SMLOUVA O POSKYTNUTÍ SLUŽBY

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník

mezi těmito smluvními stranami:

Objednatel:
Město Bučovice
IČ: 00291676
se sídlem: Jiráskova 502, 685 01 Bučovice
zastoupené: PhDr. Jiřím Horákem, Ph.D., starostou
(dále jen „Objednatel“)

a

Dodavatel:
VirusLab s.r.o.
IČ: 09429212
se sídlem: Záběhlická 131/33, 106 00 Praha 10
zastoupená: Petrem Hušákem, jednatelem
(dále jen „Dodavatel“)

Článek I. – Předmět smlouvy

1. Dodavatel se zavazuje provést pro Objednatele službu s názvem Analýza rizik kybernetické bezpečnosti, a to v souladu se svou nabídkou a požadavky Objednatele.

2. Objednatel se zavazuje za řádné a včasné poskytnutí služby zaplatit Dodavateli cenu ve výši 174.240 Kč včetně DPH.

Článek II. – Termín plnění

1. Dodavatel se zavazuje předat výstup služby nejpozději do 2 měsíců od podpisu této smlouvy oběma stranami. Při nedodržení lhůty požaduje objednatel smluvní pokutu ve výši 20.000 Kč.

3. Nedodá-li Dodavatel písemný výstup do 30 dnů po uplynutí lhůty dle čl. II odst. 1 této smlouvy, je Objednatel oprávněn od smlouvy odstoupit.

Článek III. – Mlčenlivost a důvěrnost informací

1. Dodavatel se zavazuje zachovávat mlčenlivost o všech informacích důvěrné povahy, které mu budou v rámci spolupráce sděleny nebo které jinak získá při plnění této smlouvy, zejména se

jedná o: topologii sítě, osobní údaje zaměstnanců, přístupová jména a hesla, technickou konfiguraci systémů a bezpečnostní opatření.

2. Povinnost mlčenlivosti trvá i po skončení této smlouvy.

3. Výjimkou z povinnosti mlčenlivosti je zákonná povinnost sdělení údajů orgánům veřejné moci, v takovém případě Dodavatel předem informuje Objednatele.

Článek IV. – Součinnost a odpovědnost

1. Objednatel se zavazuje poskytnout Dodavateli veškerou potřebnou součinnost nezbytnou pro řádné splnění předmětu smlouvy, zejména poskytnutím požadovaných podkladů a informací bez zbytečného odkladu.

2. V případě, že Objednatel neposkytne součinnost ani do 10 pracovních dnů od prokazatelné výzvy Dodavatele, je Dodavatel oprávněn od smlouvy odstoupit a požadovat úhradu prokazatelně vzniklých nákladů souvisejících s přípravou a částečnou realizací zakázky.

Článek V. – Závěrečná ustanovení

1. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma stranami.

2. Nedílnou součástí této smlouvy jako příloha je zadávací dokumentace Objednatele.

3. Smlouva je uzavřena na dobu určitou do splnění všech povinností z ní vyplývajících.

4. Veškeré změny a doplnění této smlouvy mohou být činěny pouze písemně formou číslovaných dodatků podepsaných oběma stranami.

5. Právní vztahy touto smlouvou výslovně neupravené se řídí příslušnými ustanoveními občanského zákoníku.

6. Tato smlouva je vyhotovena ve dvou vyhotoveních, z nichž každá strana obdrží po jednom.

Digitálně podepsal PhDr. Jiří Horák, PhD.
Datum: 09.05.2025 11:13:08 +02:00

Za Objednatele:
PhDr. Jiří Horák, Ph.D.
starosta

Petr Hušák
Digitálně podepsal Petr Hušák
Datum: 2025.05.12 08:14:28 +02'00'

Za Dodavatele:
Petr Hušák
jednatel

Příloha ke smlouvě – zadávací podmínky zadavatele

Stručná specifikace předmětu

Díky analýze rizik kyberbezpečnosti budou identifikovány, hodnoceny a řízeny potenciální hrozby a zranitelnosti informačních systémů zadavatele a celého kyberprostředí s cílem minimalizovat nebo eliminovat možné škody. Tato analýza je klíčovým prvkem efektivní kyberbezpečnostní strategie.

Analýza rizik bude provedena v souladu s těmito právními předpisy:

- se stávající právní úpravou dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen zákon o kybernetické bezpečnosti)
- s připravovaným novým zákonem o kybernetické bezpečnosti (sněmovní tisk č. 759, dostupné z Sněmovní tisk 759 a sněmovní tisk č. 760 dostupné z Sněmovní tisk 760), který implementuje platnou evropskou směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen směrnice NIS 2).

(dále jen stanovené právní předpisy)

Podrobná specifikace předmětu:

Cílem analýzy je podrobný popis vstupního stavu, umožňující následně po realizaci opatření v rámci projektu konstatovat posílení kybernetické bezpečnosti dotčených informačních a komunikačních systémů. Závěrečné zhodnocení realizace projektu podléhá závěrečnému auditu.

Minimální požadavky zadavatele na obsah analýzy rizik:

1. *Identifikace regulovaných služeb v rámci NIS2 a určení úrovně povinností*
    a. Analýza služeb zadavatele v rozsahu:
        i. rozbor procesů a produktů zadavatele
        ii. identifikace všech služeb, které jsou dle stanovených právních předpisů regulované
    b. Určení velikosti zadavatele ve smyslu NIS2
        i. Rozbor holdingové struktury zadavatele a určení s ním propojených osob

ii. Zhodnocení velikosti zadavatele (malý, střední, velký podnik) se zohledněním propojených osob

c. Určení úrovně povinností ve smyslu stanovených právních předpisů

i. Propojení identifikovaných regulovaných služeb a velikosti organizace zadavatele, případně zvláštních oborových kritérií

ii. Identifikace úrovně povinností zadavatele dle stanovených právních předpisů

d. Povinnosti dodavatele pro regulovanou službu

i. V případě, že v rámci předchozích kroků nebude identifikována povinnost zadavatele, bude proveden základní rozbor smluvních a zákonných vztahů ve kterých vystupuje zadavatel jako významný dodavatel/provozovatel nějaké regulované služby třetí strany.

ii. Zadavatel bude zařazen do úrovně povinností dle služby třetí osoby, na které se podílí.

iii. Vytvoření mapy regulovaných služeb včetně určení jejich úrovně dle stanovených právních předpisů a regulovaných služeb třetích stran, v rámci kterých je objednatel v pozici významného dodavatele (registrovat se na NÚKIB, dodržovat politiky a pravidla klientské organizace).

2. *Popis stavu systému kybernetické bezpečnosti zadavatele*

Služba zajistí popis stavu systému kybernetické bezpečnosti (organizační, procesní a technická stránka) v jednotlivých oblastech regulace se zvláštním zaměřením a zvýšenou podrobností popisu zejména v následujících oblastech:

a. Systém řízení bezpečnosti informací (§ 3 zákona o kybernetické bezpečnosti) se zaměřením na dokumentaci a nastavení procesů

b. Ochrana před škodlivým kódem (§ 21 zákona o kybernetické bezpečnosti) se zaměřením na jednotlivé segmenty sítě zadavatele a komunikaci mezi nimi a ochranu na aplikační vrstvě

c. Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů (§ 22 zákona o kybernetické bezpečnosti) se zaměřením na systém logování zadavatele a síťový monitoring

d. Detekce kybernetických bezpečnostních událostí (§ 23 zákona o kybernetické bezpečnosti) se zaměřením na systém logování zadavatele a síťový monitoring

e. Zajišťování úrovně dostupnosti informací (§ 27 zákona o kybernetické bezpečnosti) se zaměřením na identifikaci single point of failure v rámci technických řešení zadavatele a existující řešení zálohování

Výstupem tohoto kroku bude popis využitelný jako přesné zachycení stavu systému kybernetické bezpečnosti zadavatele.

3. *Assessment souladu aktuálního stavu vůči stanoveným právním předpisům.*

Zhotovitel zajistí komplexní zhodnocení organizace z hlediska povinností kybernetické bezpečnosti daných stanoveným právními předpisy.

4. *Stanovení opatření k nápravě*

V návaznosti na audit budou Zhotovitelem identifikována a navržena obecná opatření k dosažení shody.

Zadavatel požaduje, aby zhotovitel postupoval při zpracování analýzy rizik dle doporučení v oblasti kybernetické bezpečnosti pro obce, které vydal Národní úřad pro kybernetickou a infomační bezpečnost. Dostupné pod odkazem: https://portal.nukib.gov.cz/storage/uploads/2025/02/14/podpurny-material_kyberneticka-bezpecnost-obci_uid_6753022f5e89b_uid_67af075214cc3.pdf