SPRÁVA ŽELEZNIC

OBJEDNÁVKA

Číslo: 23_801170001 **S**

Zpracoval:

Tel. číslo:
Email:

Objednatel:
Správa železnic, státní organizace
Dlážděná 1003/7
Praha 110 00

Dodavatel:
ALEF NULA,a.s.
Pernerova 691/42
186 00 Praha
IČO: 61858579 DIČ: CZ61858579

Notifikace: 21.3.2023 12:23

Objednávku vystavuje organizační složka:
Správa železnic, státní organizace
Dlážděná 1003/7
Praha 1 110 00

IČO: 70994234 DIČ: CZ70994234
"Zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384"

Termín dodání: test T+1 M, re-test T+3 M	**Finanční objem (bez DPH) do:** CZK 236 000,00
Způsob dopravy: Bez_dopravy	**Způsob platby:** Převodem
Povaha nákupu: [X] provoz [ ] investice [ ] FKSP	**Účetní okruh:** [ ] MOZ [ ] HOM [X] ZDC

Č. j.:

Smlouva: 78281/2022-SZ-GR-O8

Splatnost faktury: 30 dní

Potvrzený termín dodání:

Adresa místa plnění:
Správa železnic, státní organizace
Dlážděná 1003/5
Praha 1 110 00

Fakturu zašlete:
Správa železnic, státní organizace
Centrální finanční účtárna Čechy
Náměstí Jana Pernera 217
Pardubice 530 02

Objednáváme u Vás:

Čís.ř.	Kód MTZ	Název	MJ	Množství	Cena / jedn.
1		Projektová cena za bezpečnostní testování	MD	20,000	11 800,00

Pokračování je na straně 2

Přílohy:	žádné
Záruční doba:	Dle dohody

Objednávka je podstatnou náležitostí daňového dokladu (faktury). Na daňový doklad uvádějte své IČO, DIČ nebo potvrďte, že nejste plátci DPH. Uveďte, jestli jste fyzická nebo právnická osoba. Úrok z prodlení respektujeme pouze v zákonné výši dle nařízení vlády č.351/2013 Sb. Termín splatnosti bude akceptován po doručení úplného daňového dokladu. Daňový doklad může být uhrazen ze dvou účtů, a to zvlášť základ DPH a zvlášť DPH.

Žádáme o zaslání potvrzené objednávky zpět spolu s daňovým dokladem! Bez potvrzené objednávky nelze daňový doklad akceptovat jako úplný a nemůže být proplacen.

Dodavatel včas poskytne odběrateli informaci o možných změnách týkajících se identifikačních údajů společnosti, včetně možné změny bankovních údajů.

Objednatel je povinen uveřejňovat uzavřené smlouvy (objednávky včetně její písemné akceptace) v Registru smluv na základě ustanovení zákona číslo 340/2015 Sb. (viz zadní strana objednávky).

Smluvní strany se dohodly, že stane-li se dodavatel nespolehlivým plátcem nebo daňový doklad dodavatele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je objednatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně dodavatele.

V případě poskytnutí osobních údajů dodavateli je dodavatel povinen tyto údaje zabezpečit dle Nařízení evropského parlamentu a rady o ochraně osobních údajů č. 2016/679 (GDPR).

Praha 1, dne:

(razítko, podpis)

Objednatel:

jméno: Mgr. Karel Peška MBA v.r., 22. 3. 2023

Praha, Akceptováno dne:

(jméno, příjmení, razítko, podpis)

Dodavatel: Radek Švadlenka v.r., 27. 3. 2023

Čís.ř.	Kód MTZ	Název	MJ	Množství	Cena / jedn.

Předmětem dodávky je realizace jednorázového automatizovaného bezpečnostního testu na 82 doménách Zákazníka, nacházejících se na 10 IP adresách. Cílem testování je základní mapování externího perimetru a odhalení případných zranitelností v externí infrastruktuře a na webových aplikacích, které by potenciální útočník mohl zneužít za účelem jejich navazujícího odstranění a zvýšení bezpečnosti.
Seznam domén, které budou testovány byl předán Objednatelem. Seznam IP adres, které budou v rámci bezpečnostního testu testovány byl předem domluven.

Testování externí infrastruktury, která je dostupná na výše uvedených IP adresách, bude prováděno automatizovaným způsobem za účelem základního mapování perimetru Objednatele a odhalení případných zranitelností v této infrastruktuře.
Testování webových aplikací, které jsou dostupné na předaných doménových jménech, bude prováděno automatizovaným způsobem za účelem odhalení případných zranitelností ve webových aplikacích.
Bezpečnostní testy budou realizovány formou black box/zero knowledge testu a budou realizovány v předem dohodnutém termínu po poskytnutí všech potřebných informací pro spuštění testování. Testy budou provedeny z předem definovaných veřejných IP adres Dodavatele.

Používané metodiky
Pro testování budou využity metodiky používané firmou Alef Nula a.s., které vychází z mnohaletých zkušeností jejích bezpečnostních specialistů a kombinují různé frameworky, standardy a best practice postupy. Tyto jsou používány a aplikovány dle konkrétních nároků bezpečnostního testu a řadí se mezi ně mimo jiné:
• Penetration Testing Execution Standard (PTES),
• Open Source Security Testing Methodology Manual (OSSTMM),
• NIST Special Publication (SP) 800-115,
• Metodiky Licensed Penetration Tester (LPT),
• Information Systems Security Assesment Framework (ISSAF),
• Metodiky a standardy organizace Open Web Application Security Project (OWASP):
o Web Security Testing Guide (WSTG),
o Mobile Security Testing Guide (MSTG),
o Application Security Verification Standard (ASVS),
o OWASP Top 10.
Pro potřeby evaluace charakteristiky a závažnosti zranitelnosti:
• Common Vulnerability Scoring System (CVSS) v3.1.
Testovací tým Alef Nula a.s. využívá pro hledání a testování na přítomnost zranitelností jak manuální postupy zmíněné v předchozích metodikách, tak pomocné a automatické nástroje pro specifické prostředí, účel, či služby. Jako příklad lze uvést aplikaci BurpSuite Pro, Tenable Nessus Professional, NMAP, SQLMap, Gobuster, Metasploit Framework a jiné.

Výstupy z bezpečnostního testování
Výsledky testů budou shrnuty v závěrečné zprávě. Ta bude obsahovat seznam identifikovaných služeb/portů a zranitelností v rámci bezpečnostního testu, jejich detailní popis a ohodnocení jejich nebezpečnosti dle CVSS v3.1 a také doporučení pro jejich odstranění. Přílohy závěrečné zprávy pak mohou obsahovat výstupy nástrojů či jiné průkazné informace, které by svojí velikostí nebyly vhodné pro formát závěrečné zprávy.
Součástí testů nebude vyhledávání zranitelností v jiných než uvedených aplikacích, v síťové, cloudové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů, které přímo nesouvisí s provozem cílového aplikačního systému. Součástí dodávky rovněž nebude testování odolnosti aplikace vůči volumetrickým útokům typu DoS (DDoS), testování fyzické bezpečnosti serverů, ani testy užívající phishing, nebo jiné sociotechnické postupy. Mimo rozsah projektu je také tvorba jakékoliv jiné dokumentace než výše uvedené závěrečné zprávy a jejích příloh. Při realizaci bezpečnostních testů není možné garantovat absenci dopadů na dostupnost testovaných systémů. V případě zjištění omezené dostupnosti cílového systému nebo určité služby v důsledku testů, uvědomí testovací tým o situaci neprodleně kontaktní osobu na straně Zákazníka.

Re-test zranitelností
Pro ověření, zda byly nálezy zranitelností z bezpečnostního testu odstraněny, bude v dohodnutý termín provedený re-test zranitelností. Ten se bude týkat zranitelností, na které byly uplatněny doporučení pro jejich odstranění obsažené v závěrečné zprávě. Re-test bude dále reportovaný v samostatné zprávě po skončení re-testů.

Podkladem pro akceptační protokol bude souhrnná Zpráva z testu, popř. Zpráva z re-testu.
Kontaktní osoba objednatele: Jan Šaroch, vedoucí oddělení řízení událostí a incidentů.

Tato objednávka představuje nabídku ve smyslu § 1731 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ“). Akceptace objednávky musí být písemná. Konkludentní přijetí nabídky je vyloučeno (§ 1744 OZ). Dodavatel bere na vědomí, že akceptací této objednávky dojde k uzavření smlouvy. Objednatel uveřejní objednávku i přijetí nabídky v registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „ZRS) za předpokladu, že se bude jednat o smlouvu ve smyslu ustanovení § 2 odst. 1 ZRS, na níž nedopadá výjimka dle ustanovení § 3 ZRS. Dodavatel akceptací nabídky souhlasí se zveřejněním údajů o identifikaci smluvních stran, předmětu smlouvy, jeho ceně či hodnotě a datu uzavření této smlouvy v registru smluv.

Neoznámí-li dodavatel objednateli písemně společně s akceptací této objednávky, které konkrétně specifikované údaje považuje za své obchodní tajemství ve smyslu ustanovení § 504 OZ, či že se v objednávce vyskytují informace, jež nemohou být v registru smluv uveřejněny v souladu s ustanovením § 3 odst. 1 ZRS, bude objednatel postupovat tak, jakoby se takové údaje a informace v objednávce nevyskytovaly. S částmi objednávky, které dodavatel neoznačí za své obchodní tajemství před uzavřením této objednávky, nebude objednatel jako s obchodním tajemstvím nakládat a ani odpovídat za případnou škodu či jinou újmu takovým postupem vzniklou. Za označení těchto údajů a informací odpovídá výhradně dodavatel, a to bez ohledu na to, která ze stran tyto údaje či informace znečitelní a objednávku uveřejní. Totéž platí pro oznámení dodavatele, že na jeho osobu či tuto objednávku dopadá některá z výjimek uvedených v ustanovení § 3 odst. 2 ZRS.

Dodavatel akceptací této objednávky prohlašuje, že:

1. **není** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „Zákon o střetu zájmů“) nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a že žádní poddodavatelé, jimiž prokazuje/prokazoval kvalifikaci v zadávacím řízení, nejsou obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti
2. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti na plnění této objednávky, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů, jimž se zakazuje zadat nebo dále plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, článků 7 a 8, čl. 10 písm. b) až f) a písm. h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a písm. g až i), článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ECa,
3. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti na plnění této objednávky, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014 **(tzv. sankční seznamy)** , platných ke dni akceptace této objednávky,
4. přestane-li on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti na plnění této objednávky, nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat výše uvedené podmínky, k nimž se toto četné prohlášení vztahuje, a to **kdykoliv až do okamžiku splnění této objednávky** , oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však do 3 pracovních dnů ode dne, kdy přestal splňovat výše uvedené podmínky, k nimž se toto četné prohlášení vztahuje, zadavateli této objednávky.