Smlouva o dílo č. 2024/ORI/S/0352

(dále jen „smlouva“)
uzavřená podle ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „občanský zákoník“) mezi dále uvedenými smluvními stranami podle svého prohlášení plně svéprávnými, a to:

Objednatel:	**Město Orlová**
se sídlem:	Osvobození 796, Orlová, PSČ: 735 14
IČO:	00297577
DIČ:	CZ 00297577, plátce DPH
zastoupeno:	Lenkou Brzyszkowskou, starostkou města
bankovní spojení:	banka ČSOB a.s., pobočka Orlová účet č. 103957163/0300

Osoba oprávněná k podpisu a jednání ve věcech této smlouvy na základě Pověření ze dne 22.11. 2023:
[redacted]

Osoba pověřené jednat ve věcech technických:
[redacted]

(dále jen „**objednatel**“)

a

Zhotovitel:	**DATASYS s.r.o.**
se sídlem:	Praha 3, Jeseniova 2829/20, PSČ: 130 00
IČO:	612 49 157
DIČ:	CZ61249157, plátce DPH
zastoupena:	Bc. Martinem Novákem, prokuristou
bankovní spojení:	Komerční banka a.s. účet č. 27-9647490267/0100
zapsaná:	v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 28862
kontaktní osoba:	[redacted]

(dále jen „**zhotovitel**“)

(dále též společně jako „**smluvní strany**“)

Čl. I.
Úvodní ustanovení

1. Tato smlouva je uzavírána se zhotovitelem pro provedení studie stavu kybernetické bezpečnosti ve městě Orlová (Název projektu: Kybernetická bezpečnost v Orlové), tedy objednatele s návrhem cílového stavu a technických opatření na zvýšení odolnosti organizace proti kybernetickým hrozbám, také pro provedení praktického testu zranitelnosti a vytvoření dokumentů:
   - Katalog primárních aktiv,
   - Studie stavu kybernetické bezpečnosti s tabulkovou přílohou „Hodnocení stavu kybernetické bezpečnosti“ a s návrhem doporučených opatření,
   - Návrh technických opatření na zvýšení odolnosti organizace, proti kybernetickým hrozbám,
   - Výsledek provedení skenu zranitelností .
2. Zhotovitel se zavazuje splnit předmět této smlouvy nejen v souladu s touto smlouvou, ale také v souladu s jeho nabídkou, která předcházela uzavření této smlouvy. Nabídka zhotovitele podle předchozí věty tvoří nedílnou součást této smlouvy jako příloha č. 1.

Čl. II.
Předmět a účel smlouvy

1. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro objednatele dílo v rozsahu a objemu dle této smlouvy vč. jejích příloh a objednatel se zavazuje provedené dílo převzít a zaplatit zhotoviteli za toto dílo dohodnutou cenu, to vše za podmínek stanovených dále touto smlouvou.
2. Pro účely této smlouvy se dílem rozumí souhrn těchto dílčích plnění:
   i. Hodnocení stavu kybernetické bezpečnosti provedené ve struktuře dle relevantních požadavků zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a jeho doprovodných obecně platných právních předpisů, přičemž součástí díla je: (a) Katalog IT služeb a jejich požadovaných parametrů, tzv. primárních aktiv; (b) Dokument „Analýza stavu kybernetické bezpečnosti“ s návrhem doporučených opatření; (c) Přehledy dotazníkových šetření „Hodnocení kybernetické bezpečnosti; (d) Dokument návrh technických opatření na zvýšení odolnosti organizace, proti kyberbezpečnostním hrozbám“.
   ii. Provedení testu zranitelnosti, realizovaného asistovanou zápůjčkou hardwarové sondy nástroje Greenbone Security Manager (GSM) pro získání přehledu o zařízeních v síti a zejména pro zjištění a zvládání zranitelných služeb sítě. Hardwarová sonda je ve vlastnictví zhotovitele.
3. Účelem této smlouvy je provedení studie stavu kybernetické bezpečnosti dle bodu 2i a provedení testu zranitelnosti 2ii.
4. Dílo bude provedeno v souladu s požadavky na něj kladenými touto smlouvou. Zhotovitel se zavazuje poskytnout plnění v takové kvalitě, jež je s přihlédnutím k zájmům a požadavkům objednatele a okolnostem prováděného díla pro objednatele nejvhodnější.

5. Zadavatel předpokládá spolufinancování projektu při realizaci z prostředků Ministerstva vnitra v rámci Národního plánu obnovy.

Čl. III.
Cena díla a platební podmínky

1. Celková cena díla je **90 000 Kč** bez DPH (slovy: devadesát tisíc korun českých).
2. Celková cena díla zahrnuje jednotlivá dílčí plnění, jak jsou uvedena a specifikována v Čl. II. této smlouvy takto:
    a. cena za dílčí plnění dle čl. II.2.i. činí 60 000,- Kč,
    b. cena za dílčí plnění dle čl. II.2.ii. činí 30 000,- Kč.
3. Celková cena díla je stanovena dohodou smluvních stran, zahrnuje veškeré náklady zhotovitele spojené se zhotovením díla, nebude měněna (je nepřekročitelná), kromě těch případů, kdy dojde ke změně právních předpisů, např. změny sazby DPH; případně nedohodnou-li se smluvní strany jinak.
4. Objednatel na předmětné dílo neposkytuje žádnou zálohu.
5. Cena díla bude uhrazena na základě daňového dokladu vystaveného po řádném, úplném a včasném dokončení dílčího plnění, resp. po protokolárním předání a převzetí bezvadného a řádně a včas dokončeného dílčího plnění a po odsouhlasení předávacího (akceptačního) protokolu určeným zástupcem objednatele.
6. Objednatel provede úhradu výhradně v české měně na základě příslušného daňového dokladu, který musí obsahovat všechny náležitosti dle § 28 a násl. zákona č. 235/2004 Sb., o dani z přidané hodnoty ve znění pozdějších předpisů. Faktura je splatná 30 dnů po doručení příslušné faktury v řádném stavu objednateli. Je-li faktura vystavena chybně, nebo není-li doložena sjednanými přílohami, je objednatel oprávněn ji vrátit, přičemž v tomto případě není v prodlení s úhradou pohledávky účtované příslušnou fakturou.
7. Smluvní strany si sjednaly, že veškerá další komunikace, není-li ve smlouvě stanoveno výslovně jinak, může být vedena v elektronické podobě, přičemž elektronická sdělení nemusí být opatřena uznávaným elektronickým podpisem a ani nemusí jít o autorizovanou konverzi dokumentů s výjimkou právních jednání, která v elektronické podobě musí být opatřena uznávaným elektronickým podpisem. Smluvní strany tímto zrovnoprávňují formu písemné a elektronické komunikace.
8. Faktura musí být označena registračním číslem a názvem projektu - CZ.31.2.0/0.0/0.0/23_093/0008606, Kybernetická bezpečnost v Orlové.

Čl. IV.
Termín a místo plnění

1. Zhotovitel se zavazuje provést dílčí plnění dle čl. II.2.i. a čl. II.2.ii této smlouvy nejpozději do 40 kalendářních dnů ode dne účinnosti této smlouvy.
2. Místem plnění díla je sídlo objednatele.

Čl. V.
Práva a povinnosti objednatele

1. Objednatel je oprávněn dílo a jeho provádění kdykoliv kontrolovat, zda je prováděno v souladu s touto smlouvu.
2. Objednatel se zavazuje poskytovat zhotoviteli součinnost potřebnou k řádnému provedení díla. Zejména, nikoliv však výlučně, se jedná o poskytnutí veškeré relevantní dokumentace (popis rozhraní systémů objednatele; popis rozhraní externích systémů, popis procesů objednatele apod.), zajištění účasti svých zaměstnanců na vyžádaných konzultačních schůzkách, případně zajištění účasti zaměstnanců třetích stran na vyžádaných konzultačních schůzkách a přístup k IT infrastruktuře objednatele.

Čl. VI.
Práva a povinnosti zhotovitele

1. Zhotovitel se zavazuje dílo řádně provést, předat objednateli ve stanoveném termínu, požadované kvalitě a v požadovaném provedení.
2. Zhotovitel je povinen důsledně a komplexně zjistit veškeré potřebné informace, vyžádat si nezbytné podklady a prověřit veškeré možnosti daného řešení a takto zjištěné poznatky analyzovat. Zhotovitel je povinen při plnění předmětu díla postupovat s odbornou péčí.
3. Zhotovitel prohlašuje, že má dostatečné znalosti, schopnosti a prostředky k řádnému provedení díla.
4. Zhotovitel odpovídá za výkony svých zaměstnanců a zástupců, jakož i za přesnost a úplnost všech dat a informací předkládaných zhotovitelem objednateli pro účely poskytování plnění podle této smlouvy.
5. V případě, že objednatel nedodá zhotoviteli správné a úplné informace, neposkytne včas a řádně požadovanou součinnost či potřebné podklady anebo neumožní zhotoviteli přístup ke svým zaměstnancům anebo k IT infrastruktuře podle podmínek této smlouvy, pak zhotovitel neodpovídá za případné prodlení nebo vady díla. Zhotovitel si dále vyhrazuje právo prodloužit veškeré konečné termíny o dobu odpovídající každému takovému prodlení způsobenému objednatelem, v tomto případě nebude mít objednatel právo požadovat po zhotoviteli zaplacení vzniklé škody či smluvní pokuty.
6. Objednatel souhlasí s tím, že zhotovitel může použít odkaz na obchodní firmu objednatele a typ poskytnuté služby jako referenci ve svých marketingových materiálech po dobu 3 let od udělení tohoto souhlasu.

Čl. VII.
Předání a převzetí díla

1. Zhotovitel splní svou povinnost provést dílo jeho řádným a včasným dokončením.
2. Zhotovitel je povinen písemně oznámit objednateli předem, že dokončené dílo bude připraveno k předání a převzetí. Objednatel je pak povinen do 5 pracovních dnů zahájit přejímací řízení.

Předání díla nastane na základě předávacího (akceptačního) protokolu. Předávací (akceptační) protokol bude datován a opatřen podpisy oprávněných pracovníků objednatele a zhotovitele. 4. Oprávněným zástupcem objednatele pro převzetí (akceptaci) díla je

[redacted]

Čl. VIII.
Smluvní pokuty a náhrada škody

1. Ocitne-li se zhotovitel v prodlení s dokončením díla nebo jeho části, je objednatel oprávněn vyúčtovat zhotoviteli a zhotovitel se zavazuje zaplatit objednateli smluvní pokutu ve výši 0,05 % z hodnoty díla za každý i jen započatý den prodlení. Smluvní pokuta je splatná do 14 dnů od jejího uplatnění objednatelem a lze ji započíst proti nedoplatku ceny díla. Zaplacení smluvní pokuty nemá vliv na povinnost k náhradě škody, tedy zaplacením smluvní pokuty není dotčeno právo na náhradu škody vzniklé objednateli v příčinné souvislosti s porušením závazku zhotovitele provést dílo řádně a včas, a to i nad výši sjednané smluvní pokuty. Odstoupení od smlouvy nemá rovněž vliv na povinnost k úhradě smluvní pokuty dle tohoto bodu smlouvy. Smluvní strany prohlašují, že takto sjednaná smluvní pokuta je v souladu s dobrými mravy, poctivým obchodním stykem a její výše odpovídá hodnotě zajišťované povinnosti.
2. V případě prodlení se zaplacením peněžité částky je smluvní strana, která je se zaplacením v prodlení, povinna zaplatit druhé smluvní straně úrok z prodlení ve výši 0,05 % z nezaplacené částky za každý i jen započatý den prodlení.
3. V případě porušení povinností k ochraně důvěrných informací a závazku mlčenlivosti dle čl. X této smlouvy je smluvní strana, která poruší tyto povinnosti, zaplatit druhé smluvní straně smluvní pokutu ve výši 100 000 Kč za každé porušení takové povinnosti, a to do 14 dnů ode dne doručení faktury vystavené na její uhrazení.
4. Není porušením závazku objednatele nezajištění poskytnutí součinnosti třetích stran v případě, že objednatel učinil prokazatelně veškeré kroky vedoucí k získání takovéto součinnosti, které po něm lze spravedlivě vyžadovat s přihlédnutím ke všem okolnostem v dané situaci. V takovém případě zároveň není porušením závazku zhotovitele dodání díla v kvalitě odpovídající neposkytnutí součinnosti třetích stran a nelze dílo v příslušné části považovat za vadné.
5. Zaplacením smluvní pokuty není, jakkoliv dotčen nárok druhé smluvní strany na náhradu škody. Nárok na náhradu škody je druhá smluvní strana oprávněna uplatnit vedle smluvní pokuty v plné výši.

Čl. IX.
Záruka a odpovědnost za vady

1. Zhotovitel přejímá záruku za jakost provedeného díla a poskytuje záruku v délce trvání 6 měsíců (dále jen „záruční doba“), která počíná běžet dnem předání a převzetí celého řádně dokončeného díla, které je zbaveno všech vad a nedodělků. Zhotovitel není povinen aktualizovat dílo na základě událostí, ke kterým došlo po předání konečného díla a které nebylo možné před předáním konečného díla předpokládat.
2. Objednatel je povinen vady reklamovat u zhotovitele písemně, a to kdykoli po jejich zjištění. K projednání takto reklamovaných vad nastoupí zhotovitel bezodkladně, nejpozději však do 5

pracovních dnů, pokud nebude dohodnuto jinak. Z tohoto jednání bude pořízen zápis, který bude obsahovat údaje týkající reklamované vady a dohodu o termínu jejího odstranění. Reklamace může být učiněna i elektronicky, a to na shora uvedenou mailovou adresu. V případě změny této adresy je povinen zhotovitel neprodleně průkazně informovat objednatele o nové adrese.

3. Reklamaci lze uplatnit do posledního dne záruční doby, přičemž i reklamace odeslaná objednatelem v poslední den záruční doby se považuje za včas uplatněnou.

4. Pro případ vady díla sjednávají smluvní strany přednostně právo objednatele požadovat a povinnost zhotovitele poskytovat bezplatné odstranění vady, a to bez zbytečného odkladu.

Čl. X.
Ochrana informací a závazek mlčenlivosti

1. Důvěrnými informacemi se pro účely této smlouvy a po celou dobu trvání vzájemné spolupráce smluvních stran rozumí, bez ohledu na formu a způsob jejich sdělení či zachycení a až do doby jejich zveřejnění, jakékoli a všechny skutečnosti, které se smluvní strana v průběhu vzájemné spolupráce dozví, anebo které jí druhá smluvní strana v průběhu vzájemné spolupráce zpřístupní, jakož i sama existence těchto skutečností (dále jen „důvěrné informace“).

2. Za důvěrné informace lze taktéž považovat zejména know-how, jímž se rozumí veškeré poznatky obchodní, výrobní, technické či ekonomické povahy související s činností smluvní strany a které nejsou běžně dostupné. Dále se považují za důvěrné informace takové informace, které jsou jako důvěrné výslovně některou ze stran označeny.

3. Smluvní strany jsou povinny zajistit utajení získaných důvěrných informací způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak. Povinnost utajovat důvěrné informace zavazuje smluvní strany po dobu účinnosti této smlouvy a po dobu 2 let po ukončení smluvního vztahu založeného touto smlouvou. Strany mají právo požadovat navzájem doložení dostatečnosti utajení důvěrných informací. Strany jsou povinny zajistit utajení důvěrných informací i u svých zaměstnanců, zástupců, jakož i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty.

4. Smluvní strany se zavazují zachovávat plnou mlčenlivost o všech důvěrných informacích, ledaže se jedná o informace, které jsou veřejně přístupné, smluvní strana obdrží od zpřístupňující strany písemný souhlas zpřístupňovat danou důvěrnou informaci, či je-li zpřístupnění důvěrné informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu.

5. V případě, že se zhotovitel v rámci provádění díla dostane k osobním údajům zaměstnanců, zákazníků nebo jiných osob, nebude tyto osobní údaje zpracovávat ani nikomu dalšímu ke zpracování předávat a zavazuje se o nich dodržet povinnost mlčenlivosti. Zhotovitel je povinen počínat si tak, aby jeho činností nedošlo k porušení zabezpečení osobních údajů. V případě, že by v důsledku činnosti nebo nečinnosti zhotovitele přece jenom došlo k porušení zabezpečení osobních údajů, je zhotovitel povinen o tom bezodkladně, nejpozději však do 48 hodin, informovat objednatele.

6. Po ukončení účinnosti této smlouvy je každá ze smluvních stran povinna bez zbytečného odkladu po obdržení žádosti druhé strany vrátit druhé smluvní straně všechny poskytnuté materiály obsahující důvěrné informace včetně jejich případně pořízených kopií. O předání a převzetí se sepíše protokol podepsaný oběma smluvními stranami.

Čl. XI.
Odstoupení od smlouvy

1. Od této smlouvy může odstoupit kterákoliv smluvní strana, a to pro podstatné porušení této smlouvy druhou smluvní stranou. Právní účinky odstoupení od smlouvy nastávají doručením písemného oznámení o odstoupení druhé smluvní straně. Předpokladem pro takovéto odstoupení od smlouvy je předchozí písemné upozornění jedné strany straně druhé na existenci podstatného porušení smlouvy a neodstranění takovéhoto závadového stravu druhou smluvní stranou v určené přiměřené lhůtě, nejvýše však v délce 5 pracovních dnů.
2. Odstoupením od smlouvy se závazek zrušuje od počátku. V ostatním se odstoupení řídí obecnými ustanoveními občanského zákoníku.

Čl. XII.
Změna smlouvy

1. Tuto smlouvu lze měnit pouze písemným oboustranně potvrzeným ujednáním, výslovně nazvaným dodatek ke smlouvě. Jiné zápisy, protokoly apod. se za změnu smlouvy nepovažují. Tyto dodatky musí být číslovány.
2. Nastanou-li u některé ze stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu oznámit druhé straně a vyvolat jednání zástupců oprávněných k podpisu smlouvy.

Čl. XIII.
Závěrečná ustanovení

1. Tato smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv (§ 6 odst. 1 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“), není-li stanovena účinnost pozdější, odvíjející se od lhůty stanovené v ust. § 5 odst. 2 zákona o registru smluv. Město Orlová tuto smlouvu zašle správci registru smluv k uveřejnění prostřednictvím registru smluv bez zbytečného odkladu, nejpozději do 30 dnů od jejího uzavření (§ 5 odst. 2 zákona o registru smluv). Město Orlová zašle nejpozději do 5 kalendářních dnů zhotoviteli potvrzení o uveřejnění smlouvy v registru smluv.
2. Smluvní strany se zavazují v rámci uzavřeného smluvního vztahu dodržovat Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.04.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále jen „GDPR“) a s tímto související zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon o zpracování osobních údajů“).
3. V případě porušení povinností vyplývajících z GDPR nebo zákona o zpracování osobních údajů odpovídá za tato porušení ta ze smluvních stran, jejímž jednáním či opomenutím k porušení GDPR nebo zákona o zpracování osobních údajů došlo.
4. Smluvní strany souhlasí s uvedením osobních údajů ve smlouvě tak, jak jsou tyto ve smlouvě uvedeny a prohlašují, že nakládání se smlouvou obsahující osobní údaje bude odpovídat povinnostem vyplývajícím z GDPR a zákona o zpracování osobních údajů.
5. Změnit nebo doplnit tuto smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této smlouvy a podepsány oprávněnými zástupci smluvních stran

6. Veškerá komunikace (s výjimkou právních jednání, pokud není výslovně ujednáno jinak) může být vedena elektronicky a nemusí být dle dohody stran podepsána uznávaným elektronickým podpisem. Příslušné e-mailové adresy si smluvní strany sdělí při podpisu této smlouvy. Smluvní strany zrovnoprávňují elektronickou a písemnou formu komunikace. Elektronicky mohou být zasílány i veškeré přílohy či podklady pro úkony stran činěné v souvislosti s touto smlouvou, aniž by muselo jít o autorizovanou konverzi dokumentů. Smluvní strany se zavazují doručení veškeré e-mailovou korespondence potvrzovat nejpozději následující pracovní den po jejím obdržení.
7. Případná neplatnost některého ustanovení této smlouvy nemá za následek neplatnost ostatních ustanovení. V případě, že kterékoliv ustanovení této smlouvy se stane neúčinným nebo neplatným, smluvní strany se zavazují bez zbytečného odkladu nahradit takové ustanovení novým, které svým obsahem a smyslem odpovídá nejlépe obsahu a smyslu ustanovení původního.
8. Zhotovitel není oprávněn postoupit své pohledávky vůči objednateli vzniklé z této smlouvy nebo v souvislosti s ní na třetí osobu bez předchozího písemného souhlasu objednatele. Zhotovitel není oprávněn převést ani žádná jiná svá práva ani žádné povinnosti z této smlouvy na třetí osobu bez předchozího písemného souhlasu objednatele.
9. Strany si nepřejí, aby nad rámec výslovných ustanovení této smlouvy byly jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak.
10. Smlouva je uzavřena elektronicky.
11. Smluvní strany prohlašují, že si tuto smlouvu přečetly, jejímu obsahu rozumí a že obsahuje jejich skutečnou a svobodnou vůli, na důkaz čehož připojují své podpisy
12. Vzájemné vztahy mezi smluvními stranami, neupravené zněním této smlouvy, se řídí příslušnými ustanoveními občanského zákoníku a dalších obecně závazných právních předpisů.
13. Doložka podle § 41 zákona č. 128/2000 Sb., o obcích (obecní zřízení), v platném znění: K uzavření této smlouvy o dílo došlo na základě usnesení Rady města Orlová č. 839/21 ze dne 22.11.2023.
14. Nedílnou součástí smlouvy je tato její příloha:

– Nabídka zhotovitele

V Orlové dne:

[redacted]

Ing. Martina Szotkowská,

vedoucí odboru rozvoje a investic

V Praze dne:

[redacted]

Bc. Martin Novák

prokurista

Za věcnou a ekonomickou správnost [redacted]

Za právní správnost: [redacted]

DATA SYS

NABÍDKA

Zahájení projektu kybernetické bezpečnosti

Zadavatel

Město Orlová
Osvobození 796
735 14 Orlová

DATASYS s.r.o.
Jeseniova 2829/20, 130 00 Praha 3
+420 225 308 111
datasys@datasys.cz
www.datasys.cz

POBOČKY
HRADEC KRÁLOVÉ, Hořická 283/22, 500 02
PLZEŇ, Schwarzova 50, 301 00
DĚČÍN, Labská 694/24, 405 02
OSTRAVA, Studentská 6202/17, 708 33

HOTLINE – SERVIS HW
Jeseniova 2829/20, 130 00 Praha 3
+420 225 308 250
helpdesk@datasys.cz
IČO: 61249157 / DIČ: CZ61249157

OBSAH

1. Popis situace

Tato nabídka vynikla na základě jednání ze dne 2.7. 2024 a směřuje k zvýšení odolnosti Města Orlová proti kybernetickým hrozbám v souladu s připravovaným novým zákonem o kybernetické bezpečnosti (NZoKB) a souvisejícími provádějícímu předpisy. Dalším významným vstupem pro nabídku jsou dlouhodobé zkušenosti společnosti DATASYS v této oblasti s ohledem na respektované normy a osvědčené postupy.

Nabídka je koncipovaná tak, aby směřovala k postupnému dosažení cílů a povinností v oblasti bezpečnosti informací ať již dnes známých, tak předpokládaných, které vzniknou přijetím připravované legislativy.

Přestože je přijetí zákona, resp. počátek jeho platnosti očekává až v říjnu 2024 jsme přesvědčení, že je potřeba problematiku bezpečnosti informací řešit bezodkladně.

Aktuální předpokládaný harmonogram související s přijetím NZoKB je následující:

- 18.10. 2024 – platnost NZoKB (odhad)
- Jeden rok na implementaci

Město Orlovu jakožto obec s rozšířenou působností bude podle projednávaných návrhu spadat do tzv. režimu nižších povinností.

Protože implementace systémů řízení bezpečnosti informací je vždy určitou zátěží nejen na pracovníky IT, ale všechny zaměstnance, doporučujeme postupné nasazování jednotlivých politik a opatření v návaznosti na priority vycházející ze stanoveného rozsahu.

Celý koncept je navržen tak, aby realizace jednotlivých kroků vedly k naplnění konkrétních ustanovení nové regulace a samozřejmě k posílení informační bezpečnosti. Jsme přesvědčeni, že navržený postup je postaven smysluplně s fokusem na konkrétní povinnosti a opatření v souladu s dobrou praxí.

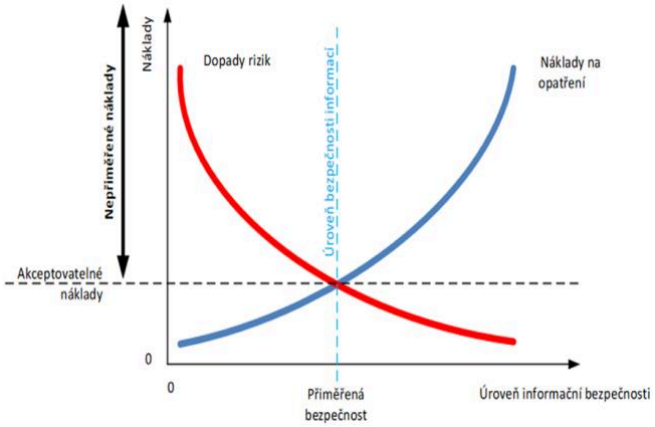
Našim cílem je pomáhat našim klientům budovat přiměřenou bezpečnost.

2. Předmět nabídky

Nabídka je rozdělena na několik oblastí, z nichž některé mají určitou návaznost a jiné mohou být řešeny samostatně. Cenová nabídka, resp. kvalifikovaný odhad je uveden v Kapitole 3.

Vzhledem k aktuálnímu stupni poznání nejsme schopni udělat přesnou kalkulaci, takže jsme navrhli realizaci úvodních kroků, doplnili o údaje předložené interními pracovníky IT a kvalifikovaným odhadem nákladů u jednotlivých položek.

Základní princip našeho přístupu k problematice je postaven na dosažení přiměřené bezpečnosti za akceptovatelné nákladů, tak jak je znázorněno na následujícím obrázku.



2.1 Seznámení vedení

Připravovaný regulace ukládá vrcholovému vedení organizací určité povinnosti, které budou dány Vyhláškou a to konkrétně **§ 5 - Povinnosti vrcholného vedení**.

Vzhledem k tomu, že jednou z připravovaných povinností je zajišťování dostupnosti zdrojů potřebných pro zajišťování kybernetické bezpečnosti považujeme za důležité realizovat seznámení vrcholového vedení neodkladně formou bezplatného workshopu, tak aby plně pochopilo jednak své povinnosti, ale zejména principy a důvody dané problematiky, které jim umožní kvalifikované rozhodování a s tím souvisejícím efektivním vynaložením nákladů.

Bezplatný workshop navrhujeme provést ve dvou krocích:

- Vrcholové vedení obce
- Vedení úřadu a zřizovaných organizací

a to formou interaktivních workshopů, které by umožnit lepší seznámení s problematikou.

2.1.1 Vstupní školení zaměstnanců

Jednou z povinností připravované regulace je realizace vstupního školení a periodická zaměstnanců – ustanovení Vyhlášky **§ 6 - Bezpečnost lidských zdrojů body c-f).** Navrhujeme provést vstupní školení zohledňující relevantní témata dle **Přílohy číslo 4 - Doporučená témata pro rozvoj bezpečnostního povědomí**, doplněná o seznámení s připravovanými kroky implementace.

2.1.2 On-line školení zaměstnanců

Jednou z možností, jak zajistit periodické školení zaměstnanců je vytvoření nástroje pro on-line školení. Pro tyto účely používáme nástroj Moodle. Vzdělávací systém dodáváme jako kompletní dodávku včetně konceptu. Moodle má široké možnosti využití, tudíž ho rádi přizpůsobíme vašim požadavkům a potřebám i v jiných oblastech, než je bezpečnost informací.

Samozřejmostí je možnost nástroje využití pro zřizované organizace.

2.2 Stanovení rozsahu kybernetické bezpečnosti

Stanovení rozsahu je implementace kybernetické bezpečnosti je základním krokem pro úspěšnou implementaci systému řízení bezpečnosti informací. Který je obsažen i v připravovaném NZoKB konkrétně **§ 13 - Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby,** ale i podle normy ČSN ISO/IEC 27001:2023 – Kontext organizace. Obecně doporučujeme pracovat se skupinou norem ISO 27000 jako s pomocným materiálem pro lepší pochopení problematiky.

Hodnocení stavu kybernetické bezpečnosti bude řízeno certifikovaným auditorem, zaměstnancem firmy DATASYS s certifikací CISA[1]. Sběr dat pro analýzu bude za DATASYS zajišťovat jeden bezpečnostní specialista. V rámci plnění dle této nabídky budou poskytnuty služby, jejichž cílem je zjistit a posoudit aktuální stav bezpečnosti IT infrastruktury Zadavatele a procesů spojených s provozem této infrastruktury, zejména pak stav technických i organizačních bezpečnostních kontrol, které jsou v provozním prostředí IT infrastruktury aplikovány. Výstupem budou též doporučená opatření vedoucí ke zlepšení stavu.

Jako další vstup pro stanovení rozsahu by mělo být expertní posouzení stavu některých dalších povinností v souladu s ustanoveními Vyhlášky **§ 8 - Řízení přístupu, § 9 - Řízení identit a jejich oprávnění, § 10 - Detekce a zaznamenávání kybernetických bezpečnostních událostí v rozsahu bodu 1), § 12 - Bezpečnost komunikačních sítí a § 14 - Kryptografické algoritmy bod 2)**. Tato část bude realizována pohovory s pracovníku IT a případnými prezentacemi používaných řešení a technologiemi včetně zálohování.

Výstupem plnění dle této části nabídky budou:

- Dokument **Katalog aktiv** s uvedením priorit primárních aktiv pro zajištění business kontinuity činnosti
- Dokument „**Analýza stavu kybernetické bezpečnosti**“ s návrhem doporučených opatření
- Základní návrh opatření ve formátu Přílohy číslo 1 **Přehled bezpečnostních opatření** Vyhlášky.

Obsahem dokumentů hodnocení je souhrnný grafický přehled úrovní členěný dle paragrafů vyhlášky o kybernetické bezpečnosti i detailní tabulkový rozpad plnění požadavků vyhlášky a konkrétní návrhy potřebných opatření. Samozřejmě nechybí přehledová manažerská zpráva z provedeného hodnocení úrovně kybernetické bezpečnosti.

2.3 Provedení testu zranitelnosti

Nad technickými aktivy doporučujeme provést vstupní sken zranitelnosti v souladu s ustanoveními Vyhlášky **§ 13 - Aplikační bezpečnost, bod c)**. Současně budou výstupy použity pro zajištění souladu s ustanoveními Vyhlášky **§ 13 - Aplikační bezpečnost, body a) a b).**

Provedením testu zranitelnosti tak získáte jistotu, že řádně chráníte své systémy/data a schopnost vyhodnotit a upřednostnit zranitelnosti, které není snadné opravit a identifikovat. Zároveň snížíte šance, že budete zdrojem infekce pro další organizace, se kterými spolupracujete, což požaduje i směrnice NIS2. V neposlední řadě odhalení problematických míst a jejich prioritizace posiluje účinnost antivirových systémů, firewallů a dalších bezpečnostních nástrojů.

Tento test bude realizován jako **asistovaná zápůjčka hardwarové sondy** nástroje Greenbone Security Manager (GSM) pro získání přehledu o zařízeních v síti a zejména pro zjištění a zvládání zranitelných služeb sítě. Asistovaná zápůjčka typicky Zadavateli slouží k ověření vlastností nástroje před jeho pořízením. Tato naše nabídka na provedení je vhodná pro téměř všechny typy společností, které nedisponují vlastním analogickým nástrojem. **Greenbone Security Manager** je renomovaný automatizovaného skener zranitelností německého výrobce.

[1] Certified Information Systems Auditor.

Služba zápůjčky GSM zahrnuje:

- Zápůjčku dvouportové hardwarové sondy „GSM 100“ na dva týdny
- Dopravu sondy k Objednateli, na místo určené k zapojení sondy do sítě (1 lokalita)
- Zapojení, instalaci a konfiguraci zařízení (ve spolupráci s IT oddělením Objednatele)
- Zaškolení pracovníků IT oddělení Objednatele
- Průběžné telefonické konzultace
- Sestavení přehledu doporučených kroků a závěrečný workshop
- Odpojení a odvoz sondy

2.4 Expertní posouzení stavu

Navrhujeme expertní posouzení stavu některých dalších povinností v souladu s ustanoveními Vyhlášky **§ 8 - Řízení přístupu, § 9 - Řízení identit a jejich oprávnění, § 10 - Detekce a zaznamenávání kybernetických bezpečnostních událostí v rozsahu bodu 1), § 12 - Bezpečnost komunikačních sítí a § 14 - Kryptografické algoritmy bod 2)**. Tato část bude realizována pohovory s pracovníku IT a případnými prezentacemi používaných řešení a technologiemi včetně zálohování.

.

2.5 Implementace bezpečnostních opatření a nástrojů

V souvislosti se zjištěnými skutečnostmi navrhujeme provést:

- Prioritní eliminace největších rizik, dle výsledku zjištění,
- bezodkladné zajištění aplikování bezpečnostních aktualizací vydaných pro technická aktiva,
- nastavení/doplnění již používaných technologií (technických aktiv),
- zahájení prací na některých povinných opatřeních zejména ve vztahu k bezpečnosti komunikačních sítí jako jsou viditelnost zařízení, škálovatelnost a usnadnění administrace,
- výběr a zahájení nasazování podpůrných technologií pro práci IT (další detekční nástroje, logmanager atd,)

Tuto část nejsme v této chvíli schopni přesně nacenit, takže si musíme pomoct kvalifikovaným odhadem.

2.5.1 Prioritní eliminace rizik

Tento krok je zaměřen na rychlé odstranění problémů, které se objeví při Stanovení rozsahu. Podle současného stavu poznání můžeme soudit, že by se nemusely objevit zásadní problémy. Z aktuálních rozhovorů vyplývá, že pracovníci interního IT hlavní body řeší (multifaktor, off-line zálohy, perimetr, ochrana koncových bodů), příprava na obměnu síťových prvků apod. Ale bez provedené analýzy nelze tuto možnost vyloučit.

2.5.2 Aplikace bezpečnostních aktualizací

Jde o požadavek připravované Vyhlášky **§ 13 - Aplikační bezpečnost, bod a)** a současně velmi osvědčený/nezbytný prostředek pro eliminaci známých zranitelností. U méně významných aktiv nebi již nepodporovaných aktiv, lze jejich ochranu dosáhnout jinými opatřeními, jako je například jejich umístění do samostatného segmentu sítě v souladu s body **b) 2-3. uvedeného paragrafu**. Součástí výstupu bude i vytvoření patřičné dokumentace.

U významných již nepodporovaných aktiv bude zpracován návrh na jejich nahrazení. Tuto problematiku již pracovníci interního IT průběžně řeší.

2.5.3 Optimalizace využité již používaných technických aktiv

Organizace velmi často disponují řadou užitečných a často velmi vyspělých technologií, které nejsou z různých důvodu plně využívány. V této oblasti lze správným nastavením dosáhnout významného zvýšení bezpečnosti za

rozumné prostředky. Součástí řešení může být například i změna licenční politiky, která může vést i k případným úsporám.

2.5.4 Zahájení prací

Na základě stanoveného rozsahu, doporučujeme zahájit práce na realizaci povinných opatření podle stanovených priorit. Jde v podstatě a rozumné a užitečné věci, jejichž realizaci nemá smysl odkládat.

2.6 Další technologie

Oproti předchozí kapitole jde o implementaci technických aktiv nebo procesů, které nejsou povinné, ale umožní jednak další zvýšení bezpečnosti nebo usnadnění práce IT pracovníků. Případné nasazení doporučujeme provést až po vyhodnocení účelnosti. S ohledem na limitovaný počet pracovníků IT může dávat smysl realizace formou tzv. řízené služby.

2.6.1 Logmanager/SIEM

Log Manager je nástroj pro správu protokolů, který shromažďuje, ukládá a analyzuje logy (záznamy o událostech) z různých zdrojů v síti. To pomáhá organizacím identifikovat a řešit problémy v síti, detekovat bezpečnostní incidenty a dodržovat předpisy týkající se uchovávání dat.

SIEM kombinuje správu bezpečnostních informací a správu událostí v reálném čase. Poskytuje celkový pohled na bezpečnostní stav organizace tím, že shromažďuje a analyzuje logy a upozornění z různých zdrojů, což usnadňuje rychlou detekci, vyšetřování a reakci na bezpečnostní hrozby.

2.6.2 Network Access Control

NAC je řešení pro kontrolu přístupu k síti, které zajišťuje, že všechna zařízení a uživatelé splňují určité bezpečnostní normy, než jim umožní přístup do síťových zdrojů. To pomáhá chránit síť před neautorizovaným přístupem, usnadňuje práci s připojením k wifi, správě BYOD zařízená, hlídání servisních oken a v neposlední řadě usnadňuje administraci sítě.

V kombinaci se správně provedenou segmentací sítě, nastavením přístupových práv a dalšími opatřeními poskytuje velmi dobrý základ tzv. architektury nulové důvěry (Zero trust Architecture), což je bezpečnostní model, který přistupuje k ochraně IT prostředí s předpokladem, že žádný uživatel nebo zařízení uvnitř, nebo vně sítě není automaticky důvěryhodný. Tento model je založen na principu "nikomu nedůvěřovat, všechno ověřovat".

2.6.3 Monitoring datových toků a detekce anomálií

Tento nástroj monitoruje a analyzuje síťový provoz prostřednictvím sledování datových toků v síti. Umožňuje identifikovat vzorce provozu, detekovat anomálie a optimalizovat výkon sítě.

NDR (Network Detection and Response): NDR se zaměřuje na detekci a reakci na bezpečnostní hrozby v síti. Používá pokročilé analytické techniky a umělou inteligenci k identifikaci podezřelého chování v síťovém provozu, což pomáhá včas odhalit a zareagovat na bezpečnostní incidenty.

2.6.4 Pokročilá ochrana DNS

DNS je systém, který překládá lidsky čitelné názvy domén (např. www.priklad.com) na IP adresy. Ochrana DNS může pomoct při blokování škodlivých webových stránek a obsahu, čímž chrání uživatele před chrání uživatele před malwarem, phishingem a jinými internetovými hrozbami. Ochrana proti různým typům útoků zaměřených na DNS, jako jsou DNS spoofing a DDoS útoky, které mohou ohrozit dostupnost a integritu DNS služeb a řadu dalších.

2.7 Projektový management implementace

Součástí nabídky je i zajištění projektového řízení eventuálně outsourcing role osoby odpovědné za kybernetickou bezpečnost, resp. pomoc při výchově interního člověka, a to včetně koordinace a sledování legislativních povinnosti a bezpečnostních trendů nebo konzultační činnost.

3. Cena

Zjištění rozsahu řízení kybernetické bezpečnosti vůči požadavkům zákona spolu s volitelným provedením základního technického testu pro praktické ověření reálné stávající úrovně zabezpečení vašeho IT nabízíme provést **za níže uvedené ceny bez DPH**. Zároveň jde o první kroky, které doporučujeme provést a které definují celkový rozsah, priority a další kroky a jejich cenový rámec.

3.1 Zjištění rozsahu řízení kybernetické bezpečnosti

Popis	Cena bez DPH
Provedení analýzy KB s návrhem cílového stavu	60 000 Kč

Ceny jsou uvedeny bez DPH.

3.2 Volitelné praktické bezpečnostní testy

Praktické testy doporučujeme provést, aby hodnocení studie nevycházelo jen z informací získaných z řízených rozhovorů s pracovníky IT a garanty aktiv ale i těchto testů.

Popis	Cena bez DPH
Sken zranitelností služeb počítačové sítě s návrhem doporučení k jejich odstranění	30 000 Kč

Ceny jsou uvedeny bez DPH.

3.3 Další kroky

Není možné stanovit jinak, než expertním odhadem a pro další technologie, uvedené níže v bodě 2.6, není možné při současné znalosti prostředí vytvořit ani tento odhad.

Položka	Typ ceny/poznámka	Cena
2.1 Seznámení vedení	**Úvodní školení zdarma**	**0 Kč**
2.1.2 Vstupní školení zaměstnanců	Bude upřesněno podle rozsahu a způsobu realizace	cca 20 000 Kč
2.1.3 On-line školení zaměstnanců	Bude upřesněno podle rozsahu	cca 100 000 Kč
2.4 Expertní posouzení stavu	podle zjištěného/schváleného rozsahu	
2.5 ***Implementace bezpečnostních opatření a nástrojů***	podle zjištěného/schváleného rozsahu	
2.5.1 Prioritní eliminace rizik	podle zjištěného/schváleného rozsahu	
2.5.2 Aplikace bezpečnostních aktualizací	podle zjištěného/schváleného rozsahu	
2.5.3 Optimalizace využité již používaných technických aktiv	podle zjištěného/schváleného rozsahu	

2.5.4 Zahájení prací na realizaci povinných opatření	podle zjištěného/schváleného rozsahu	
2.6 Další technologie	Bude upřesněno po zjištění rozsahu	
2.6.1 Logmanager/SIEM	podle zjištěného/schváleného rozsahu	
2.6.2 Network Access Control	podle zjištěného/schváleného rozsahu	
2.6.3 Monitoring datových toků a detekce anomálií	podle zjištěného/schváleného rozsahu	
2.6.4 Pokročilá ochrana DNS	podle zjištěného/schváleného rozsahu	
2.7 Projektový management implementace	podle zjištěného/schváleného rozsahu	

3.4 Platnost nabídky, platební podmínky a harmonogram realizace

Platnost nabídky jsou 3 měsíce. DPH činí 21 %. Splatnost faktury vystavené na základě této nabídky je 90 dnů od protokolárního převzetí. Harmonogram realizace bude stanoven po dohodě se Zadavatelem. DATASYS je připraven práce zahájit do 2 týdnů od objednávky.

4. Kvalifikace firmy Datasys

Společnost Datasys svým zákazníkům poskytuje služby v oblasti kybernetické bezpečnosti dlouhodobě. Jedná se zejména o zpracování bezpečnostních studií a analýz rizik, penetrační testy a technické prověrky.

Rozsahem podobné bezpečnostní studie:

1. Severomoravské vodovody a kanalizace Ostrava a.s. (2018)
2. Pramacom Group (2017)
3. ŽĎAS a.s. (2017)
4. LUKOV Plast spol. s r.o. (2017)

Největší obdobné referenční projekty:

1. Analýza rizik v Informačním systému datových schránek (2017)
    a. Ustavení systému řízení bezpečnosti informací (ISMS) dle požadavků ZKB (2017)
    b. Implementace bezpečnostního monitoringu, včetně SIEM (2017)
2. Analýza rizik neklasifikovaných informačních systémů MZV ČR (2013)
    a. Implementace bezpečnostního monitoringu, včetně log management systému (2015)
3. Identifikace aktiv a analýza rizik Správy Pražského hradu (2013)
    a. Zpracování bezpečnostní dokumentace dle požadavků ZKB (2015)

4.1 Platnost nabídky a platební podmínky

Platnost nabídky je 60 dnů.
DPH činí 21%. Splatnost faktury vystavené na základě této nabídky je 30 dnů od protokolárního převzetí.

5. Závěr

Jménem společnosti DATASYS si dovolujeme vyjádřit přesvědčení, že výše uvedená nabídka bude po technické i ekonomické stránce vyhovovat potřebám Vaší organizace a její realizace přispěje ke zkvalitnění prostředí a služeb provozovaných informačních technologií a systémů.
Věříme současně, že náš výklad zadání, navržené postupy, stejně tak jako know-how, technické i lidské zdroje, kterými společnost DATASYS disponuje, skýtají záruky realizace předmětného projektu v nejvyšší kvalitě a k plné spokojenosti Vaší společnosti.

V Ostravě dne 2. 7. 2024

Nabídku zpracoval:
Radim Pracuch

DATA SYS

*Také v IT naleznete **rodinné společnosti.** DATASYS je jednou z nich. Na trhu působíme **od roku 1994** a přinášíme **spolehlivá řešení** v následujících oblastech:*

BEZPEČNOST

Jsme dodavatelem bezpečnostních řešení, nástrojů a služeb. Naší specializací je sledování vzdálených přístupů. Umíme však zabezpečit a monitorovat informační systémy na mnoha úrovních, náš přístup je pragmaticky vyvážený, realizace důsledná.

VÝVOJ A INOVACE

Pokrokové nápady převádíme v realitu. Dodáváme serverové back-end aplikace, klient/server řešení, webové aplikace i aplikace pro mobilní telefony. Dokážeme integrovat oddělené systémy i navrhovat zcela nová řešení.

INFRASTRUKTURA

Informační systémy nemohou fungovat bez pevných základů. Infrastruktura představuje páteř každého informačního systému a my se zaměřujeme na komplexní implementační a integrační služby.

IT AS A SERVICE

Umíme se postarat o všechny vaše IT. Vyřešíme vaše problémy se softwarem i hardwarem, jsme na příjmu 24 hodin denně, 7 dní v týdnu. Budeme vaším opravdovým partnerem pro inovace a IT vám doručíme jako spolehlivou službu.

NAŠI KLIENTI

ČESKÁ POŠTA · SKUPINA ČEZ · PRE · ČSOB · ŠKODA · Allianz · McDonald's

80+
kmenových zaměstnanců

415 mil. Kč
obrat v roce 2018

5000+
realizovaných projektů

25 let
zkušeností

Pojďme se potkat a společně najít vhodné řešení.

Držitel certifikátů ISO 9001:2015, ISO 14001:2015, BS OHSAS 18001:2007, ISO/IEC 20000-1:2011, ISO/IEC 27001:2013