CyberSecurity Hub, z. ú.

Nabídka služeb poskytovaných prostřednictvím organizace Network Security Monitoring Cluster, družstvo

CyberSecurity Hub, z. ú. IČO: 09705163 Spisová značka: U 301 vedená u Krajského soudu v Brně Den zápisu: 26. listopadu 2020 Sídlo: Šumavská 416/15, Ponava, 602 00 Brno	**Network Security Monitoring Cluster, družstvo (poskytovatel)** IČO: 29220777 Spisová značka: Dr 4959 vedená u Krajského soudu v Brně Den zápisu: 18. května 2010 Sídlo: Jundrovská 618/31, Komín, 624 00 Brno

Obsah

1 Úvod

CyberSecurityHub[cz]

Jedná se o expertní organizaci zastřešenou třemi českými univerzitami:

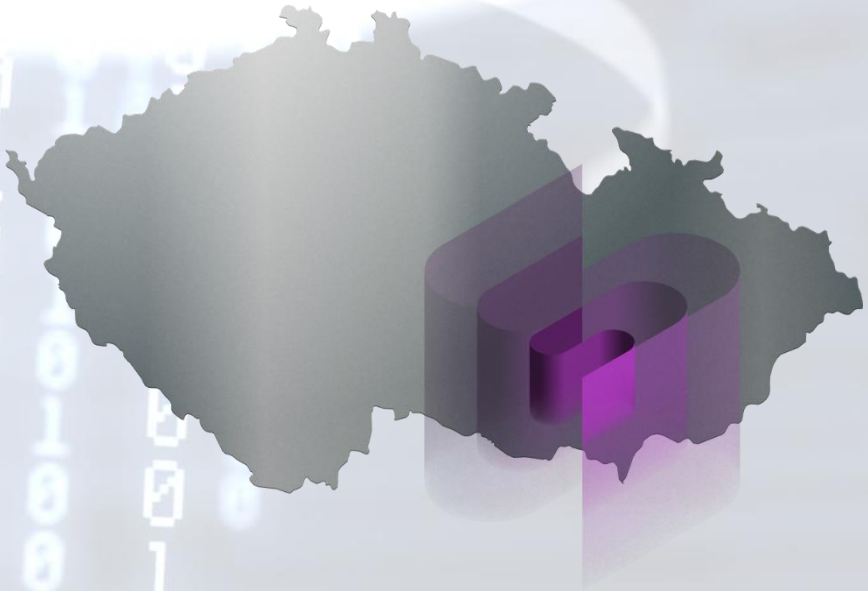
- MU,
- ČVUT,
- VUT.

Členy CSH jsou dále:

- Industry Cluster 4.0,
- Network Security Monitoring Cluster,
- Regionální hospodářská komora Brno,
- CzechInno,
- Technologické centrum Praha.

Klíčové charakteristiky:

- Jediný EDIH v ČR zaměřený na kyberbezpečnost.
- Smyslem je navyšovat konkurenceschopnost ČR i EU tím, že pomáháme SME a veřejné správě využívat potenciál ICT díky posilování kyberbezpečnosti.
- CSH je expertním průvodcem transformačním procesem z pohledu kyberbezpečnosti.
- Jedno místo, řada služeb.
- Zprostředkování know-how, kontaktů i technologií se strategickým dopadem.
- CSH je součástí města Brna. Města univerzit, studentů, justice, kultury, IT, výzkumu, inovací i kyberbezpečnosti.
- CSH patří do **CyberCampus**[cz], českého prostoru zaměřeného na budování odolné rozvinuté informační společnosti.



2 CyberCampus[CZ]

3 Přehled služeb CSH

- Služby pro malé i střední podniky a veřejnou správu v ČR se zaměřením na praxi, včetně integrace do procesů a služeb.
- Zvláštní pozornost je věnována odvětvím, kde jsou inovace v oblasti kybernetické bezpečnosti klíčové a poptávka po nich vysoká, jako je energetika, zdravotnictví, strojírenství a průmysl 4.0.
- CSH pomáhá zvyšovat znalosti a povědomí, zohledňovat bezpečnostní parametry při zavádění technologií a zajišťovat přístup k financování inovací.

4 Služby poskytované prostřednictvím NSMC – **předmět této nabídky**

Jedná se o služby z kategorie:

Inovační příležitosti a networking.

4.1 Výčet a ohodnocení služeb poskytovaných prostřednictvím NSMC

Pozn.: *Nacenění v tabulce níže je uplatněno* ***pouze pro MSP****, které* ***podléhají povinnosti zápisu plnění do RDM****. Subjekty z kategorie* ***veřejná správa této povinnosti nepodléhají.***

NSMC služby	Počet plnění (KPI)	EUR/službu	Kč/službu	Částka dotace do registru de minimis (RDM) EUR/Kč	Termín realizace	Poznámka
Basic cyber security assessment	25	2.150,-	52.277,-	1.075,- EUR/26.139,- Kč	do 14 dní	1KPI=1 posouzení
Advanced cyber security assessment	16	3.200,-	77.808,-	1.600,- EUR/38.904,- Kč	do 21 dní	1KPI=1 posouzení
Cyber security consultancy services	25	1.000,-	24 315,-	500,- EUR/12.158,- Kč	1 den	1KPI = 1MD

Pozn.: *Cena v Kč je přepočítána ke dni tvorby žádosti, tedy kurzem 24,315 Kč.*
Jak je z tabulky výše zřejmé, ***organizacím typu MSP*** *je do registru de minimis* ***zapsána pouze 50% částka z dotace (jedná se o část dotace z NPO, jejíž čerpání podléhá povinnosti de minimis).***

4.1.1 Proces zajištění a realizace služby u NSMC:

1. klient projeví zájem a osloví NSMC
2. klient vyplní formulář Čestné prohlášení žadatele o podporu (obdrží od NSMC)
3. NSMC ověří klienta a propojené subjekty v registru de minimis
4. NSMC sepíše s klientem smlouvu o poskytnutí služby
5. do 5 dnů od podpisu smlouvy je plnění zapsáno do registru de minimis
6. s klientem je sepsáno NDA a proběhne plnění služby
7. služba je ukončena ve stanoveném termínu a je podepsán předávací protokol

Pozn.: *V případě klienta,* ***který není MSP*** *a tím pádem* ***nepodléhá*** *povinnosti* ***zápisu*** *plnění služby do* ***RDM****, se ve výše uvedeném procesu* ***nerealizuje ani prohlášení (2), ani ověření v RDM (3), ani zápis plnění do RDM (5)****.*

4.1.2 Služba Basic cyber security assessment

Jedná se o **základní** posouzení stavu kybernetické bezpečnosti v organizaci, které spočívá ve formulářovém šetření, kdy klient obdrží dotazník s otázkami, které následně zodpoví. Klientovi je na závěr předána podrobná zpráva s vyhodnocením.

Popis průběhu posouzení:

- Klient obdrží dotazník s otázkami, které následně zodpoví a předá poskytovateli.
- Poskytovatel dotazník vyhodnotí.
- Poskytovatel vypracuje závěrečnou zprávu s případnými doporučeními k nápravě.
- Poskytovatel předá závěrečnou zprávu klientovi.

Délka plnění služby od zaslání objednávky klientem po předání závěrečné zprávy poskytovatelem je ovlivněna součinností na straně organizace klienta, nejzazší termín plnění je však do 14 dní od zahájení plnění služby.

Rámcem pro posouzení je Minimální bezpečnostní standard NÚKIB viz https://nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

4.1.3 Advanced cyber security assessment

Jedná se o **rozšířené** posouzení stavu kybernetické bezpečnosti v organizaci klienta, které spočívá ve formulářovém šetření a následném vytěžení informací jak dalším doptáváním, tak i prostřednictvím vedení případných řízených pohovorů se zainteresovanými osobami na straně klienta. Klientovi je na závěr předána podrobná zpráva s vyhodnocením.

Popis průběhu posouzení (po podpisu smlouvy a NDA):

- Klient obdrží dotazník s otázkami, které následně zodpoví a předá poskytovateli.
- Poskytovatel si vyžádá případnou doplňující dokumentaci.
- Poskytovatel v případě potřeby vytěží od klienta další relevantní informace.
- Poskytovatel se seznámí s informacemi předanými klientem.
- Poskytovatel provede (v případě potřeby) doplňující řízené pohovory se zainteresovanými osobami na straně klienta.
- Poskytovatel zpracuje a vyhodnotí nashromážděné podklady.
- Poskytovatel vypracuje závěrečnou zprávu s případnými doporučeními k nápravě.
- Poskytovatel předá závěrečnou zprávu klientovi.

Délka plnění služby od zaslání objednávky klientem po předání závěrečné zprávy poskytovatelem je ovlivněna součinností na straně organizace klienta, nejzazší termín plnění je však do 21 dní od zahájení plnění služby. Za den zahájení plnění služby se bere datum zaslání dotazníku klientovi.

Rámcem pro posouzení je Minimální bezpečnostní standard NÚKIB viz https://nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

4.1.4 Consultancy services

Jedná se o **konzultační** služby poskytnuté poskytovatelem klientovi z oblasti kybernetické bezpečnosti. Jeden klient má nárok na čerpání 1MD (1x8h) této služby. Tato služba je přednostně uvažována pro klienty, kteří se rozhodli využít služby Basic cyber security assessment.

Popis průběhu poskytnutí služby:

- Jeden klient vyčerpá 1MD této služby.

5 Uvažovaní klienti

5.1 MSP

Služby jsou poskytovány v režimu de minimis, tedy se zápisem do RDM (registr de minimis) do 5 dnů od podpisu smlouvy s poskytovatelem. Cena služeb, která bude předmětem zápisu do RDM je uvedena v ceníku výše (viz 4.1 Výčet a ohodnocení služeb poskytovaných prostřednictvím NSMC).

5.2 Organizace veřejné správy menší velikosti

Služby jsou poskytovány menším organizacím např. městská část, střední škola, obec. **Tyto organizace nepodléhají povinnosti zápisu čerpání služby do RDM.** Čerpání služeb pro tento typ zákazníka je evidováno pouze v interní evidenci poskytovatele služby.

6 Informace o zpracovateli nabídky a poskytovateli zde uvedených služeb

Ing. Jiří Sedláček, NSMC CEO

Pan Jiří Sedláček se věnoval oblasti informačních a komunikačních technologií již při studiu na vysoké škole. Po studiu působil v rámci své profesní kariéry jako programátor, administrátor, systémový administrátor, supervisor senior, zástupce ředitele informatiky a ředitel informatiky. Závěrem své kariéry v oblasti ICT na pozici ředitele informatiky spoluvytvářel ICT a bezpečnostní strategii nadnárodní společnosti. Právě oblast informační a kybernetické bezpečnosti se stala jeho následnou profesní náplní již na plný úvazek až do dneška. V bezpečnostní oblasti působí naplno od roku 2015, současně zastává pozici výkonného ředitele organizace Network Security Monitornig Cluster, družstvo.

Činnosti a kompetence:

- Analytické práce.
- Konzultační a poradenská činnost.
- Evangelizační (přednášková, lektorská, osvětová) činnost.
- Návrh architektury kybernetické bezpečnosti.
- Specializace na zajištění bezpečnosti lidských zdrojů.
- Vzdělávání.
- Autorství:
    - Autor osnovy vzdělávacího programu kybernetické bezpečnosti pro střední školy.
    - Autor SŠ Koncepce junior center excelence informační bezpečnosti v ČR (www.jc3.cz, podporuje NÚKIB v Akčním plánu k národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025).
    - Autor vzdělávacích kurzů kybernetické bezpečnosti.
    - Autor metodik, metrik a politik k bezpečnosti lidských zdrojů.
    - Autor metodik, metrik a materiálů k table-top cvičením.

Pan Jiří Sedláček je členem výboru pro řízení kybernetické bezpečnosti statutárního města Brna a má rovněž několikaleté zkušenosti z prostředí MSP, korporací, sektoru zdravotnictví a veřejné správy.

Kontakt:

jiri.sedlacek@nsmcluster.com +420 602 129 224

Ing. Jiří Sedláček

Digitálně podepsal Ing. Jiří Sedláček
Datum: 2023.11.30 12:10:39 +01'00'