Objednávka č. O-0048/INF/2024

Středočeský kraj

Odběratel:
Středočeský kraj
Zborovská 11, 150 21 Praha 5
číslo účtu: [redacted]
IČ 70891095
DIČ CZ70891095

Dodavatel:
TOTAL SERVICE a.s.
U Uranie 954/18,
17000, Praha
IČO: 25618067
DIČ: CZ25618067

Datum: 02. 04. 2024

Objednáváme u Vás:

Předmět objednávky	Množství	Jednotka	Cena vč. DPH Kč
Bezpečnostní test (penetrační testy Portálu Středočeského kraje	1	akce	172 667,00 Kč

Dodávka je podrobně specifikována v příloze k této objednávce, která je nedílnou součástí objednávky.
V souladu s nabídkou NAB-15454-T1F6H5 ze dne 27.03.2024

Celková cena dodávky včetně DPH 172 667,00 Kč

Celková cena bez DPH 142 700,00 Kč

Místo dodání: **Krajský úřad Středočeského kraje**

Termín dodání: **Předpoklad do 21 dní od účinnosti objednávky, tj. po zveřejnění objednávky v registru smluv**

Délka záruční doby za jakost dodávky: ----------

Při fakturaci uvádějte číslo naší objednávky. Faktury bez tohoto označení Vám budou vráceny k doplnění.
Splatnost faktury je 30 dní od jejího doručení odběrateli.

Daniel Rokos
Digitálně podepsal Daniel Rokos
Datum: 2024.04.02 10:45:27 +02'00'

.....

Mgr. Bc. Daniel Rokos, vedoucí Odboru informatiky
Datum a podpis

Potvrzení objednávky dodavatelem:

Výše uvedenou objednávku akceptujeme a souhlasíme s jejím zveřejněním v registru smluv.

Jan Navrátil
Digitálně podepsal Jan Navrátil
Datum: 2024.04.03 12:32:18 +02'00'

.....

Jméno, příjmení, funkce
Datum a podpis

Razítko dodavatele:
(jestliže je objednávka podepisována dodavatelem ručně a dodavatel používá razítko)

Předmětem objednávky je závazek Dodavatele poskytovat Zadavateli služby spočívající zejména v:

Provádění vnějších penetrační testů (Portál SK – stredoceskykraj.cz) představujících simulaci napadení systémů útočníkem, který má k dispozici pouze veřejně dostupné informace. Cílem testů je zjistit, jak snadno identifikovatelný cíl Portál SK Zadavatele představuje, jaké informace lze získat o zvenčí dostupném Portálu SK, jak detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění.

Vnější penetrační testy budou provedeny ze sídla Dodavatele vůči testovanému Portálu SK, který je provozován v rámci Technologického centra kraje. Seznam IP adres bude dodán před zahájením vlastního testování Zadavatelem. Použité IP rozsahy, ze kterých bude testování prováděno, budou registrovány na Dodavatele.

Penetrační test se bude skládat z: Vypracování zprávy o stavu bezpečnosti prověřovaného Portálu SK Zadavatele vypracované Dodavatelem budou předány v elektronické podobě.

testů k získání informací, identifikace funkčních systémů;

všeobecných testů zranitelnosti;

testů týkajících se charakteristiky infrastruktury systému;

testů spolehlivosti konfigurace, testů existence backdoors;

testů autentizace a schémat pro kontrolu přístupu;

kontroly operačních systémů;

testů aplikačních chyb a vad v systému;

testů nedostatečného provozního zabezpečení;

testování slabých míst zahrnující body selhání, s cílem způsobit odmítnutí služeb webové aplikace;

zneužití odchycených informací a komunikace směrem k aplikačním službám (serverům).

Testování se bude skládat z následujících fází.
Identifikace cíle;

Identifikace aktivních služeb;

Identifikace zranitelností;

Získání přístupu;

Eskalace privilegií a ovládnutí cíle;

Reakce na testy.

Penetračními testy, které jsou předmětem plnění, není pouze provádění automatizovaných (vulnerability) skenů.

Pro testování budou využity nejméně 3 následující metodiky a doporučení týkající se bezpečnosti informačních systémů. Metodiky mohou být interně přizpůsobeny Dodavatelem.

Doporučení OWASP (Open Web Application Security Project), která se zaměřují na pomoc organizacím při identifikaci bezpečnostních hrozeb webových aplikací;

Standard OSSTMM (Open Source Security Testing Methodology Manual) – metodologie pro testování bezpečnosti;

OSVDB – Open Source Vulnerability Dababase – komunitní databáze zranitelností;

Doporučení organizace IETF (Internet Engineering Task Force) – organizace vydávající RFCs tzv. standardy internetu;

Doporučení organizace NIST (např. NIST SP 800-44 Guidlines on Securing Public Web Servers);

CVE – Common Vulnerabilities and Exposures – standardizovaný slovník obecných zranitelností a ohrožení;

Common Criteria (ISO/IEC 15408) – standard pro hodnocení úrovně bezpečnosti systémů;

Normy pro řízení bezpečnosti IS/ICT, řízení kvality projektu a provádění auditů: ▪ normy řady ISO/IEC 27000 pro oblast řízení bezpečnosti informačních systémů;

▪ BS 7799-3 Směrnice pro řízení rizik souvisejících s informační bezpečností;

▪ ČSN EN ISO 19011:2002 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu;

▪ ČSN ISO 10006 – Management jakosti – Směrnice jakosti v managementu projektu.