Dohoda ohledně provádění penetračních testů při plnění smlouvy na implementaci systému řízení bezpečnosti informací a poskytování služeb dohledového centra

1.
Smluvní strany

1. Moravskoslezské datové centrum, příspěvková organizace

se sídlem: Na Jízdárně 2824/2, 702 00 Ostrava - Moravská Ostrava
zastoupena: [redacted] ředitel organizace
IČO: 068 39 517
DIČ: CZ06839517
bankovní spojení: UniCredit Bank
číslo účtu: 01388070172/2700

(dále jen ***„objednatel")***

a

2. Společníci společnosti „KONSORCIUM VISITECH A DATASYS"

společnost dle § 2716 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, jež tvoří:

VISITECH a.s.

se sídlem: Košinova 655/59, 612 00 Brno, Královo Pole
zastoupena: [redacted] předseda představenstva
IČO: 25543415
DIČ: CZ25543415
bankovní spojení: Česká spořitelna, a.s.
číslo účtu: 574660139/0800

Zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, sp. zn. B6323

jako vedoucí společník

a

DATASYS s.r.o.

se sídlem: Jeseniova 2829/20, 130 00 Praha 3
zastoupena: [redacted] na základě smlouvy o společnosti ze dne 5. 8. 2022
IČO: 61249157
DIČ: CZ61249157

Číslo smlouvy objednatele: 22076

Číslo smlouvy poskytovatele: SOD/2211/2022

Zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. C28862

jako druhý společník

(dále jen ***„poskytovatel")***

(objednatel a poskytovatel dále jednotlivě též jen ***„smluvní strana*** nebo společně ***„smluvní strany")***

II.

Základní ustanovení

1. Smluvní strany uzavřely v souladu s ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen ***„občanský zákoník"),*** s přihlédnutím k § 2586 a násl. občanského zákoníku dne 2. 12. 2022 smlouvu na implementaci systému řízení bezpečnosti informací a poskytování služeb dohledového centra (dále jen **„Smlouva"),** a to na základě výsledku zadávacího řízení na veřejnou zakázku s názvem *„Řešení kybernetické bezpečnosti v nemocnicích MSK"* (dále jen ***„Veřejná zakázka"),*** zadávanou v otevřeném zadávacím řízení dle ust. § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů (dále jen ***„ZZVZ").*** Dne 30. 3. 2023 smluvní strany uzavřely dodatek č. 1 ke Smlouvě.
2. Při realizaci Smlouvy vyvstala potřeba mezi smluvnímu stranami vyjasnit rozsah provádění penetračních testů v rámci předmětu plnění Smlouvy, proto se smluvní strany dohodly na uzavření této písemné dohody (dále jen ***„Dohoda").***
3. Dohoda vychází ze závěrů koordinační schůze č. 46, která se konala dne 30. 5. 2024
4. Dohoda nezakládá podstatnou změnu závazku, neboť dle stanoviska smluvních stran nenaplňuje podmínky dle § 222 odst. 3 ZZVZ.

III.

Předmět Dohody

1. Smluvní strany potvrzují, že plnění Smlouvy zahrnuje smluvní zajištění penetračních testů ve zdravotnických zařízeních, což vyplývá z odst. 5.2 přílohy č. 1 Smlouvy (Technická specifikace).
2. Pro vyloučení jakýchkoli nejasností smluvní strany upřesňují a doplňují odst. 5.2 přílohy č. 1 Smlouvy následovně *(doplněná částJe označena kurzívou a podtržením)'.*

   Penetrační testy jsou předmětem plnění této veřejné zakázky/Smlouvy. Je však požadováno, aby je prováděla na systému řízení zcela nezávislá organizace. Dodávatě*Zposkytoygtel* má povinnost smluvně zajistit nezávislou organizaci, která před každým prováděným penetračním testem musí prokázat svou nezávislost. Současně je *dodavate\/poskytovatel* povinen toto učinit kdykoli je objednatelem o to požádán. V případě prokazatelných pochybností objednatele o nezávislosti organizace provádějící penetrační testování si objednatel vyhrazuje právo požadovat změnu této organizace.

Výsledky jsou silnou zpětnou vazbou pro hodnocení účinnosti implementované kybernetické bezpečnosti.

První sadu penetračních testů ve zdravotnických zařízeních dle Smlouvy poskytovatel smluvně zajistí v rozsahu, který Je vymezen v příloze č. 7 na svůj náklad u nezávislé organizace dle shora uvedeného, a to po dokončení analýzy rizik v návaznosti na identifikaci aktiv, která budou podrobena penetrační testům.

Nad rámec první sady penetračních testů, zajištěných poskytovatelem dle předchozího odstavce, bude v Provozní fázi SOC povinnost poskytovatele smluvně zajistit nezávislou organizaci k provedení penetračních testů (Jednotlivých testů, souhrnných sad testů či opakovaných testů) zahrnovat následující činnosti poskytovatele:

- *asistence objednateli při sestavení žádosti o předložení nabídky na provedení penetračních testů - verifikace zadání z technického hlediska*
- *vyhledání vhodných subjektů k oslovení s žádostí o předložení nabídky na provedení penetračních testů*
- *komunikace s vybranými subjekty dle preferencí objednatele a Jejich přímé oslovení s žádostí o předložení nabídky na provedení penetračních testů*
- *asistence objednateli při posouzení došlých nabídek*
    - *posouzení nabídek z hlediska technického*
    - *připomínkování smluvní dokumentace z hlediska technického a best practices*

Provedení dalších sad penetračních testů již poskytovatel nezajišťuje na svůj náklad.

Tímto rozsahem smluvního zajištění je ve vztahu k provádění penetračního testování naplněn také čl. XV.24. Smlouvy.

IV.
Závěrečná ustanovení

1. V případě, že jsou v této Dohodě používány pojmy s velkým písmenem na počátku a nejsou definovány v těle této Dohody, jedná se o pojmy definované ve Smlouvě nebo v přílohách Smlouvy.
2. Práva a povinnosti smluvních stran vyplývající z Dohody, která nejsou změněna touto Dohodou, zůstávají nedotčena.
3. Tato Dohoda je uzavřena v elektronické podobě a podepsána elektronickým podpisem zástupců smluvních stran.
4. Dohoda nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem, uveřejnění smlouvy v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen ***„zákon o registru smluv").*** Uveřejnění Dohody v registru smluv zajistí objednatel.

5. Nedílnou součástí této Dohody je příloha č. 1 - Rozsah penetračního testování (1. sada penetračních testů).

V Ostravě dne 19.6.2024

[redacted]

V Brně dne 19.6.2024

[redacted]

1.1 Cíl penetračního testování

Cílem penetračních testů je otestovat tu část infrastruktury, která zpracovává pacientská data (zvláštní data dle GDPR), otestovat zálohovací systémy daného zdravotnického zařízení (dále jen ZZ) a případně otestovat všechna aktiva, za pomoci, kterých mohou být kompromitována pacientská data, ale neslouží primárně k účelu jejich zpracovávání.
Jsou tedy kladeny otázky: *"Dokáže útočník odcizit pacientská data?"* a *„Dokáže se útočník napříč infrastrukturu nemocnice dostat k pacientským datům?".*

1.2 Scénáře

Jsou požadovány **tři scénáře pro testování.**

1.2.1 Test zvenčí

V tomto scénáři je požadováno, aby se tester pokusil kompromitovat FW, a skrze něj infiltrovat IT infrastrukturu daného ZZ a pokračovat dle cíle viz 4.1.

1.2.2 Fyzický vnitřní test

V tomto scénáři je požadováno, aby se tester fyzicky dostavil do lokality ZZ (jedná se o 7 nemocnic MSK - Krnov, Opava, Bílovec, Frýdek-Místek, Třinec, Karviná, Havířov), a pokusil se kompromitovat personální (ne pacientské volně dostupné) bezdrátové Wi-Fi sítě a pokračoval dle cíle viz 4.1.

1.2.3 Logický vnitřní test

V tomto scénáři je simulováno převzetí stanice útočníkem (např. instalací škodlivého souboru na uživatelské stanici apod.). V tomto scénáři je požadováno, aby tester měl k dispozici stanici (virtuální) v segmentu, kde pracují běžní zaměstnanci ZZ. Za pomocí této stanice se bude snažit eskalovat práva a pokračovat dle cíle viz 4.1.

1.3 Rozsah

Rozsahem pro penetrační testování ZZ budou kritická technická aktiva dle provedené analýzy rizik dodavatelem a případně i taková aktiva, která zpracovávají pacientská data a nejsou klasifikována jako kritická. Počtem se jedná o přibližně 50 aktiv za všechny ZZ.
Z pohledu délky naceňovaného období se jedná o jednorázový test.

1.4 Certifikace

Pro zajištění kvalitních a relevantních výstupů a maximalizaci nedestruktivity jsou vyžadovány minimálně dvě z následujících certifikací:

- CEH
- OSCP
- OSWP
- CPENT

Tyto certifikace zaručují, že dodavatel penetračních testů má potřebné znalosti a dovednosti k provedení penetračních testů na vysoké úrovni, a v souladu s nejlepšími postupy a standardy v oboru.

1.5 Reference

Pro zajištění důvěryhodnosti a kvality prováděného penetračního testování je požadována minimálně jedna reference dodavatele v oblasti zdravotnictví nebo bankovnictví. Tento požadavek je klíčový, jelikož budou testovány IT infrastruktury obsahující citlivá data. Referenční zkušenosti v těchto oborech potvrzují schopnost dodavatele pracovat s vysokými standardy zabezpečení a přizpůsobit své služby specifickým potřebám a

regulacím těchto citlivých odvětví. Tímto způsobem je zaručeno, že penetrační testování bude prováděno odborníky s relevantními zkušenostmi a znalostmi, což maximalizuje účinnost a bezpečnost celého procesu.

REFERENČNÍ ZAKÁZKA	
název realizované zakázky:	
název objednatele:	
sídlo nebo místo podnikání:	
IČO objednatele:	
kontaktní osoba objednatele:	
telefonní spojení na objednatele:	
místo realizace zakázky:	
popis předmětu plnění zakázky a její rozsah:	
doba (termín) plnění zakázky:	

1.6 Výstupy

Penetrační testování bude zakončeno publikací zprávy, která bude obsahovat minimálně:

- popis metod, metodik, norem, doporučení a vlastních postupů, které byly použity,
- seznam a charakteristiku nástrojů, které byly použity,
- popis prostředí, které bylo předmětem testů včetně,
  - seznamu IP adres, které byly předmětem testu,
  - seznam identifikovaných portů a na nich běžících služeb a protokolů použitých pro komunikaci s těmito porty a rovněž identifikovaného SW použitého pro realizaci služeb na portech
- seznam a charakteristiku testů, které byly provedeny,
- detailní seznam zjištění, minimálně v rozsahu:
  - identifikace zjištění zranitelnosti,
  - popis kde a jakým způsobem byla zranitelnost identifikována,
  - označení/název zranitelnosti (pokud lze přiřadit),
  - charakteristika zranitelnosti včetně potenciálního dopadu,
  - klasifikace zranitelnosti podle použité metodiky, kde bude obsaženo:
    - kategorii/typ zranitelnosti,
    - úroveň zranitelnosti,
    - dle pravděpodobnosti zneužití,
    - náročnosti odstranění/nápravy.
  - popis zranitelného místa/nálezu,
  - navržené opatření nebo Rozsah doporučení k eliminaci nebo minimalizaci zranitelnosti, případně odkazy na doporučení výrobce/distributora nebo jiné best practice,
  - další využití zranitelnosti, pokud bylo v rámci manuálních testů,
  - další podstatné skutečnosti,
- stručné manažerské shrnutí včetně přehledových charakteristik a celkového hodnocení zabezpečení prostředí testované organizace
- závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti infrastruktury
- celková doporučení nebo navržení dalších kroků,
- přílohy (výstupy z použitých nástrojů, důkazy apod.).

Dodavatel penetračních testů dále seznámí dotčené ZZ s výsledky penetračních testů formou online schůzky, kde budou prezentovány a komentovány výsledky z testování.