nebo ministrem financí pověřená osoba. K jednáním směřujícím ke zmíněným změnám v tomto článku je za Dodavatele oprávněn Dodavatel sám, je-li fyzickou osobou podnikající, nebo statutární orgán či prokurista Dodavatele, a to dle způsobu jednání uvedeném v obchodním rejstříku. Jiné osoby mohou tato právní jednání činit pouze s písemným pověřením osoby či orgánu vymezených v předchozí větě (dále jen „Odpovědné osoby pro věci smluvní“). Odpovědné osoby pro věci smluvní mají současně všechna oprávnění Oprávněných osob.
7) Doplňování nebo změnu této Smlouvy včetně jejích příloh lze provádět jen se souhlasem Smluvních stran, a to pouze formou písemných dodatků, datovaných a podepsaných Smluvními stranami na jedné listině, není-li v této Smlouvě stanoveno jinak.
8) Jakékoliv změny kontaktních údajů, včetně bankovního spojení a Oprávněných osob, je příslušná Smluvní strana oprávněna provádět jednostranně a je povinna tyto změny neprodleně písemně oznámit druhé Smluvní straně. Platí, že takové změny nejsou důvodem k uzavření dodatku k této Smlouvě.
9) Smluvní strany berou na vědomí, že tato uzavřená Smlouvy, bude v plném rozsahu v elektronické podobě zveřejněna v registru smluv, dle ZZVZ na profilu Objednatele, případně na jiném místě, bude-li k tomu Objednatel povinován, a to bez časového omezení. Dodavatel souhlasí se zveřejněním této Smlouvy nebo její části na internetových stránkách Objednatele, a to bez časového omezení. Objednatel se zavazuje, že tuto Smlouvu v souladu se zákonem o registru smluv, ve znění pozdějších předpisů, uveřejní v Registru smluv.
10) Dodavatel není oprávněn bez předchozího písemného souhlasu Objednatele postoupit práva a povinnosti plynoucí z této Smlouvy třetí osobě.

11) Jestliže kterákoli ze Smluvních stran neuplatní nárok nebo nevykoná právo podle této Smlouvy, nebo je vykoná se zpožděním či pouze částečně, nebude to znamenat vzdání se těchto nároků nebo práv. Vzdání se práva z titulu porušení této Smlouvy nebo práva na nápravu anebo jakéhokoliv jiného práva podle této Smlouvy musí být vyhotoveno písemně a podepsáno Smluvní stranou, která takové vzdání se činí.
12) Pokud se jakékoliv ustanovení této Smlouvy stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení této Smlouvy. Smluvní strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a touto Smlouvou jako celkem.
13) Tato Smlouva se řídí právním řádem České republiky. Veškeré spory vzniklé z této Smlouvy nebo v souvislosti s některou z nich budou smluvní strany řešit především vzájemnou dohodou. Nedojde-li k dohodě ani do 60 (šedesáti) dnů ode dne zahájení jednání o řešení sporu, bude spor vyplývající ze závazkového vztahu upraveného touto Smlouvou řešen podle obecně závazných právních předpisů České republiky. Smluvní strany se ve smyslu ust. § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů dohodly, že soudem příslušným pro všechny spory vzniklé z této Smlouvy je obecný soud Objednatele.
14) Smluvní strany se dohodly, že v rámci této Smlouvy vylučují aplikaci ustanovení § 557 Občanského zákoníku.
15) Tato Smlouva je vyhotovena v 1(jednom) vyhotovení v českém jazyce s platností originálu s elektronickými podpisy obou Smluvních stran v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.
16) Přílohy jsou nedílnou součástí této Smlouvy.
17) Pokud tato Smlouvy nestanoví jinak, řídí se tento smluvní vztah příslušnými ustanoveními Občanského zákoníku, zejména ustanoveními § 2586 a násl. upravujícími smlouvu o dílo.

Příloha č. 1: Definice rozsahu testování IS CEDR MF-EHPNF
Příloha č. 2: Odbornost zástupců dodavatele v Koordinačním a v Realizačním týmu
Příloha č. 3: Dohoda o zachování mlčenlivosti a ochraně neveřejných informací
Příloha č. 4: Metodika realizace penetračních testů

V Praze dne dle elektronického podpisu

_____

za Objednatele

**xxx**
**xxx**

Za finální znění k č.j.: MF-29420/2020/7001

**xxx**

Dne dle elektronického podpisu

_____

za Dodavatele
**xxx**
**xxx**

## Definice rozsahu testování – IS CEDR MF-EHP/NF

| Oddíl / činnost / podklady | Příklad |
|---|---|
| **Definice testování** | |
| natavení rozsahu testování | Zaměřený |
| nastavení informovanosti | Provozního monitoringu |
| nastavení míry, kdy je přerušeno testování z důvodu nadměrného zatížení prvku ICT | max. 70% vytíženosti prvků ICT IS |
| nastavení doby od zálohy nastavení a dat každého prvku ICT | 24 hodin |
| nastavení informovanosti správců napojených informačních systémů | Informace podána |
| nastavení omezení služeb pro uživatele a systémy | Omezení se neplánuje |
| nastavení nakládání s citlivými informacemi | Definice NDA a rozsahu zpřístupněných informací |
| nastavení požadavku na uchování důkazů | Realizováno po předání zprávy z penetračního testování na DVD |
| metodiky testování | Metodika realizace penetračních testů<br>IS KII a VIS Ministerstva financí ČR |
| framework testování | OWASP Web Security Testing Guide (WSTG) 4.2 v plném rozsahu |
| agresivita testování | cílená |
| Automatické nástroje | Během testování prostředí IS je dovoleno testovat pouze automatizovanými nástroji maximálně do objemu 50% testů. |
| Viditelnost testování | Otevřený test |
| Vstupní bod | externí |
| Informační báze | Black box |
| nastavení koordinačního týmu | Ano |
| nastavení realizačního týmu | Ano |
| nastavení Emergency kontaktů | Ano |

| **Externí adresní rozsahy** | |
|---|---|
| veřejné IP adresy | 4x veřejná IP adresa uvedená v Příloze č. 2.1 úplná |
| veřejné DNS | 2x veřejné DNS uvedené v Příloze č. 2.1 úplná |

Příloha č. 2 smlouvy

# Odbornost zástupců dodavatele v Koordinačním a v Realizačním týmu

**Pravidla pro vyplnění:**

1. Dodavatel odpoví na všechny otázky a je povinen uvést ve všech níže označených žlutě podbarvených polích "ANO".

2. Dodavatel je povinen uvést osobu Specialisty - testera pro technologie 1.1 až 1.3, každý z testerů musí mít certifikaci nebo osvědčení testera. Tyto funkce lze kumulovat.

Požadavky lze vždy splnit prokázat certifikáty či osvědčeními:
Certified Penetration Testing Engineer (CPTE),
Offensive Security Certified Professional (OSCP),
EC-Council Certified Ethical Hacker (CEH)
EC-Council Certified Security Analyst (CSA)
Computer Hacking Forensic Investigator (CHFI)
Certified Network Defender (CND)
EC-Council's Certified Penetration Tester (CPENT)
Licenced Pentrating Tester (LPT)
Offensive Security Exploitation Expert (OSEE) certification
Offensive Security Certified Expert (OSCE))

Pokud dodavatel předkládá jinou certifikaci či osvědčení, je povinen na výzvu zadavatel doložit podmínky pro vydání certifikátu či osvědčení.

3. Pokud dodavatel prokazoval v žádosti o účast splnění kritéria technické kvalifikace prostřednictvím jiné osoby, je povinen nominovat zástupce jiné osoby:
a) jako Vedoucí týmu dodavatele penetračního testování nebo alternativně
b) jako alespoň 1 Specialistu - testera.

Pokud dodavatel neprokazoval v žádosti o účast splnění kritéria technické kvalifikace prostřednictvím jiné osoby, nemůže nominovat zástupce jiné osoby.

| **Požadavky objednatele:** | **Nabídka dodavatele:** | |
|---|---|---|
| **I. Testeři dodavatele** | | |
| **1. Odborné znalosti a praktické zkušenosti:** | **Splňuje ANO/NE** | **Jméno držitele, kopie certifikátu** |
| 1.1. Realizace testování operačního systému: | | |
| Tester pro OS Microsoft | | xxx |
| Certfikace nebo osvědčení Specialisty - testera | ANO | Certified Ethical Hacker |
| Tester zajišťován jinou osobou | NE | |
| 1.2. Realizace testování virtuálního prostředí (hypervisory): | | |
| Tester pro Vmware | | xxx |
| Certfikace nebo osvědčení Specialisty - testera | ANO | Certified Ethical Hacker |

| | | |
|---|---|---|
| Tester zajišťován jinou osobou | NE | |
| 1.3. Realizace testování databází: | | |
| Tester pro MS SQL | | xxx |
| Certfikace nebo osvědčení Specialisty - testera | ANO | Certified Ethical Hacker |
| Tester zajišťován jinou osobou | NE | |
| 1.4 Realizace provedení vnějších penetračních testů IS dle metodiky OWASP: | | |
| Specialista - tester | | xxx |
| Znalost metodiky OWASP Web Security Testing Guide (WSTG) 4.2 v plném rozsahu a realizace simulace napadení z vnějšího prostředí informačních systémů organizace | ANO | Ministerstvo financí - Provedení penetračního testování IS Viola - Spcialista - tester<br>Raiffeisen - Leasing, s.r.o. - Provedení bezpečnostního auditu procesního řízení vývoje, řízení testování a zdrojového kódu aplikace „Matrix“ – Člen týmu/pentester<br>La Biorganica s.r.o. – Testování E- commerce platformy – Člen týmu/pentester<br>ARETE INVEST, a.s. – Testování emailového systému – Člen týmu/pentester<br>ARETE Property s.r.o. – Testování prostředí MSAD – Člen týmu/pentester<br>Raiffeisen - Leasing, s.r.o. – Provedení penetračního testu www.financovanivozu.cz – Člen týmu/pentester<br>Raiffeisen - Leasing, s.r.o. - Provedení penetračního testu tkleasing.rl.cz – Člen týmu/pentester<br>Raiffeisen - Leasing, s.r.o. - Provedení penetračního testu www.rl.cz – Člen týmu/pentester<br>ELVAC – Provedení penetračního testu Elvac RTU Komunikační sada – Člen týmu/pentester<br>ELVAC – Provedení penetračního testu Elvac RTU7M – Člen týmu/pentester<br>ELVAC – Provedení penetračních testů Elvac HMI – Člen týmu/pentester<br>Správa základních registrů – Provádění penenetračních testů – člen týmu/pentester<br>Státní veterinární správa – Provedení penetračních testů aplikace OIS SVS - člen týmu/pentester<br>Správa základních registrů – Penetrační testy v prostředí RAZR, Bezpečnostní audit ICT – člen týmu/pentester<br>Český Aeroholding – Provedení penetračních testů WEB a Systému Jednorázové vstupy – člen týmu/pentester<br>Česká spořitelna – Audit přístupových sítí ČS – Penetrační testování zabezpečení sítí – člen týmu/pentester<br>Ministerstvo zemědělství ČR – Penetrační testování webového portálu - člen týmu/pentester<br>Tipsport – Penetrační testování portálu - člen týmu/pentester |
| Certfikace nebo osvědčení Specialisty - testera | ANO | Certified Ethical Hacker |
| Tester zajišťován jinou osobou | NE | |
| **II. Vedoucí týmu dodavatele penetračního testování:** | | |
| **Požadavky na roli** | **Splňuje ANO/NE** | **Jméno držitele, kopie certifikátu** |
| Vedoucí týmu dodavatele penetračního testování | | xxx |
| Certifikace nebo osvědčení metodik projektového řízení (IPMA, PRINCE2, PMBOK) | ANO | PRINCE2 ® Practitioner |

| | | |
|---|---|---|
| Zkušenost s realizací návrhu doporučení k optimalizaci zabezpečení informačního systému | ANO | Ministestvo financí - Provedení penetračního testování IS VIOLA - Vedoucí projektu<br>Raiffeisen - Leasing, s.r.o. - Provedení bezpečnostního auditu procesního řízení vývoje, řízení testování a zdrojového kódu aplikace „Matrix“ – Vedoucí projektu<br>La Biorganica s.r.o. – Testování E- commerce platformy – Vedoucí týmu<br>ARETE Property s.r.o. – Testování prostředí MSAD – Vedoucí týmu<br>Raiffeisen - Leasing, s.r.o. - Provedení penetračního testu www.rl.cz – Vedoucí týmu<br>ELVAC – Provedení penetračního testu Elvac RTU Komunikační sada – Vedoucí týmu<br>ELVAC – Provedení penetračního testu Elvac RTU7M – Vedoucí týmu<br>Správa základních registrů – Provádění penenetračních testů – Vedoucí týmu<br>Státní veterinární správa – Provedení penetračních testů aplikace OIS SVS - Vedoucí týmu<br>Správa základních registrů – Penetrační testy v prostředí RAZR, Bezpečnostní audit ICT – Vedoucí týmu<br>Český Aeroholding – Provedení penetračních testů WEB a Systému Jednorázové vstupy – Vedoucí týmu<br>Česká spořitelna – Audit přístupových sítí ČS – Penetrační testování zabezpečení sítí – Vedoucí týmu<br>Ministerstvo zemědělství ČR – Penetrační testování webového portálu - Vedoucí týmu<br>Tipsport – Penetrační testování portálu - Vedoucí týmu |
| Zkušenost s realizací ověření nápravných opatření. | ANO | dtto |
| Vedoucí penetračního testování zajišťován jinou osobou | NE | |

**Číslo Smlouvy MF**
9006/003/2023

# DOHODA O ZACHOVÁNÍ MLČENLIVOSTI A OCHRANĚ NEVEŘEJNÝCH INFORMACÍ

uzavřená dle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů
(dále jen „Dohoda")

**Česká republika – Ministerstvo financí**
se sídlem: Letenská 525/15, 118 10 Praha 1
IČ: 00006947
DIČ: CZ00006947
bankovní spojení: Česká národní banka
č. účtu: 3328-001/0710
ID datové schránky: xzeaauv
za niž jedná: xxx

(dále jen „Zadavatel")

a
**BELCOM Digital a.s.**
se sídlem: Generála Šišky 2375/6, Modřany, 143 00 Praha 4
zapsaná v obchodním rejstříku pod spisovou značkou B 4080 vedenou u Městského soudu v Praze
zastoupena: xxx
IČO: 25056646
DIČ: CZ25056646
Bankovní spojení: Raiffeisenbank, a.s.,
číslo účtu: 465434001/5500
ID datové schránky: p43c3pq

(dále jen „Účastník zadávacího postupu")

(Zadavatel a Účastník zadávacího postupu společně dále též jen jako „Smluvní strany" a jednotlivě jako „Smluvní strana")

## Preambule

Tato Dohoda se uzavírá v souvislosti s veřejnou zakázkou „**Dynamický nákupní systém na služby penetračního testování – Výzva 4-2023**" zadávanou v Dynamickém nákupním systému na služby penetračního testování, jehož oznámení bylo uveřejněno ve Věstníku veřejných zakázek dne 04. 01. 2021 pod evidenčním číslem VZ Z2020-046552" (dále jen „Veřejná zakázka") z důvodu zajištění ochrany neveřejných informací poskytnutých Zadavatelem Účastníkovi zadávacího postupu.

V rámci zadávacího postupu budou účastníkům zadávacího postupu předány neveřejné informace, které se týkají **Informačního systému Evidence dotací MF** (dále též „IS CEDR MF - EHP/NF nebo „Informační systém"), jež mají být předmětem Služeb penetračního testování (dále jen „Neveřejné informace"). Tyto Neveřejné informace jsou považovány Zadavatelem za mimořádně citlivé z důvodu, že IS CEDR MF - EHP/NF je Významný informační systém (VIS).

## I.
## Předmět Dohody

1.1 Předmětem této Dohody je závazek Účastníka zadávacího postupu, že udrží v tajnosti a nezpřístupní třetím osobám jakékoliv Neveřejné informace a skutečnosti, které se dozvěděl v rámci Veřejné zakázky, týkající se uvedeného Informačního systému Zadavatele a dále závazek Účastníka zadávacího postupu, že veškeré Neveřejné informace, které fyzicky získal od Zadavatele v rámci Veřejné zakázky v analogové či digitální, znehodnotí na základě písemné výzvy Zadavatele nebo po uplynutí doby platnosti této Dohody tak, aby nemohly být nadále jakkoliv využitelné.

1.2 Za Neveřejné informace se považují veškeré informace, týkající se uvedeného Informačního systému, poskytnuté v jakékoliv objektivně vnímatelné formě tj. ústně, v listinné, elektronické, vizuální nebo jiné podobě, jakož i know-how. Jedná se o informace, které mají hodnotu a nejsou v příslušných obchodních kruzích běžně dostupné. Zejména se jedná o:

1.2.1 Přílohy Výzvy k podání nabídky č. 2.1 úplná, č. 3 a č. 4 a o

1.2.2 Případné další dokumenty, které by Účastníkovi zadávacího postupu poskytl adresně Zadavatel (zejména se může jednat o přílohy Vysvětlení Výzvy či o Přílohu Výzvy ve znění Vysvětlení Výzvy).

1.3 Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů není tímto ustanovením dotčena.

1.4 Povinnost udržovat v tajnosti, uvedená v předchozím článku, se nevztahuje na informace:

1.4.1 které jsou nebo se stanou všeobecně a veřejně přístupnými jinak než porušením právních povinností ze strany některé ze Smluvních stran;

1.4.2 u nichž je Účastník zadávacího postupu schopen prokázat, že mu byly známy ještě před přijetím těchto informací od Zadavatele, avšak pouze za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů.

1.5 V případě, že Účastník zadávacího postupu poruší jakékoliv povinnosti vyplývající z této Dohody, zavazuje se uhradit smluvní pokutu dle čl. III. a i nadále odpovídá v plném rozsahu za škodu, která Zadavateli v důsledku takového porušení vznikne, přičemž Smluvní strany výslovně sjednávají, že k okolnostem vylučujícím odpovědnost ve smyslu ustanovení § 2913 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů se v takovém případě nepřihlíží.

## II.
## Platnost Dohody

Tato Dohoda se uzavírá na dobu určitou, a to do okamžiku kdy se stane veřejně známou informace, že smlouva na Veřejnou zakázku byla uzavřena s jiným dodavatelem (například uveřejněním smlouvy v registru smluv, na profilu zadavatele, nebo uveřejněním Oznámení o uzavření smlouvy způsobem podle § 212 ZZVZ). Pro Účastníka zadávacího postupu, kterému byla zadána smlouva na Veřejnou zakázku, se tato dohoda uzavírá do okamžiku splnění Veřejné zakázky. Povinnost zachovávat mlčenlivost ve vztahu k Neveřejným informacím, tj. nesdělit je ani k nim neumožnit přístup třetím osobám, trvá neomezeně a Smluvní strany se zavazují ji dodržovat.

## III.
## Sankční ujednání a náhrada škody

3.1 Smluvní strany se dohodly, že pro případ, že Účastník zadávacího postupu prokazatelným způsobem poruší povinnosti vyplývající z této Dohody, je povinen uhradit v případě každého jednotlivého porušení svých povinností Zadavateli smluvní pokutu ve výši 1.000.000,- Kč (slovy: jeden milión korun českých).

3.2 Smluvní strany se současně dohodly, že Smluvní strana, která prokazatelným způsobem poruší povinnosti vyplývající z této Dohody vedle smluvní pokuty i nadále odpovídá v plném rozsahu za škodu, která druhé Smluvní straně v důsledku takového porušení vznikne, přičemž Smluvní strany výslovně sjednávají, že k okolnostem vylučujícím odpovědnost ve smyslu ustanovení § 2913 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů se v takovém případě nepřihlíží.

3.3 Lhůta splatnosti pro zaplacení smluvní pokuty a náhrady škody činí (čtrnáct) kalendářních dní ode dne jejích uplatnění u Smluvní strany.

## IV.
## Závěrečná ustanovení

4.1 Tato Dohoda nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

4.2 Žádná Smluvní strana nemá právo od této Dohody odstoupit nebo ji vypovědět před ukončením doby, na kterou byla uzavřena (viz. čl. II této Dohody) .

4.3 Situace neupravené touto Dohodou se řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a dalšími obecně závaznými právními předpisy České republiky.

4.4 Jestliže se některé ustanovení této Dohody, nebo jeho část ukáže jako neplatné, neúčinné, nesrozumitelné, zdánlivé nebo nevymahatelné, nebude tím dotčena platnost ani účinnost Dohody jako celku ani jejích zbývajících ustanovení, nebo jejich částí. V takovém případě smluvní strany změní nebo přizpůsobí takové neplatné, neúčinné, nesrozumitelné, zdánlivé nebo nevymahatelné ustanovení písemnou formou tak, aby bylo dosaženo úpravy, které odpovídá účelu a úmyslu stran v době uzavření této Dohody, která je nejbližší neplatnému, neúčinnému, nesrozumitelnému, zdánlivému nebo nevymahatelnému ustanovení, popřípadě podniknou jakékoliv další právní kroky vedoucí k realizaci původního účelu takového ustanovení.

4.5 Smluvní strany prohlašují, že tato Dohoda byla uzavřena podle jejich pravé a svobodné vůle, vážně a srozumitelně, nikoli v tísni a za nápadně nevýhodných podmínek, a že souhlasí s jejím obsahem, což stvrzují svými podpisy.

4.6 Pokud je tato Dohoda zhotovena v listinné podobě, pak ve dvou vyhotoveních. Každá ze smluvních stran obdrží po jednom vyhotovení.

| | |
|---|---|
| V Praze dne _____ | V _____ dne _____ |
| Za Zadavatele | Za Účastníka zadávacího postupu |
| xxx, | |
| xxx | xxx |

# 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 | | MF-33092/2019/7001-8 | |
| | | | | |

# 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).