

Nabídka – Posouzení stavu zajištění kybernetické bezpečnosti se zohledněním požadavků NIS2



Pro zákazníka:

Město Valašské Meziříčí

IČ: 00304387

Soudní 1221 757 01 Valašské Meziříčí 1

O₂ IT Services

O2 IT Services s.r.o., Za Brumlovkou 266/2, 140 00 Praha 4 – Michle

IČO 02819678, www.o2its.cz

Obsah

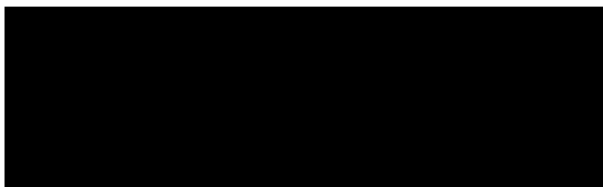
Obsah	2
1. Identifikační údaje dodavatele	3
2. Požadavek Zákazníka	4
3. Návrh řešení	5
4. Harmonogram dodávky	7
5. Cenová nabídka	8
5.1 Cena	8

1. Identifikační údaje dodavatele

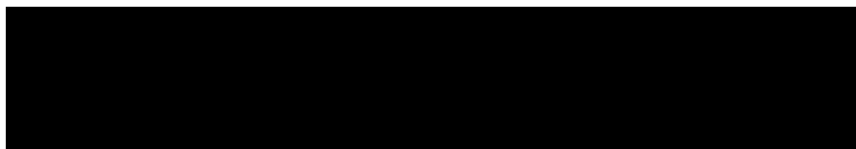
Identifikační údaje dodavatele:

Obchodní jméno:	O2 IT Services s.r.o.
Sídlo firmy:	Za Brumlovkou 266/2, 140 00 Praha 4
IČO:	02819678
DIC:	CZ02819678
Zapsaná:	v obchodním rejstříku Městského soudu v Praze, oddíl C, vložka 223566

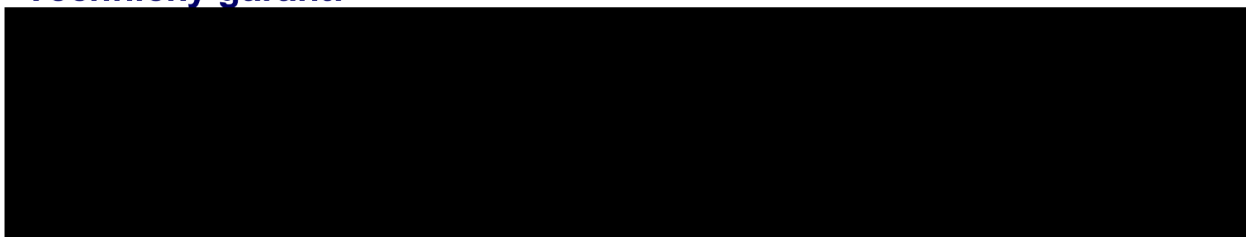
Kontaktní osoba pověřená jednáním jménem dodavatele:



Obchodní garant:



Technický garant:



2. Požadavek Zákazníka

Město Valašské Meziříčí (dále jen Zákazník) vnímá jako problematickou otázku souladu se směrnicí Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Evropské unii, tzv. směrnice NIS2. Cílem Zákazníka je proto prověřit aktuální stav zajištění jeho kybernetické bezpečnosti s ohledem na požadavky směrnice NIS2, a v závislosti na výsledku provedené analýzy stanovit plán konkrétních organizačních i technických opatření.

3. Návrh řešení

Dodavatel na základě požadavku Zákazníka provede komplexní analýzu stavu zajištění jeho kybernetické bezpečnosti, a to především jeho stávající úrovně systému řízení bezpečnosti informací, včetně dokumentace, bezpečnostních pravidel, zavedených procesů a postupů a zralosti stávajících technických opatření, a to mj. i s ohledem na požadavky připravované novely zákona o kybernetické bezpečnosti, včetně prováděcích právních předpisů (národní úprava směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Evropské unii, tzv. směrnice NIS2).

Při provedení analýzy budou využity odborné zkušenosti našeho týmu se znalostí národních i mezinárodních standardů a best practises vztahujících se k bezpečnosti informací, kybernetické bezpečnosti a bezpečnosti informačních systémů. Vždy však bude zohledněn i charakter činnosti Zákazníka a možné dopady narušení jeho kybernetické bezpečnosti jak přímo na jeho činnosti, tak na činnost dalších subjektů, s nimiž spolupracuje a/nebo je jinak propojen.

Nezbytnou podmínkou úspěšného provedení analýzy je součinnost na straně Zákazníka. Základem analýzy budou interview realizačního týmu s vybranými pracovníky Zákazníka. Interview probíhá nad předem stanovenými tématy dle kontrolního listu vycházejícího z požadavků směrnice NIS2 (resp. stávajícího návrhu novely kybernetického zákona a s ní souvisejících právních předpisů, které mají včlenit pravidla směrnice NIS2 do českého práva). Výstup ve formátu xls obsahuje ke každému bodu detailní zhodnocení úrovně zralosti, doporučená nápravná opatření, jejich pracnost a prioritu.

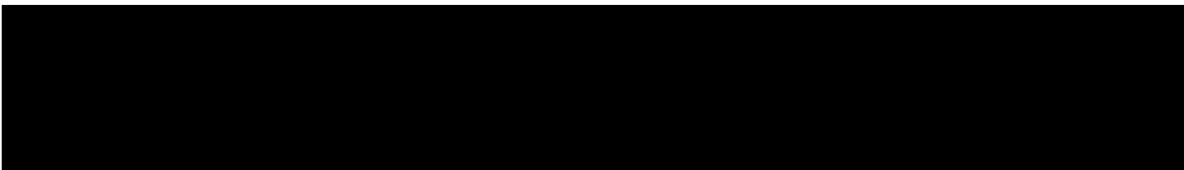
Č.	paragraf	Ref.	Požadavek	Maturity level	Číselná hodnota	Návrh opatření	Pracnost / Cena	Priorita
§ 4 Systém řízení bezpečnosti informací								
4	Systém řízení bezpečnosti informací	4.2.c.4	Povinná osoba v případě neplnění povinností řízení rizik podle odstavce 1 písm. c): kybernetické bezpečnostní incidenty, včetně dříve řešených,	Optimised	5			3
4	Systém řízení bezpečnosti informací	4.2.c.5	Povinná osoba v případě neplnění povinností řízení rizik podle odstavce 1 písm. c): výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti	Limited	2			2
4	Systém řízení bezpečnosti informací	4.2.c.6	Povinná osoba v případě neplnění povinností řízení rizik podle odstavce 1 písm. c): výsledky penetračního testování a skenování zranitelností,	Managed & Control	4			3
4	Systém řízení bezpečnosti informací	4.2.d	v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.	Standardized	3			2
§ 5 Povinnosti vrcholového vedení								
5	Povinnosti vrcholového vedení	5.1.	Vrcholové vedení s ohledem na systém řízení bezpečnosti informací	Nonexistent	0			1
5	Povinnosti vrcholového vedení	5.1.a	se prokazatelně účastní školení podle § 11 odst. 3 písm. a),	Ad-hoc	1			1

Mimo tohoto detailního přehledu je vypracována závěrečná zpráva, která obsahuje manažerské shrnutí, popis krátko i střednědobé strategie pro posílení kybernetické bezpečnosti Zákazníka, hlavní oblasti rozvoje a popis nejvíce rizikových faktorů.

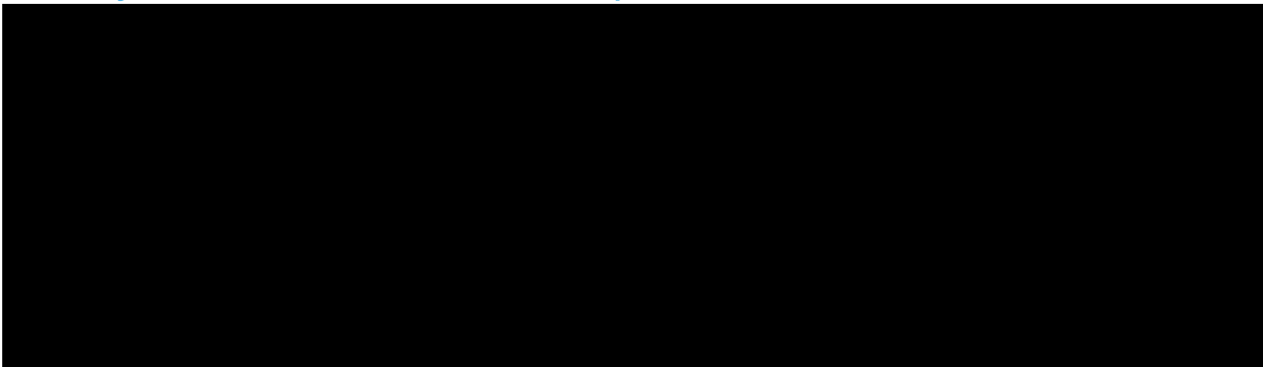
1. Úvodní workshop



2. Provedení analýzy



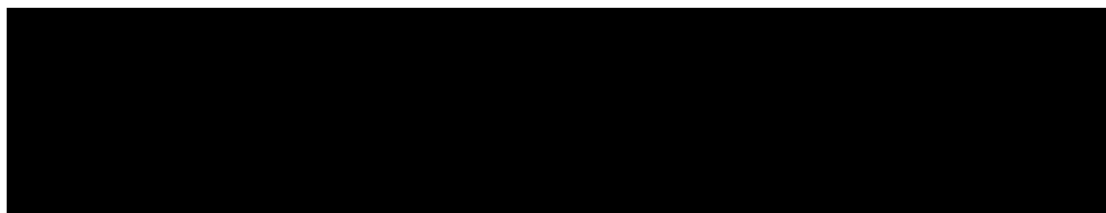
3. Vyhodnocení a závěrečná zpráva



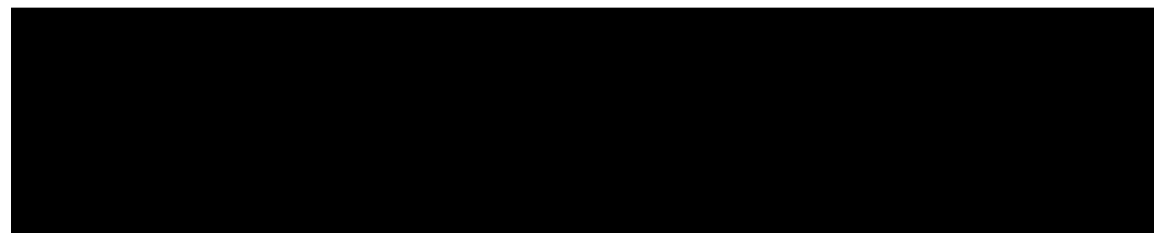
4. Harmonogram dodávky

Realizaci projektu předpokládáme Q4 2024.

5. Cenová nabídka



5.1 Cena



SHRNUTÍ PODMÍNEK KONZULTAČNÍCH SLUŽEB PREZENTOVANÝCH V NABÍDCE:**(„PODMÍNKY“):****O2 IT Services s.r.o.,**

IČO 02819678, DIČ CZ02819678, sídlo Za Brumlovkou 266/2, Praha 4 - Michle, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 223566 („Poskytovatel“ nebo též „my“).

Pokud Zákazník akceptuje Nabídku, akceptací souhlasí s následujícími podmínkami konzultačních služeb, které jsou obsažené v této Nabídce („Služby“) a zavazuje se jimi řídit:

1. Srozumitelnost a konkrétnost

Kybernetická bezpečnost je oblast, u níž je více než kde jinde podstatné, aby klient chápal, co konkrétně pro něj tato oblast obnáší. Poskytovatel je technologickou společností, jejíž výhodou je ovšem i to, že dokáže svým zákazníkům lidsky vysvětlit, co pro ně konkrétně bude znamenat rámec opatření známý pod zkratkou NIS2. Obecné principy se vždy snažíme vztáhnout na konkrétního zákazníka. Jsme připraveni stát se průvodcem, který umožní zákazníkům se zamyslet nad metodicky kladenými otázkami, určit klíčové procesy a určit vhodná nápravná opatření.

2. Spolupráce v průběhu projektu

Součinnost ze strany zákazníka je u Služeb naprosto zásadní. Zákazník se pro účely řádného plnění Služeb zavazuje vytvořit Poskytovateli a spolupracovníkům Poskytovatele veškeré pracovní podmínky pro řádný a bezpečný výkon práce při poskytování Služby a veškerou součinnost při řešení všech otázek souvisejících s poskytováním Služby.

Zákazník se proto pro účely řádného poskytnutí Služby zavazuje poskytnout Poskytovateli veškerou součinnost potřebnou k poskytnutí Služby, resp. je povinen učinit vše, aby mohl Poskytovatel Službu poskytnout podle Nabídky. Zejména se zavazuje poskytnout Poskytovateli veškeré informace, podklady, materiály, přístupy, které jsou nebo mohou být pro poskytování Služby Poskytovatelem potřebné a Poskytovatel je takto označí.

3. Úvodní posouzení stavu

Tým odborníků s potřebnými certifikacemi je připraven provést zákazníka úvodním posouzením, v jakém stavu se nachází jeho bezpečnostní, organizační a technologická opatření a poskytnout srozumitelnou metodiku k tomu, aby případné nedostatky napravil. Výsledkem diagnostické fáze, kterou naši specialisté procházejí společně se zákazníkem, je prvotní vyhodnocení, které je východiskem pro naplánování dalších aktivit.

4. Doporučení pro nápravu

Další fází konzultačních Služeb je srozumitelné doporučení, jaké kroky má zákazník ohledně kybernetické bezpečnosti dále učinit a jaké interní nebo externí procesy má zavést. Doporučení mohou obsahovat i opatření technického rázu, tedy zejména nákup zařízení či služeb, které mohou přispět ke zvýšení úrovně kybernetické bezpečnosti u zákazníka.

5. Potřeba následného převzetí ze strany zákazníka

Kybernetickou bezpečnost nelze přirozeně zajistit jedním krokem, nákupem jednoho zařízení či jedné služby ani ji považovat vyřízenou jednorázově. Kybernetická bezpečnost je disciplína vyžadující soustavnost a spočívá v aplikování celé řady postupů. Implementovaný systém opatření proto následně vyžaduje soustavné udržování a případný vývoj v rámci životního cyklu zákazníka a jeho činností (například pokud se začne zabývat novou oblastí podnikání nebo agendy). Proto je následně potřeba i zajistit pravidelné ověřování aktuálnosti implementovaného rámce opatření, pokud se změnily vnitřní či vnější okolnosti. Součástí doporučení tedy může být i návrh, v jakém rozsahu mají být obsazeny interní role vyžadované předpisy upravujícími kybernetickou bezpečnost. Konzultační Služby podle této Nabídky tedy přirozeně trvale nenahrazují interní role ani procesy ani nepřenesají odpovědnost za dodržování opatření a právních předpisů na Poskytovatele. Konzultační Služby podle této Nabídky tedy může vedení zákazníka vzít v úvahu při vytváření svého systému zajištění kybernetické bezpečnosti, nicméně podle právních předpisů vedení zákazníka zůstane i nadále odpovědné za samotné dodržování principů kybernetické bezpečnosti a zajištění dostatečných dlouhodobých kapacit (personálních, technických i finančních) umožňujících dosáhnout trvalý soulad s relevantními předpisy a/nebo best practice.

Jako Poskytovatel poskytneme Službu s náležitou péčí, avšak neodpovídáme jakýmkoliv způsobem zákazníkovi ani jakékoliv jiné osobě za následnou implementaci řešení a případná porušení nebo nedodržování předpisů ze strany zákazníků či třetích osob poté.

Abychom udržovali vaši informovanost jakožto zákazníka o stavu našich prací a usnadnili projednávání, můžeme v průběhu prací poskytovat dílčí připomínky, zprávy nebo sdělení, a to v jakékoli formě. Takové dílčí průběžné informace nebo sdělení přitom nelze vytrhovat z kontextu a vždy je třeba je chápat v souladu s ostatními zjištěními a doporučeními.

Celková odpovědnost Poskytovatele při poskytování Služby a v souvislosti se Službou je v maximálním rozsahu přípustném právními předpisy omezena na odpovědnost za skutečnou škodu způsobenou Poskytovatelem při poskytování Služby, a to do maximální výše 100.000 Kč (slovy: sto tisíc korun českých). Poskytovatel zejména neodpovídá zákazníkovi za ušlý zisk zákazníka ani jakékoliv jiné osoby ani za jakoukoliv nepřímou nebo následnou škodu nebo nemajetkovou újmu vzniklou zákazníkovi a/nebo jakékoliv jiné osobě. Ustanovení § 2898 obč. zákoníku tím samozřejmě není dotčeno.

6. Spoléháme na pravdivost informací zákazníka

Správnost doporučení a vyhodnocení je samozřejmě závislá i na správnosti a pravdivosti odpovědí a vstupů od zákazníka. Součástí těchto služeb není nezávislé ověřování skutečnosti tvrzených zákazníkem. Pro dosažení kýženého účelu proto platí, že zákazník musí být při spolupráci s našimi specialisty (zejména ve fázi prvotního posouzení stavu) upřímný jak k nám, tak především sám k sobě. Jako Poskytovatel neodpovídáme za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání zákazníka.

7. Kybernetická bezpečnost je důležitá pro každého

S ohledem na skutečnost, že dosud není známá finální podoba českých právních předpisů upravujících kybernetickou bezpečnost podle směrnice NIS2, vychází posouzení z aktuálně známého textu návrhu. NIS2 se formálně bude vztahovat jen na určitou skupinu podnikatelů a orgánů či agend, a to takových, které jsou pro chod státu anebo obsluhu základních potřeb obyvatel či hospodářství důležité. Kybernetická bezpečnost je ale podle našeho názoru důležitá pro všechny, ať již se na ně předpisy formálně vztahovat budou či nikoli. Technická, bezpečnostní a organizační opatření popisovaná v NIS2 a návrzích předpisů je totiž možné doporučit všem subjektům. Pokud by kybernetický incident mohl jim samotným způsobit závažné škody, musí se i ony samy na tuto eventualitu připravit. Myslíme si tedy, že povědomí o kybernetické bezpečnosti (co to vlastně znamená a jak se dá řešit), by měli mít všichni naši zákazníci a nejen ti, kteří budou formálně spadat pod regulaci. Konzultační Služby podle této Nabídky tak jsou přínosem pro každého potencionálního zákazníka. Pro uvedení do souladu s regulací, si zákazník po nabytí účinnosti nové regulace musí překontrolovat podle účinného znění právních předpisů, zda a do jaké kategorie regulovaných subjektů bude spadat. Doporučujeme pravidelně ověřovat předpoklady pro zařazení do určité kategorie, protože se změnou rozsahu činností, změnou velikosti podniku zákazníka, změnou předpisů nebo rozhodovací praxe se zařazení může v čase měnit. Smluvní strany prohlašují, že se žádná z nich necítí být vůči druhé smluvní straně slabší stranou.

8. Nepřenosnost na další osoby

Jakýkoli materiál obsahující naše doporučení, analýzu nebo shrnutí, který zákazníkovi poskytneme, je určen pouze zákazníkovi pro výše uvedený účel. Není přirozeně použitelný pro jakékoli jiné zákazníky a další osoby či orgány. Nepřijímáme proto žádnou odpovědnost vůči žádné další straně. Jakýkoli materiál obsahující naše doporučení, analýzu nebo shrnutí nesmí být poskytnut k nahlédnutí nebo jakkoli jinak komunikován či dán ve známost žádné další straně bez našeho předchozího písemného souhlasu, který můžeme podle svého uvážení udělit, odepřít nebo udělit za určitých podmínek (včetně podmínek týkajících se spoléhání se třetích stran, nebo vylučujících či omezujících naši odpovědnost).

9. Rozsah služeb, ceny a splatnost

Poskytovatel poskytne Službu v rozsahu a způsobem specifikovanými v zákaznickém akceptované Nabídce. Smluvní vztah nelze uzavřít s výhradou, dodatkem či odchylkou od těchto Podmínek ani rekapitulací jinými slovy. Zákazník se zavazuje Poskytovatelovo řádně poskytnuté plnění převzít a zaplatit Poskytovateli cenu uvedenou v akceptované Nabídce. Není-li v Nabídce uvedena odlišná splatnost, platí splatnost 30 dní od doručení faktury (daňového dokladu) zákazníkovi.