Smlouva

o poskytování systému pro skenování zranitelností – vulnerability management

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník"), mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel" nebo „ČNB")

a

Risk Analysis Consultants, s.r.o.
zapsanou v obchodním rejstříku vedeném Městským soudem v **Praze**, oddíl C vložka **36666**
sídlo/místo podnikání: Konviktská 291/24, 110 00 Praha 1
IČO: 63672774
DIČ: CZ63672774
zastoupenou: Ing. Michalem Žipajem, MBA, jednatelem
č. účtu: 576900263, kód banky 0300

(dále jen „poskytovatel")

Preambule

ČNB provozuje systémy ABO, CERTIS a SKD náležející mezi informační systém/y kritické informační infrastruktury a je dále provozovatelem významných informačních systémů DMS, eSpis, ISAI, JERRS a KRZR ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB") a vyhlášky č. 82/2018 Sb., 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 (dále jen „VKB"). Vzhledem k důležitosti těchto informačních systémů z pohledu naplňování úkolů a fungování ČNB a rovněž i vzhledem k naplňování požadavků výše uvedených právních předpisů v oblasti kybernetické bezpečnosti stanovuje objednatel dále uvedené požadavky, lhůty, platební podmínky, smluvní pokuty a další smluvní ujednání, která z této důležitosti vycházejí.

Článek I

Předmět smlouvy

1. Předmětem této smlouvy je závazek poskytovatele poskytnout objednateli systém pro skenování zranitelností – vulnerability management systém (dále též „Řešení"), poskytnuté Řešení nainstalovat, zprovoznit a implementovat do systémového prostředí objednatele, popsaného v příloze č. 2, a provést zaškolení nejvýše 3 osob určených

objednatelem. Podrobné požadavky na Řešení stanoví příloha č. 1 této smlouvy „Technické podmínky předmětu plnění“ a odst. 3 tohoto článku.

2. Řešení neukládá veškeré zjištěné nebo vkládané informace lokálně (v paměťovém prostoru určeném objednatelem na jeho zařízeních) nebo není lokálně zajištěna jejich správa.
3. Poskytovatel se touto smlouvou dále zavazuje poskytovat, od okamžiku předání a převzetí Řešení, objednateli podporu Řešení, zajistit objednateli podporu Řešení v nejvyšším možném rozsahu přímo výrobcem Řešení (vč. např. knowledgebase, hotline nebo eskalace ticketu, pokud je výrobce Řešení poskytuje), ve lhůtách poskytovaných výrobcem Řešení, a zajistit objednateli aktualizace Řešení a všech jeho komponent (především databáze zranitelností) v souladu s přílohou č. 1, to vše po dobu účinnosti této smlouvy. V rámci podpory Řešení musí být zajištěno přijímání hlášení vad Řešení zajišťující písemné potvrzení o okamžiku nahlášení vady (vč. elektronické formy) a odstraňování vad Řešení bez dalších nákladů pro objednatele, pakliže vadu Řešení nezpůsobil sám objednatel.
4. Poskytovatel se touto smlouvou rovněž zavazuje na žádosti objednatele rozšiřovat Řešení navyšováním počtu Aktiv (ve smyslu přílohy č. 1) v rozsahu podle přílohy č. 1, a to bez povinnosti uzavírat dodatek k této smlouvě. Žádost dle tohoto odstavce musí být podepsána nejméně jednou pověřenou osobou objednatele a objednatel ji doručí poskytovateli vždy písemně na adresu sídla poskytovatele nebo na e-mail pověřené osoby poskytovatele či do datové schránky poskytovatele; v pochybnostech se žádost považuje za doručenou třetí den ode dne jejího odeslání objednatelem.
5. Poskytovatel se touto smlouvou taktéž zavazuje na žádosti objednatele poskytovat objednateli konzultace a asistenci (on-site, remote) při aktivitách souvisejících s Řešením. Žádost dle tohoto odstavce musí být podepsána nejméně jednou pověřenou osobou objednatele, musí obsahovat požadovaný počet člověkodnů, bližší vymezení předmětu konzultace či asistence, a požadovaný termín poskytnutí plnění, a objednatel ji doručí poskytovateli vždy písemně na adresu sídla poskytovatele nebo na e-mail pověřené osoby poskytovatele či do datové schránky poskytovatele; v pochybnostech se žádost považuje za doručenou třetí den ode dne jejího odeslání objednatelem. Plnění podle tohoto odstavce lze uplatnit pouze, pokud není součástí podpory podle odst. 3 tohoto článku.
6. Zaškolení podle odst. 1 tohoto článku bude spočívat v seznámení osob určených objednatelem s ovládáním a funkcionalitami Řešení, s důrazem na znalosti potřebné ke správě a užívání Řešení, a to v minimální délce jednoho dne (8 hodin). Zaškolení proběhne v objektu poskytovatele na adrese Praha 1, Senovážná 3. Konkrétní datum a čas zaškolení určí objednatel po dohodě s poskytovatelem a s přihlédnutím ke lhůtám podle čl. II.
7. Řešení musí umožňovat snižování počtu Aktiv bez účasti pracovníků poskytovatele nebo dodatečných finančních nákladů objednatele.
8. Objednatel se zavazuje **za poskytnutá plnění hradit ceny dle čl. IV**.

Článek II

Lhůty, předání a převzetí díla, místo plnění

1. Plnění bude provedeno v následujících lhůtách:

    a) **Do 20 pracovních dnů od podpisu této smlouvy** poskytovatel poskytne, nainstaluje, zprovozní a implementuje do systémového prostředí objednatele (viz příloha č. 2) Řešení **v testovacím rozsahu 50 objednatelem určených Aktiv** (ve smyslu přílohy

č. 1), zaškolí osoby určené objednatelem a předá Řešení objednateli do ověřovacího provozu při naplnění podmínek podle kap. 1 přílohy č. 3.

b) **Do 80 pracovních dnů od podpisu této smlouvy** poskytovatel poskytne, nainstaluje, zprovozní a implementuje do systémového prostředí objednatele (viz příloha č. 2) Řešení **v plném rozsahu 1 400 Aktiv** (ve smyslu přílohy č. 1) v souladu s čl. I odst. 1 a přílohou č 1.

c) Bylo-li Řešení podle odst. 2 tohoto článku převzato s výhradami, pak **ve lhůtách určených v předávacím protokolu** poskytovatel odstraní vady Řešení v tomto protokolu uvedené.

d) **Do 20 pracovních dnů ode dne doručení žádosti podle čl. I odst. 4 poskytovateli** poskytovatel poskytne, nainstaluje, zprovozní a implementuje do systémového prostředí objednatele (viz příloha č. 2) rozšíření Řešení navýšením počtu Aktiv (ve smyslu přílohy č. 1) podle příslušné žádosti.

e) **V termínu podle žádosti podle čl. I odst. 5** poskytovatel poskytne objednatelem požadované plnění podle příslušné žádosti. **Poskytovatel není povinen plnění podle příslušné žádosti poskytnout, pokud je termín pro poskytnutí plnění v příslušné žádosti stanoven dříve, než 5 pracovních dnů ode dne doručení žádosti poskytovateli.**

2. **Řešení v plném rozsahu (podle odst. 1 písm. b) tohoto článku)** bude předáno na základě předávacího protokolu, který podepíše alespoň jedna pověřená osoba za každou smluvní stranu; vzor předávacího protokolu je přílohou č. 4. Vykazuje-li Řešení v okamžiku předání vady, **je převzato s výhradami** a objednatel, po projednání s poskytovatelem, určí v předávacím protokolu **pro každou z vad závaznou lhůtu pro její odstranění; lhůta může být stanovena i s odkládací podmínkou[1]; lhůta se nestanovuje pro neodstranitelné vady kategorie C**.

3. **Poskytovatel není oprávněn Řešení předat a objednatel není povinen Řešení převzít, nebyl-li ověřovací provoz nebo poslední opakovaný ověřovací provoz ukončen úspěšně.**

4. **Bez ohledu na úspěšné ukončení ověřovacího provozu není poskytovatel oprávněn Řešení předat a objednatel není povinen Řešení převzít, vyskytla-li se vada Řešení kategorie A, B, neodstranitelná vada kategorie C nebo více než 3 odstranitelné vady kategorie C (ve smyslu přílohy č. 3) v Řešení poté, co bylo poskytnuto, nainstalováno, zprovozněno a implementováno do systémového prostředí objednatele v plném rozsahu 1 400 Aktiv (ve smyslu přílohy č. 1).**

5. Objednatel si vyhrazuje možnost prodloužit lhůtu(y) uvedenou(é) v tomto článku, v příloze č. 3 a popř. v předávacím protokolu o předání Řešení, a to přiměřeně okolnostem, na základě písemné a odůvodněné žádosti poskytovatele, ve které poskytovatel doloží, že objektivně nemůže pokračovat v plnění dle této smlouvy z důvodu neposkytnutí povinné a nezbytné součinnosti objednatelem, nebo z důvodu skutečností stojících na straně poskytovatele, které ani poskytovatel jednající s náležitou péčí nemohl předvídat a které sám nezpůsobil (včetně např. výpadku či zdržení v dodavatelsko-odběratelském řetězci, výpadku v pracovní síle poskytovatele z důvodu opatření uložených orgány veřejné moci, nikoli však v důsledku protiprávního jednání poskytovatele, zdržení v plnění jiných smluvních partnerů objednatele, kterého se plnění dle této smlouvy dotýká a které nebylo způsobeno objednatelem). Žádost

[1] Např. do 5 pracovních dnů poté, co výrobce programového prostředku (SW) vydá příslušný update nebo patch.

poskytovatele dle tohoto odstavce musí být objednateli doručena v dostatečném předstihu před uplynutím lhůt(y) v tomto článku, v příloze č. 3 a popř. v předávacím protokolu o předání Řešení, a musí obsahovat i návrh jejich prodloužení, ten však není pro objednatele závazný. Úprava lhůt(y) bude provedena formou dodatku ke smlouvě.

6. Místem plnění budou prostory výpočetního střediska v objektech objednatele na adrese Praha 1, Senovážná 3 a Praha 5, Strojírenská 175 a dále jakékoliv místo, na kterém se nachází některé z Aktiv ve smyslu přílohy č. 1 této smlouvy.

Článek III

Poskytnutí technických prostředků

1. Bude-li za účelem plnění dle této smlouvy potřeba, aby poskytovatel poskytl objednateli technické prostředky (HW), pak:
    a) Technické prostředky (HW), s výjimkou paměťových médií podle písm. c) tohoto odstavce, zůstávají po celou dobu platnosti a účinnosti této smlouvy ve vlastnictví poskytovatele.
    b) Poskytovatel se objednateli zavazuje, že veškeré technické prostředky (HW), budou nové a nepoužité (maximálně z továrny zahořelé z výroby nebo zapnuté pro ověření funkčnosti v rámci kompletace technických prostředků poskytovatelem před poskytnutím).
    c) Poskytovatel bere na vědomí, že jakákoliv paměťová média (např. SSD, HDD, flash paměti), která budou poskytnuta jako technické prostředky (HW) nebo jejich součásti, přejdou okamžikem jejich poskytnutí objednateli do vlastnictví objednatele a budou po skončení této smlouvy zničena postupem určeným objednatelem.
    d) Objednatel se zavazuje neprovádět na poskytnutých technických prostředcích (HW) žádné technické zásahy, montáž či demontáž a zavazuje se používat poskytnuté technické prostředky (HW) pouze v souladu s uživatelskou dokumentací, kterou je mu povinen poskytovatel současně s poskytnutím technických prostředků (HW) předat. Uvedené se nevztahuje na paměťová média podle písm. c) tohoto odstavce.
    e) Objednatel se zavazuje po skončení této smlouvy předat poskytovateli všechny poskytnuté technické prostředky (HW), a to na základě výzvy poskytovatele, zaslané na e-maily pověřených osob dle této smlouvy. Uvedené se nevztahuje na paměťová média podle písm. c) tohoto odstavce.
2. Cena za případné poskytnutí technických prostředků (HW) je zahrnuta v ceně podpory Řešení dle čl. IV odst. 2 této smlouvy.

Článek IV

Cena a platební podmínky

1. Cena za plnění podle čl. I odst. 1, včetně odměny za poskytnutí licence podle dalších ustanovení této smlouvy, byla stanovena dohodou smluvních stran a činí 410 800 Kč bez DPH z toho cena za zaškolení objednatelem určených osob činí 0 Kč bez DPH. Cena zahrnuje veškeré náklady poskytovatele spojené s poskytnutím plnění dle čl. I odst. 1 a je konečná.

2. Cena za plnění podle čl. I odst. 3, včetně odměny za poskytnutí licence podle dalších ustanovení této smlouvy, byla stanovena dohodou smluvních stran a činí 405 000 Kč bez DPH ročně. Cena zahrnuje veškeré náklady poskytovatele spojené s poskytnutím plnění dle čl. I odst. 3.
3. Cena za plnění podle čl. I odst. 4 této smlouvy, včetně odměny za poskytnutí licence podle dalších ustanovení této smlouvy, byla stanovena dohodou smluvních stran a činí 110 000 Kč bez DPH za rozšíření Řešení navýšením počtu o každých 100 Aktiv (ve smyslu přílohy č. 1). Cena zahrnuje veškeré náklady poskytovatele spojené s poskytnutím plnění dle čl. I odst. 4.
4. Cena za plnění podle čl. I odst. 5 této smlouvy, včetně odměny za poskytnutí licence podle dalších ustanovení této smlouvy, byla stanovena dohodou smluvních stran a činí 12 800 Kč bez DPH za každý jeden člověkoden. Cena zahrnuje veškeré náklady poskytovatele spojené s poskytnutím plnění dle čl. I odst. 5.
5. K cenám dle odst. 1 až 4 tohoto článku se připočítá DPH v sazbě platné vždy v den uskutečnění zdanitelného plnění.
6. Cena podle odst. 1 tohoto článku bude hrazena na základě daňového dokladu, vystaveného vždy nejdříve v den předání a převzetí plnění; kopie protokolu o předání a převzetí plnění je přílohou dokladu k úhradě.
7. Cena podle odst. 2 tohoto článku bude hrazena ročně na základě daňového dokladu, vystaveného vždy nejdříve k výročí zahájení plnění podle čl. I odst. 3. V případě, že podpora Řešení bude ukončena jiným dnem, než posledním dnem roku, na který byla zaplacena, je objednatel oprávněn žádat vrácení alikvotní části ceny uhrazené za podporu Řešení pro daný rok.
8. Cena podle odst. 3 tohoto článku bude hrazena na základě daňového dokladu, vystaveného vždy nejdříve v den uskutečnění zdanitelného plnění, tj. v den předání a převzetí plnění podle čl. I odst. 4; kopie příslušné žádosti, s podpisem pověřené osoby objednatele potvrzujícím uskutečnění zdanitelného plnění, je přílohou dokladu k úhradě.
9. Cena podle odst. 4 tohoto článku bude hrazena na základě daňového dokladu, vystaveného vždy nejdříve v den uskutečnění zdanitelného plnění, tj. v den poskytnutí plnění podle čl. I odst. 5; kopie příslušné žádosti, s podpisem pověřené osoby objednatele potvrzujícím uskutečnění zdanitelného plnění, je přílohou dokladu k úhradě.
10. Doklad k úhradě (fakturu) zašle poskytovatel vždy elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej poskytovatel v analogové formě na adresu:

    Česká národní banka
    sekce rozpočtu a účetnictví
    odbor účetnictví
    Na Příkopě 28
    115 30 Praha 1
11. Doklady k úhradě budou obsahovat údaje podle § 435 občanského zákoníku a bankovní účet, na který má být placeno, a který je uveden v záhlaví této smlouvy nebo který byl později

aktualizován poskytovatelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References). Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je ČNB oprávněna jej vrátit poskytovateli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.

12. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřená osoba poskytovatele povinna na základě výzvy ČNB sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle předchozí věty.
13. Poskytovatel je oprávněn navrhnout objednateli změnu cen podle odst. 2 až 4 v návaznosti na vývoj indexu cen v tržních službách, stejné období předchozího roku = 100, konkrétně index „J62“ Služby v oblasti programování a poradenství a související služby, sloupec „Průměr od počátku roku“, a to průměr za předchozí kalendářní rok, který vyhlašuje Český statistický úřad. Úpravu cen je poskytovatel oprávněn navrhnout nejdříve po uplynutí jednoho roku ode dne nabytí účinnosti smlouvy. Úpravy cen budou prováděny písemnými dodatky ke smlouvě podepsanými oprávněnými zástupci obou smluvních stran.
14. Splatnost dokladu k úhradě je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.
15. Smluvní strany se ve smyslu ustanovení § 1991 občanského zákoníku dohodly, že je objednatel oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.

Článek V

Licenční ujednání

1. Poskytovatel tímto poskytuje objednateli nevýhradní, místně neomezené právo užívat jakékoliv, v rámci plnění dle této smlouvy objednateli poskytnuté či zpřístupněné, autorské dílo či jiný předmět duševního vlastnictví, a to s množstevním omezením vyplývajícím toliko z rozsahu Řešení, tj. počtu Aktiv (ve smyslu přílohy č. 1), a bez jakýchkoli dalších množstevních omezení (počtem současně připojených uživatelů, výpočetních jader, kategoriemi uživatelského přístupu atd.) (dále též „licence“).
2. Licence výslovně zahrnuje i autorská díla či jiné předměty duševního vlastnictví, poskytnuté nebo zpřístupněné objednateli třetími osobami na základě jednání poskytovatele dle této smlouvy. Licence výslovně zahrnuje i aktualizace či jiné úpravy Řešení v rámci podpory Řešení, tj. update / upgrade / patch / hotfix atd.
3. Licenci ve stanoveném rozsahu zajistí poskytovatel objednateli vždy nejpozději v den poskytnutí či zpřístupnění příslušného plnění dle této smlouvy.
4. Odměna za poskytnutí licence je zahrnuta v cenách plnění podle čl. IV této smlouvy.
5. Objednatel není povinen poskytnutou licenci využít ani zčásti.
6. Poskytovatel prohlašuje, že mu v zajištění uvedené licence nebrání žádná práva třetích osob a zajištěná licence bude prostá jakýchkoliv právních vad, jinak odpovídá za škodu způsobenou nepravdivostí tohoto prohlášení.

Článek VI

Pověřené osoby

1. Pověřenými osobami smluvních stran jsou:

   a) za objednatele **s oprávněním podepsat žádost** podle čl. I odst. 4 nebo 5 této smlouvy:

   [redacted]

   b) za objednatele **bez oprávnění podepsat žádost** podle čl. I odst. 4 nebo 5 této smlouvy:

   [redacted]

   c) za poskytovatele:

   [redacted]

2. V případě změny v osobě nebo údajích uvedených v odst. 1 tohoto článku je smluvní strana, která změnu provedla, povinna změnu druhé smluvní straně oznámit bez zbytečného odkladu. Změna je účinná dnem doručení jejího oznámení e-mailem pověřeným osobám druhé smluvní strany, bez povinnosti uzavřít dodatek.

Čl. VII

Osoby poskytovatele poskytující plnění

1. Poskytovatel je povinen:

   a) V souladu s ust. § 105 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), poskytnout objednateli identifikační údaje všech poddodavatelů, kteří nebyli identifikováni dle věty první uvedené v § 105 odst. 3 ZZVZ a kteří se následně zapojí do plnění předmětu dle této smlouvy, a to nejpozději před zahájením plnění předmětu dle této smlouvy poddodavatelem;

   b) V případě poskytování služeb prostřednictvím poddodavatele platí všechna ustanovení tohoto článku také pro poddodavatele a jeho pracovníky, kteří se budou na plnění smlouvy podílet. V případě, že poskytovatel splnil některý z požadavků stanovených objednatelem v zadávací dokumentaci zadávacího řízení na předmět této smlouvy prostřednictvím poddodavatele, je povinen v případě změny tohoto poddodavatele požádat objednatele o souhlas a prokázat, že nový poddodavatel tento požadavek splňuje, a to do 5 pracovních dnů přede dnem zahájení poskytování plnění dle této smlouvy poddodavatelem. Odsouhlasení změny poddodavatele bude provedeno e-mailem alespoň jednou pověřenou osobou objednatele, bez povinnosti uzavřít dodatek k této smlouvě;

   c) Za plnění poskytovaná poddodavatelem je poskytovatel odpovědný jako by toto plnění poskytoval sám. Poskytovatel se zavazuje, že poskytne objednateli, pokud bude i část plnění poskytována poddodavatelem, seznam kontaktních údajů na osoby provádějící plnění za poddodavatele. Objednatel je oprávněn průběh plnění realizovaný poddodavatelem řešit napřímo s jeho pracovníky a poskytovatel není oprávněn tuto komunikaci s poddodavatelem či jeho

pracovníky jakkoliv omezovat nebo mařit.

Článek VIII

Mlčenlivost, bezpečnostní požadavky objednatele, požadavky na doložení ISO a SOC, další povinnosti poskytovatele

1. Poskytovatel se zavazuje zajistit, že veškeré osoby podílející se na plnění dle této smlouvy zachovají mlčenlivost o všech skutečnostech, se kterými se seznámí v průběhu plnění této smlouvy a které nejsou veřejně dostupné. Povinnost mlčenlivosti trvá i po skončení platnosti smlouvy.
2. Pracovníci či poddodavatelé poskytovatele a jejich pracovníci smí používat informace získané v souvislosti s plněním dle této smlouvy výhradně pro účely plnění této smlouvy. Dostane-li se kterákoliv z osob uvedených v tomto odstavci v průběhu plnění do kontaktu s údaji objednatele vyplývajícími z jeho provozní činnosti, zavazuje se tyto údaje nezneužít, nezměnit ani nijak nepoškodit, neztratit či neznehodnotit.
3. Poskytovatel se zavazuje zajistit, aby jeho pracovníci či poddodavatelé poskytovatele a jejich pracovníci v plném rozsahu dodržovali bezpečnostní požadavky objednatele uvedené v příloze č. 5 této smlouvy.
4. Poskytovatel se zavazuje **do 10 pracovních dnů ode dne uzavření této smlouvy a dále do 2 měsíců od skončení platnosti předchozího certifikátu** objednateli doložit, že výrobce Řešení má platnou certifikaci podle normy ISO/IEC 27001:2013 Information Security Management Systém pokrývající vývoj software.
5. Poskytovatel se zavazuje objednateli doložit zprávu nezávislého auditora SOC 2 Type 2, obsahující popis a stav bezpečnostních opatření, chránících Řešení v uplynulém roce, a to v následujících termínech:
    a) do 10 pracovních dnů ode dne uzavření smlouvy zprávu za rok 2020 nebo 2021,
    b) bezodkladně poté co ji má k dispozici, nejpozději do 3. září každého roku zprávu za rok předcházející.
6. Poskytovatel se dále zavazuje, že v souvislosti s plněním dle této smlouvy:
    a) zajistí legální zaměstnávání osob a férové a důstojné pracovní podmínky pro všechny pracovníky podílející se na plnění této smlouvy. Férovými a důstojnými pracovními podmínkami se přitom rozumí takové pracovní podmínky, které splňují alespoň minimální standardy stanovené pracovněprávními a mzdovými předpisy. Poskytovatel je povinen zajistit splnění požadavků dle tohoto ustanovení i u svých poddodavatelů;
    b) zajistí řádné a včasné plnění finančních závazků vůči svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá poskytovateli v souvislosti s touto smlouvou, a to nejpozději do 10 dnů od obdržení platby ze strany objednatele (pokud již splatnost poddodavatelem vystavené faktury nenastala dříve). Objednatel je oprávněn požadovat předložení dokladů o provedených platbách poddodavatelům.

Článek IX

Kybernetická bezpečnost

1. Poskytovatel bere na vědomí, že objednatel je správcem informačních systémů kritické

informační infrastruktury dle ustanovení § 3 písm. c) ZKB a správcem významných informačních systémů dle ustanovení § 3 písm. e) ZKB uvedených v preambuli této smlouvy. Poskytovatel dále bere na vědomí, že poskytování služeb uvedených v čl. I bude prováděno na aktivech systémů kritické informační infrastruktury a aktivech významných informačních systémů.

2. Poskytovatel je při plnění této smlouvy v postavení významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 VKB a bere na vědomí, že po dobu účinnosti této smlouvy bude veden v evidenci významných dodavatelů objednatele ve smyslu § 8 odst. 1 písm. b) a c) VKB.
3. Rozsah zapojení poskytovatele na zajištění bezpečnosti aktiv informačních systémů kritické informační infrastruktury a aktiv významných informačních systémů používaných v prostředí objednatele je určen předmětem této smlouvy.
4. Poskytovatel je při poskytování plnění oprávněn užívat data předaná mu objednatelem za účelem plnění předmětu smlouvy či data za tímto účelem získaná pouze v rozsahu nezbytném ke splnění smlouvy a pouze v souladu s touto smlouvou a příslušnými právními předpisy, tj. zejména ZKB a VKB.
5. Poskytovatel se zavazuje zajistit, aby jeho pracovníci či poddodavatelé poskytovatele a jejich pracovníci v plném rozsahu dodržovali obecná pravidla pro dodavatele v oblasti bezpečnosti IT uvedená v příloze č. 5 této smlouvy (dále jen „pravidla bezpečnosti“).
6. Poskytovatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy, a zajistit ve spolupráci s objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční a efektivní.
7. Poskytovatel je srozuměn s tím, že objednatel provádí v pravidelných intervalech hodnocení rizik v souvislosti s informačními systémy dle odst. 1 tohoto článku, kterých se týká poskytování plnění dle této smlouvy.
8. Dojde-li u poskytovatele nebo konečného poskytovatele cloudových služeb nebo dodavatele informací o zranitelnostech nebo výrobce Řešení k výskytu bezpečnostních incidentů souvisejících s plněním této smlouvy, zavazuje se poskytovatel o těchto bezpečnostních incidentech bezodkladně informovat objednatele. Poskytovatel se dále zavazuje oznamovat objednateli bezodkladně neobvyklé chování informačních systémů, jichž se plnění dle této smlouvy dotýká, a podezření na jakékoliv zranitelnosti bezpečnosti informací.
9. Poskytovatel se zavazuje informovat objednatele o významné změně ovládání poskytovatele nebo konečného poskytovatele cloudových služeb nebo dodavatele informací o zranitelnostech nebo výrobce Řešení, a to do 5 pracovních dnů od uskutečnění této změny. Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů či ekvivalentní postavení.
10. Poskytovatel se zavazuje informovat objednatele o změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými poskytovatelem nebo konečným poskytovatelem cloudových služeb nebo dodavatelem informací o zranitelnostech nebo výrobcem Řešení k plnění této smlouvy, a to do 5 pracovních dnů od uskutečnění této změny.
11. Poskytovatel je povinen zajistit, aby byly v případě ukončení smlouvy veškerá data a informace získané či vzniklé v souvislosti s plněním této smlouvy likvidovány bezpečným způsobem, který zaručí, že nebude možné zrekonstruovat jednotlivé datové struktury, části dat a informací do podoby, jež by umožnila identifikovat obsah a zpracování nebo použití

dat a/nebo informací na konkrétním nosiči dat. Poskytovatel je přitom povinen zajistit soulad postupu při likvidaci dat s přílohou č. 4 VKB.

12. Dojde-li za dobu účinnosti této smlouvy ke změnám ZKB a/nebo VKB takového charakteru a rozsahu, že s nimi nebude smlouva v souladu, zavazují se smluvní strany uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava či doplnění práv a povinností smluvních stran nezbytných k nápravě tohoto stavu, a to bez zbytečného odkladu poté, co legislativní změny ZKB a/nebo VKB nabydou platnosti.

Článek X

Smluvní pokuty a úrok z prodlení

1. V případě prodlení poskytovatele ve lhůtě podle čl. II odst. 1 písm. a) nebo písm. b) je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 5 000,- Kč za každý pracovní den prodlení.
2. V případě prodlení poskytovatele s odstraněním vad ve lhůtách podle čl. II odst. 1 písm. c) je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 500,- Kč za každou vadu kategorie C a každý pracovní den prodlení, ve výši 2 000,- Kč za každou vadu kategorie B a každý pracovní den prodlení a ve výši 5 000,- Kč za každou vadu kategorie A a každý pracovní den prodlení
3. V případě prodlení poskytovatele ve lhůtě podle čl. II odst. 1 písm. d) je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 500,- Kč za každých 100 Aktiv, o které má být Řešení rozšířeno podle příslušné žádosti, a každý pracovní den prodlení.
4. V případě nedodržení termínu poskytovatelem podle čl. II odst. 1 písm. e) je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 2 000,- Kč za každý neplněný člověkoden, kteří měl být součástí plnění podle příslušné žádosti.
5. V případě nedostupnosti příjmu hlášení vad Řešení podle čl. I odst. 3 delší než 48 hodin je objednatel oprávněn požadovat 5 000,- Kč za každou další hodinu nedostupnosti příjmu hlášení vad Řešení; na plynutí času podle tohoto odstavce nemá vliv jakákoliv provozní, pracovní či jinak stanovená doba dostupnosti příjmu hlášení vad Řešení.
6. V případě, že se kdykoliv poté, co bylo poskytnuto, naistalováno, zprovozněno a implementováno do systémového prostředí objednatele v plném rozsahu 1 400 Aktiv (ve smyslu přílohy č. 1), vyskytne v Řešení v průběhu 12 po sobě jdoucích měsíců více než třikrát vada kategorie A, vada kategorie A, jejíž odstranění trvalo déle 10 pracovních dnů, více než šestkrát vada kategorie B, vada kategorie B, jejíž odstranění nebo nalezení workaroundu trvalo více ne 20 pracovních dnů, nebo neodstranitelná vada jakékoliv kategorie, je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 200 000,- Kč za každý takový případ.
7. V případě porušení kterékoli povinnosti poskytovatele podle čl. VII nebo VIII odst. 1 až 3, nebo čl. IX, je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 200 000,- Kč za každý takový případ.
8. V případě prodlení poskytovatele ve lhůtě podle čl. VIII odst. 4 nebo 5 je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 50 000,- Kč za každý pracovní den prodlení.
9. V případě prodlení s uhrazením daňového dokladu zaplatí objednatel poskytovateli úrok z prodlení podle předpisů občanského práva.
10. Smluvní pokutou není dotčen nárok na náhradu škody.

11. Smluvní pokuty a úroky z prodlení jsou splatné do 14 kalendářních dnů ode dne doručení dokladu k úhradě povinné smluvní straně. Úhradou smluvní pokuty není dotčena povinnost uhradit škodu v plné výši vzniklou v důsledku neplnění povinnosti podle této smlouvy. Povinnost uhradit smluvní pokutu je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.

Článek XI

Trvání smlouvy, výpověď smlouvy a odstoupení od smlouvy

1. Tato smlouva se uzavírá na dobu neurčitou. Smlouvu lze ukončit písemnou výpovědí bez udání důvodu. Poskytovatel je oprávněn smlouvu vypovědět nejdříve po uplynutí 4 let od okamžiku předání a převzetí Řešení. Výpovědní doba činí 6 měsíců a počíná běžet první den kalendářního měsíce následujícího po doručení výpovědi druhé smluvní straně.
2. V případě, že se kdykoliv poté, co bylo poskytnuto, naistalováno, zprovozněno a implementováno do systémového prostředí objednatele v plném rozsahu 1 400 Aktiv (ve smyslu přílohy č. 1), vyskytne v Řešení v průběhu 12 po sobě jdoucích měsíců více než třikrát vada kategorie A, vada kategorie A, jejíž odstranění trvalo déle 10 pracovních dnů, více než šestkrát vada kategorie B, vada kategorie B, jejíž odstranění nebo nalezení workaroundu trvalo více ne 20 pracovních dnů, nebo neodstranitelná vada jakékoliv kategorie, je objednatel oprávněn vypovědět smlouvu bez výpovědní doby.
3. Pokud došlo k porušení kteréhokoliv ustanovení podle čl. VII nebo VIII odst. 1 až 5 nebo ustanovení podle čl. IX odst. 8 (vč. prodlení ve lhůtě tam uvedené), je objednatel oprávněn vypovědět smlouvu bez výpovědní doby.
4. V případě, že některá ze smluvních stran podstatně poruší smluvní povinnost vyplývající pro ni z této smlouvy, je druhá smluvní strana oprávněna od smlouvy odstoupit. Objednatel je oprávněn odstoupit i od části smlouvy.
5. Za podstatné porušení smluvní povinnosti ze strany poskytovatele se považuje zejména:
    a) prodlení poskytovatele ve kterékoliv lhůtě podle čl. II delší než 20 pracovních dnů;
    b) nedodržení termínu poskytovatelem podle čl. II odst. 1 písm. e) o více než 20 člověkodnů za dobu účinnosti smlouvy;
    c) pokud byl ověřovací provoz opakován více než jednou.
6. Za podstatné porušení smluvní povinnosti ze strany objednatele se považuje zejména:
    a) pokud je objednatel v prodlení s úhradou kteréhokoliv daňového dokladu k úhradě delším než 30 dnů.
7. Objednatel je dále oprávněn odstoupit od smlouvy, pokud dojde k významné změně kontroly nad poskytovatelem, nebo konečným poskytovatelem cloudových služeb nebo dodavatelem informací o zranitelnostech nebo výrobcem Řešení, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými poskytovatelem k plnění této smlouvy a tato změna bude objednatelem vyhodnocena jako bezpečnostní riziko ve smyslu ZKB a/nebo VKB.
8. Smluvní strany se dále dohodly, že objednatel je oprávněn odstoupit od smlouvy kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele.

9. Odstoupení od smlouvy je účinné dnem doručení oznámení o odstoupení od smlouvy druhé smluvní straně.
10. Odstoupením od smlouvy nejsou dotčena ustanovení týkající se vyrovnání smluvních závazků, smluvních pokut, závazku mlčenlivosti poskytovatele a ustanovení týkající se takových práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení.

Článek XII

Uveřejnění smlouvy a dalších souvisejících skutečností

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle ZZVZ, uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.
3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XIII

Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
2. Smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.
3. Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě uvedeno jinak. Za písemnou formu nebude pro účel uvedený v tomto odstavci považována výměna e-mailových či jiných elektronických zpráv, není-li ve smlouvě uvedeno jinak.
4. Poskytovatel není oprávněn postoupit práva, povinnosti anebo závazky z této smlouvy třetí osobě nebo osobám bez předchozího písemného souhlasu objednatele.
5. Závazkové vztahy touto smlouvou založené se řídí českým právním řádem, zejména občanským zákoníkem.
6. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní, bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
7. Odpověď strany této smlouvy podle § 1740 odst. 3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
8. Uplatnění domněnky doby dojití dle § 573 občanského zákoníku se vylučuje.
9. Smlouva je vyhotovena ve třech stejnopisech s platností originálu, z nichž objednatel obdrží dva stejnopisy a poskytovatel jeden stejnopis.

Přílohy:

č. 1 Technické podmínky předmětu plnění

č. 2 Systémové prostředí objednatele

č. 3 Ověřovací provoz

č. 4 Vzor předávacího protokolu

č. 5 Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

V Praze dne 27. 6. 2022

Za objednatele:

[redacted]

Ing. Milan Zirnsák

ředitel sekce informatiky

[redacted]

Ing. Zdeněk Virius

ředitel sekce správní

[redacted]

ČNB ČESKÁ NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1
48

V Praze dne 24. 6. 2022

Za poskytovatele:

[redacted]

Ing. Michal Zipaj, MBA

jednatel

[redacted]

RAC
Risk Analysis Consultants, s.r.o.
Konviktská 24, 110 00 Praha 1
Tel.: 222 360 001 www.rac.cz
DIČ: 63672774

Příloha č. 1

Technické podmínky předmětu plnění

1. Požadavky na Řešení

Řešení musí odpovídat smlouvě a následujícím podmínkám

2. Rozsah Řešení

Řešení musí být plně způsobilé pro skenování nejméně 1400 zařízení resp. unikátních IP adres (dále jen „Aktiva“). **Řešení musí umožňovat odebrání/přidání Aktiva bez nutnosti asistence výrobce nebo poskytovatele.**

3. Rozšiřitelnost Řešení

Řešení musí být schopno dalšího rozšíření (licenčně i funkčně) na žádosti objednatele až do potenciální celkové výše 3 000 Aktiv, a to po balíčcích vždy o 100 Aktivech (překročení počtu 3 000 Aktiv je možné, avšak není požadováno).

4. Skenování zranitelností

Řešení musí podporovat skenování zařízení v ČNB používaných platforem (Windows, Linux (RedHat, Debian a jejich klony), VMware, Checkpoint produkty, Oracle produkty, Cisco produkty)

Řešení musí umožňovat

- neautentizované skeny (bez ověření na skenovaném Aktivu, někde uváděné jako network scan)
- autentizované skeny, kterými rozumí sken, který ke zjišťování zranitelností využívá platné ověření/přihlášení do skenovaného Aktiva (např. operační systém, aplikace, databáze apod.). Ověření/autentizace musí být možné pomocí jména/hesla i pomocí private/public klíče (na Aktivech, která ověření klíčem podporují). Musí být zajištěno bezpečné uložení přihlašovacích údajů v Řešení. Řešení musí podporovat ukládání a vyzvedávání údajů pro autentizované skeny v credential vault řešení CyberArk PIM Suite.
- skenování webových aplikací včetně autentizace pomocí jména/hesla, nebo klíče (PKI)
- tzv. mapping - základní skeny sítě/ip rozsahů (obdoba NMAPu) bez nutnosti mít pro tyto skeny subscription – to znamená, že mapping nesmí být omezen počtem Aktiv, které pokrývá licence

Součástí Řešení je i endpoint agent, který je podporovaný na operačním systému (dále též „OS“) Windows (Win 7 a vyšší, Windows Server 2012 R2 a vyšší) a Linux (Red Hat a Oracle Enterprise Linux). Agentem je myšlen software, nebo služba, která se instaluje na koncové zařízení (Aktivum) a zajišťuje alespoň skenování zranitelností na Aktivu a sběr informací o Aktivu

V Řešení musí být dostupný seznam proběhlých skenů s možností vyhledávání alespoň podle cíle skenu, názvu skenu a data spustění. Musí být možné vyhledat všechny skeny, v rámci kterých bylo určité Aktivum skenované. Seznam musí obsahovat historii proběhlých skenů alespoň 90 dnů.

V Řešení musí být možnost vytvářet profily skenování – definice skenovaných portů, nebo jejich rozsahů, úrovně intenzity skenování, parametrů autentikace, HTTP hlaviček apod.

Řešení musí umožňovat plánovat spouštění skenovacích úloh a reportů (viz dále) jednorázově i v pravidelných intervalech – tzv. scheduling

5. Zranitelnosti

Informace o jednotlivých zranitelnostech musí obsahovat alespoň

- podrobný popis zranitelnosti – tj. v čem zranitelnost spočívá, čeho se týká
- popis dopadu zranitelnosti – tj. co se stane, když bude zranitelnost zneužita
- závažnost (severity) – alespoň ve škále 1-5, s možností manuální úpravy
- číslo CVE a odkaz na oficiální CVE ID zdroje - např. MITRE
- skóre podle metodiky Common Vulnerability Scoring System (CVSS)
- kontrolované parametry - např. existence souborů, verze souborů, klíče v registrech, verze produktu apod. a hodnoty těchto parametrů, které byly skenem zjištěny
- dotčené systémy a jejich verze
- odkaz na relevantní zdroje výrobce produktu, týkající se zranitelnosti
- informace o existenci/dostupnosti patche, a pokud existují, tak i návody na odstranění zranitelnosti
- informace o existenci exploitu, nebo exploitů a případný odkaz na ně
- changelog – tj. datum zveřejnění v Řešení, datum poslední změny, popis případných změn

Řešení musí disponovat možností definovat a provádět dotazy do databáze zranitelností

6. Aktiva

- Řešení obsahuje evidenci Aktiv. Údaje k jednotlivým Aktivům musí být možné přiřazovat automaticky (na základě informací získaných ze skenů – např. DNS hostname, operační systém a jeho verze) a manuálně – například vlastník Aktiva. V evidenci aktiv musí být možné vyhledávat podle údajů, které jsou u Aktiv evidované. Musí být možné vytvářet a evidovat skupiny Aktiv s možností mít pro tyto skupiny přiřazeného vlastníka. U Aktiva musí být možné smazat všechny uložené údaje a následně ho oskenovat „načisto“
- Řešení musí disponovat funkcí manuálního i automatického „tagování“. Tím je myšlena možnost jednotlivým Aktivům přiřazovat tagy (značky, štítky) buď manuálně, nebo na základě definovaných pravidel. Tagy následně umožňují vykonávat akce nad více aktivy najednou (vyhledávání, skenování, změna atributů, reporting a další).
- Řešení musí obsahovat vazbu mezi jednotlivými zranitelnostmi a Aktivy, na kterých byla zranitelnost detekována

7. Uživatelé

- Řešení obsahuje management uživatelů a uživatelských rolí s různou úrovní oprávnění. Ověřování uživatelů je realizováno pomocí uživatelského jména a hesla, nebo certifikátu. V případě hesel musí být možné nastavit politiku hesel (délka, složitost/komplexita, maximální doba platnosti). U uživatelů musí být evidovaná historie přihlášení do Řešení a musí být možné disablovat účet uživatele (bez nutnosti smazání z Řešení).
- Řešení musí umožňovat vícefaktorovou autentizaci uživatele.
- Musí být zajištěno, že každý uživatel má přístup pouze k Aktivům, nebo skupinám Aktiv, jejichž je vlastníkem. Přístupem jsou myšleny především záznamy v evidenci Aktiv, výsledky skenů a možnost plánování a spouštění skenů a reportů. V Řešení musí být uživatelská role, umožňující plný přístup ke všem Aktivům, položkám a zalicencovaným fuknčím Řešení.

8. Reporting – přehledy zranitelností

- generované reporty
  - manuální, nebo automatizované generování reportů zranitelností nad jednotlivými Aktivy, nebo skupinami Aktiv s možností zasílání reportů emailem.
  - předdefinované šablony reportů.
  - formát reportů musí umožňovat aktivně se v reportech pohybovat pomocí odkazů (linků), alespoň v úrovni jednotlivých skenovaných Aktiv
- dostupné přímo v Řešení
  - přehledy zranitelností jednotlivých Aktiv/skupin Aktiv s možností filtrování informací o zranitelnostech (Aktivum, závažnost, doba výskytu apod.)
  - závažnosti zranitelností
  - časové informace o prvním nálezu zranitelnosti a době trvání výskytu s možností filtrování

9. Ticketing

Řešení obsahuje workflow pro sledování nálezů/zranitelností použitelné v enterprise prostředí

10.Skenery

- součástí Řešení musí být kromě interních skenerů (1x skener v LAN a 3x skener v DMZ) i v internetu umístěný skener umožňující skeny skrze internetový firewall „zvenku“ umožňující objednateli provádět skeny Aktiv dosažitelných z internetu.
- Pokud budou využity virtuální skenery, budou poskytnuty ve formě připravených images (OS včetně Řešení) pro virtualizační platformy VMware a Oracle. V případě, že skenery nejsou poskytovány formou images, ale je třeba instalace OS, pak musí být podporovaný RedHat Enterprise Linux verze 7.5 a vyšší. Hypervizor a OS budou plně pod správou zaměstnanců objednatele a dodavatel nebude mít vzdálený přístup do žádné části řešení. On-site přístup je možný za dohledu pracovníků objednatele.

11.Ostatní – bezpečnost, logování, notifikace

- Správcovský přístup do Řešení (management, skenovací appliance apod.) z klientské stanice musí být realizován pomocí šifovaného spojení, v případě HTTPS protokolem TLS verze 1.2 a vyšší.
- V Řešení musí být logovány veškeré proběhlé akce a aktivity a musí být zachována historie za posledních nejméně 90 dní. Zásadní jsou informace týkající se uživatelů (přihlášení, odhlášení, změna), skenů, reportů a naplánovaných úloh (spuštění, dokončení, změna parametrů), a Aktiv a jejich skupin (přidání, smazání, změna). Řešení musí být schopné posílat data do systému typu SIEM, konkrétně musí být podporován systém ArcSight
- Řešení musí mít funkcionalitu emailových notifikací pokrývající alespoň následující oblasti
    - skeny - start, dokončení
    - reporty - dokončení, zaslání výsledků
    - vypršení platnosti hesla u uživatelského účtu
    - vypršení platnosti subscription/licence
- Řešení má zdokumentované API pro napojení na CMDB

12.Updaty

- Výrobce pravidelně poskytuje update databáze zranitelností i samotného Řešení. Stahování updatů probíhá z internetu (v případě updatů databáze zranitelností je nutné, aby stažení i update proběhl automaticky bez nutnosti zásahu administrátora) a výrobce musí být schopen definovat internetovou adresu zdroje aktualizací (buď jako FQDN, nebo jako IP adresu, nebo seznam, případně rozsah IP adres)
- K Řešení musí být po celou dobu smluvního vztahu poskytovány updaty odstraňující zjištěné zranitelnosti v jednotlivých komponentách Řešení

Příloha č. 2

Systémové prostředí objednatele

1. STANDARDNÍ SYSTÉMOVÉ PROSTŘEDÍ ČNB

Standardní systémové prostředí je soubor konkrétních produktů technického a programového vybavení včetně pravidel pro jejich provoz a dále seznam definovaných služeb, které souhrnně tvoří základní platformu pro provoz informačních systémů a informačních technologií (IS/IT) v prostředí České národní banky (ČNB).

1.1 Prostředí datové sítě

- Klientské stanice připojeny rychlostí typicky 1 $Gbsec^{-1}$ 1000Base-T
- Servery připojeny typicky rychlostí 10 $Gbsec^{-1}$ či v záloze 1$Gbsec^{-1}$ 1000Base-T
- Mezi servery a klientskými stanicemi pouze L3 konektivita, mezi servery možná L2 nebo L3 konektivita
- Adresace dle RFC 1918 (10.x.y.z)
- Plně přepínaná síť s redundantním jádrem

1.2 Serverové prostředí

- Platforma architektury x86/X64 - MS Windows Server 2016 Server, cp 1250

Platforma Red Hat Linux v. 7.x či vyšší a Oracle Enterprise Linux 7.0 a vyšší

Virtualizační platforma

- Platforma VMware vSphere 7.x
- Platforma Oracle VM 3.x

Centrální diskové kapacity

Slouží pro ukládání dat spravovaných databázovými systémy, pro sdílení programového vybavení a dat organizačních útvarů ČNB, poskytují prostor pro uložení dat jednotlivých uživatelů.

Jsou využita fault tolerantní disková pole instalované v geograficky vzdálených lokalitách.

Zálohování dat

Zálohování informačních systémů a dalších dat je v ČNB řešeno centrálně. Zálohována jsou pouze data uložená na centrálních kapacitách ve správě sekce informatiky. Pro zálohování je určen zálohovací systém HP Data Protektor 10.70 nebo vyšší.

Elektronická pošta

- Server elektronické pošty - MS Exchange 2016
- Klient elektronické pošty – MS Outlook 2016 nebo OWA

Tisková zařízení

- Síťová tisková zařízení,
- Komunikační protokol – TCP/IP,
- Podporované síťové služby – SNMP, DHCP, DNS.

Databázové servery

Data standardních IS jsou uložena v databázích Oracle:

- Oracle RDBMS 19
- Protokol Oracle Net

Zálohování dat provozních databází je zajištěno stanovenými prostředky a postupy.

Aplikační a WWW servery

- Oracle Web Logic Server 11, 12 a vyšší
- JBoss,

Monitoring systémů

- System Center Operations Manager 2019 – centrální sběr provozních logů
- SIEM HP ArcSight– sběr bezpečnostních logů

1.3 Prostředí klientské stanice

Klientská stanice uživatele je osobní počítač IBM-PC kompatibilní koncipovaný jako nástroj zajišťující přístup uživatele k centrálně provozovaným IS nebo virtualizovaný desktop (dále jen vDesktop) pomocí technologie Citrix. Minimální parametry klientské stanice provozované ve standardním systémovém prostředí ČNB:

- MS Windows 10 Enterprise edice LTSC , cp 1250 + aktuální aktualizace
- Citrix XenApp 7.x na MS Windows 2016 Serveru (virtuální desktop využívající MS terminálové služby)
- TCP/IP síťové služby (DHCP klient, SNMP klient)
- MS Office 2016 Professional Plus CZ
- WWW prohlížeče – IE11, Google Chrome (alternativně i Firefox)
- Adobe Acrobat Reader DC CZ – prohlížeč souborů ve formátu PDF
- Symantec EndPoint Protection v.14.x - antivirový program

Instalace programového vybavení na klientskou stanici je prováděna především prostřednictvím vzdálené automatické instalace (WDS). Instalace musí být kompatibilní se službou MS Installer (standardní služba operačního systému). Instalace programového vybavení na vDesktop je prováděna centrálně pomocí tzv. image z provisioning serverů.

Není přípustné ukládat na klientskou stanici/vDesktop data trvalé hodnoty, taková data je nutno ukládat na centrální diskové kapacity. Na klientské stanici nesmí být prováděno dávkové zpracování dat IS.

Dávkové zpracování centrálně uložených dat je přípustné spouštět a provádět pouze na databázovém serveru nebo případně na aplikačním serveru.

Uživatel nebo aplikace mohou ukládat na klientskou stanici dočasná data a programové komponenty, které jsou odvozeny z centrálně uložených dat, mohou také provádět lokální zpracování dat. Pro případné vytváření dočasných souborů a ukládání dat při činnosti komponent je třeba využívat předdefinované adresáře dostupné přes proměnné prostředí (USERPROFILE, TEMP, TMP, APPDATA). V případě vDesktop jsou data na lokálním disku po restartu serveru smazána.

Přístupová práva na klientských stanicích a vDesktop odpovídají defaultnímu nastavení od firmy Microsoft po instalaci MS Windows 10 Enterprise (v případě vDesktop se jedná o Win 2016). Výjimky pro potřeby aplikací je v nezbytných případech možné povolit po přesném definování potřebných změn v adresářích a v registrech a po náležitém zdůvodnění požadovaných změn. Výjimky jsou centrálně řízeny a aplikovány na klientské stanice a vDesktop prostřednictvím GPO (politiky v Active Directory). Obdobné požadavky platí i pro registrování knihoven a vytváření nebo změny hodnot klíčů v registrech.

Na klientské stanici a vDesktop pracuje uživatel standardně pod právy přidělené skupině „Users“.

Při realizaci informačního systému je nutné zajistit, aby programové komponenty realizovaného IS nebyly v rozporu s komponentami dalších provozovaných IS. Realizovaný IS tedy musí být provozovatelný v systémovém prostředí ČNB a současně nesmí narušovat funkčnost ostatních IS.

2. APLIKAČNÍ PROGRAMOVÉ VYBAVENÍ

2.1 Provozní prostředí

Standardní služby poskytované uživatelům ČNB v provozním prostředí jsou definovány v pokynech o provozování a správě produktů a služeb informačních systémů a informačních technologií v ČNB.

Zálohování dat provozních databází je spolehlivě zajištěno stanovenými prostředky a postupy.

Každý produkt IS/IT provozovaný v ČNB má stanoveného věcného a technického správce.

Dávkové zpracování dat uložených v databázi je možné provádět pouze na databázovém serveru nebo na aplikačním serveru.

2.2 Testovací prostředí

Testovací prostředí je odděleno od provozního prostředí. V testovacím prostředí není garantována dostupnost a funkcionalita instalovaných produktů IS/IT. Pro účely otestování některých produktů IS/IT mohou být vytvořena dílčí testovací prostředí s přesně definovaným rozsahem.

Testovací data musí být oddělena od provozních dat, nesmí obsahovat informace ve smyslu příslušných vnitřních předpisů o zásadách ochrany informací a utajovaných skutečností.

2.3 Vývojové prostředí

Standardní vývojové prostředí slouží pro vytváření aplikačního programového vybavení informačních systémů ČNB. Standardní vývojové prostředí ČNB tvoří produkty firmy Oracle v aktuální verzi.

Vývoj aplikačního SW se řídí relevantními částmi interních pokynů a metodiky projektování.

2.4 Funkce Single Sign-On

U IS ČNB je požadována realizace funkce Single Sign-On s využitím služby MS AD (autentizační protokol Kerberos).

2.5 Vazby na další IS

Napojení úlohy na informace z primárních zdrojů dat je standardně zajištěno prostřednictvím databázových pohledů na příslušné tabulky přes synonyma dostupná v databázi Oracle.

3. Organizační standardy

3.1 Rozvoj a provoz produktů IS/IT upravují následující pokyny ČNB

a) Pokyny ČNB o rozvoji informačních systémů a technologií v České národní bance - upravují metodiku pro řízení, plánování a realizaci rozvoje IS/IT v ČNB.

b) Pokyny o provozování a správě produktů a služeb informačních systémů a informačních technologií v ČNB upravují zásady provozování a užívání IS/IT.

c) Pokyny o bezpečnostní politice ČNB v oblasti informačních technologií upravují standardně platnou bezpečnostní politiku IS.

d) Interní metodika odboru projektování informačních systémů doplňuje pokyny o rozvoji IS/IT o další zásady a postupy při interním a externím vývoji a implementaci IS ve standardním systémovém prostředí ČNB.

Příloha č. 3

Ověřovací provoz

Objednatel zkontroluje funkčnost Řešení před jeho převzetím provedením ověřovacího provozu v systémovém prostředí objednatele (viz příloha č. 2) a ve zpřístupněném cloudovém prostředí. Při ověřovacím provozu se ověřuje, že **Řešení naplňuje všechny požadavky podle smlouvy (vč. jejích příloh) a že jako celek funguje, je schopné detekce zranitelností Aktiv a nezpůsobuje problémy v systémovém prostředí objednatele** (viz příloha č. 3).

Během ověřovacího provozu je poskytovatel povinen zajistit přítomnost pracovníků poskytovatele v dostatečném počtu, nejméně však jednoho pracovníka, a poskytovat součinnost objednateli k naplnění účelu ověřovacího provozu.

Průběh ověřovacího provozu, ani jeho opakování či opakování jakékoliv jeho části, nemá vliv na lhůty a doby podle smlouvy, resp. na jejich plynutí, nestanoví-li smlouva jinak.

1. Podmínky zahájení ověřovacího provozu:

    - poskytovatel poskytl, nainstaloval, zprovoznil a implementoval **Řešení v testovacím rozsahu 50 Aktiv do systémového prostředí objednatele** (viz příloha č. 2),
    - poskytovatel **zaškolil osoby určené objednatelem** podle čl. I odst. 1 a 6 smlouvy,
    - poskytovatel **poskytl objednateli technické prostředky (HW) a předal jejich uživatelskou dokumentaci** podle čl. III smlouvy, je-li jejich poskytnutí třeba za účelem plnění této smlouvy, a
    - poskytovatel **informoval e-mailem všechny pověřené osob objednatele, že je možno započít s ověřovacím provozem**.

2. Průběh ověřovacího provozu:

    Ověřovací provoz bude probíhat zejména:
    - prováděním skenů provozních a testovacích serverů a dalších technických Aktiv objednatele,
    - testováním integrace Řešení na systémy uvedené v této smlouvě,
    - dalším užíváním Řešení a všech jeho funkcionalit v systémovém prostředí objednatele (viz příloha č. 2),
    - dalšími operacemi s Řešením v systémovém prostředí objednatele (viz příloha č. 2), a
    - to vše při různých stupních zátěže.

3. Průběh ověřovacího provozu – kategorizace vad:

    Během ověřovacího provozu je **poskytovatel povinen průběžně odstraňovat zjištěné vady Řešení.**

    Každé zjištěné vadě Řešení, které nebude odstraněna poskytovatelem bezprostředně po jejím zjištění, bude **přidělena kategorie**:
    - **A – Kritická vada** – tj. vada, která znemožňuje či omezuje práci s Řešením, zapříčiňuje chování Řešení takového charakteru, že dochází k nenapravitelnému poškozování informací v Řešení uložených, resp. ke ztrátě důvěry v pravdivost a úplnost těchto informací, způsobuje problémy v systémovém prostředí objednatele (viz příloha č. 2), popř. jiným

závažným způsobem narušuje chod Řešení. Kritickými vadami jsou zejména:
- Řešení je nefunkční,
- Řešení při svém fungování zapříčiňuje porušování platných právních předpisů,
- Řešení při svém fungování zapříčiňuje ohrožení provozu nebo dostupnosti ostatních programových prostředků (SW) nebo technických prostředků (HW) v systémovém prostředí objednatele (viz příloha č. 2),
- není možné ovládání Řešení jako celku nebo není možné ovládání základních funkcí Řešení,
- není možné používání Řešení jako celku nebo je znemožněno používání základních funkcí Řešení,
- Řešení ohrožuje bezpečnost objednatele,
- došlo ke ztrátě dat uložených v Řešení a tato data nelze obnovit bez záruky, že jsou úplná a totožná k okamžiku ztráty,
- Řešení není schopno zpracovávat běžnou provozní zátěž.

- **B – Podstatná vada –** tj. vada, která podstatně ztěžuje práci s Řešením, zapříčiňuje chování Řešení takového charakteru, že dochází k poškozování informací v Řešení uložených, avšak informace uložené v Řešení lze obnovit s plnou důvěrou v jejich pravdivost a úplnost, popř. jiným způsobem narušuje chod Řešení. Podstatnými vadami jsou zejména**:**
  - není možné ovládání méně podstatných funkcí Řešení,
  - není možné používání méně podstatných funkcí Řešení,
  - došlo ke ztrátě dat uložených v Řešení, tato data lze však obnovit se zárukou, že jsou úplná a totožná k okamžiku ztráty,
  - Řešení není schopno zpracovávat maximální provozní zátěž.
- **C** – Nepodstatná vada – tj. vada, která není kritickou vadou ani podstatnou vadou, např. pravopisná nebo gramatická chyba v rozhraní Řešení.

O kategorizaci vady rozhodne s konečnou platností objednatel.

Poskytovatel je povinen bez zbytečného odkladu odstranit jakoukoliv zjištěnou vadu Řešení znemožňující pokračovat v ověřovacím provozu.

4. Výsledek ověřovacího provozu:

Do 30 pracovních dnů od naplnění podmínek pro zahájení ověřovacího provozu Řešení informuje kterákoliv z pověřených osob objednatele e-mailem pověřené osoby poskytovatele že:
- Řešení je bez vad nebo vykazuje pouze vadu/y kategorií B a/nebo C, které objednatel považuje za plně a snadno odstranitelné, včetně jejich výčtu, a tedy **ověřovací provoz byl ukončen úspěšně**;
- Řešení vykazuje vadu/y kategorie A nebo vadu/y kategorie B, které objednatel považuje za neodstranitelné nebo odstranitelné pouze obtížně, včetně jejich výčtu, a tedy **ověřovací provoz byl ukončen neúspěšně**;
- Řešení vykazuje vadu/y kategorie C, které objednatel považuje za neodstranitelné nebo odstranitelné pouze obtížně, včetně jejich výčtu:
  - avšak jejich počet nepřekračuje 3 a objednatel je považuje za natolik nevýznamné, že zájem na předání a převzetí Řešení převažuje a tedy **ověřovací provoz byl ukončen úspěšně**;

- a objednatel je považuje za natolik významné, že s nimi nelze Řešení převzít, nebo jejich počet překračuje 3, a tedy **ověřovací provoz byl ukončen neúspěšně**.

Lhůta podle předchozího odstavce neběží po dobu, po kterou není možno provádět ověřovací provoz:

- Protože poskytovatel neposkytuje potřebnou součinnost, zejména jeho pracovník či pracovníci se nejsou přítomni ověřovacímu provozu.
- Vyskytla se vada Řešení znemožňující pokračovat v ověřovacím provozu a nebyla doposud poskytovatelem odstraněna (zejména, avšak nikoliv výlučně, vady Řešení kategorie A).

Uvedené nemá vliv na další lhůty a doby podle smlouvy, resp. na jejich plynutí.

Pokud byl ověřovací provoz ukončen neúspěšně, může poskytovatel odstranit vady, které vedly k neúspěchu, a předat objednateli Řešení k opakování ověřovacího provozu; poté se opakuje ověřovací provoz obdobně podle této přílohy.

Při opakování ověřovacího provozu rozhoduje o jeho trvání objednatel. Zkrácení trvání ověřovacího provozu neopravňuje poskytovatele jakkoliv namítat, že nemohl odstranit vady Řešení, které se v opakovaném ověřovacím provozu projevily.

Byl-li ověřovací provoz opakován více než jednou, je objednatel oprávněn od smlouvy odstoupit podle čl. XI odst. 5 písm. c).

Poskytovatel není oprávněn Řešení předat a objednatel není povinen Řešení převzít, nebyl-li ověřovací provoz nebo poslední opakovaný ověřovací provoz ukončen úspěšně.

Příloha č. 4

Vzor předávacího protokolu

ČESKÁ ČNB NÁRODNÍ BANKA

Předávací protokol

Poskytovatel	**Objednatel**
	Česká národní banka **Na Příkopě 28** **115 03 Praha 1**
IČO: **DIČ:**	**IČO: 48136450** **DIČ: CZ48136450**

Evidenční číslo smlouvy v ČNB	
Název smlouvy	
Předmět předání:	

Dne …… poskytovatel předal a objednatel převzal ……

- ……
- ……

dle smlouvy …… (evidenční číslo ČNB: ……).

Převzato bylo **s výhradami/bez výhrad.**

Následné kroky, např.: *Poskytovatel akceptoval uvedené vady s tím, že odstraní vady* ***uvedené v příloze č.1*** *ve lhůtách tam uvedených atd*.

V Praze dne ……

Za poskytovatele: Za objednatele:

ČESKÁ ČNB NÁRODNÍ BANKA

Předávací protokol – Příloha č.1

Seznam vad a lhůty k odstranění vad

ID	Kategorie	Popis vady	Lhůta k odstranění vady

Příloha č. 5

Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu smlouvy nebo zadávací dokumentace nebo její jinou přílohou, má přednost ustanovení textu smlouvy nebo zadávací dokumentace nebo její jiná příloha.
2) Dodavatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
3) Dodavatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy s ČNB.
4) Dodavatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
5) Pracovníci dodavatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
6) Dodavatel a jeho pracovníci nejsou oprávněni:
   a) obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
   b) sdělovat své přístupové údaje k systémům ČNB;
   c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
   d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
7) Dodavatel a jeho pracovníci jsou povinni:
   a) okamžitě nahlásit sekci informatiky ČNB, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro dodavatele, jejichž předmět smlouvy obsahuje tuto činnost;
   b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit, a ověřit, že k odhlášení/uzamčení opravdu došlo;
   c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku ČNB;
   d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
   e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk ČNB a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku ČNB.
8) Pracovníci dodavatele nesmí:
   a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);

b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).

9) Pracovníci dodavatele nejsou oprávněni:

a) používat soukromou e-mailovou schránku pro činnosti související s plněním dle smlouvy, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;

b) nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;

c) ukládat jiné než veřejné informace mimo úložiště pod správou ČNB nebo dodavatele (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).

10) Dodavatel a jeho pracovníci nejsou oprávněni:

a) nepovoleně používat, kopírovat a šířit software, jako např.:

i) instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);

ii) instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět smlouvy obsahuje tuto činnost;

iii) instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí

(1) pro situace výslovně schválené a popsané v jiném vnitřním předpisu (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a

(2) v případech, kdy předmět smlouvy obsahuje tuto činnost;

b) používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;

c) bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

1) Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.

2) Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů na Internet ze sítě ČNB automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).