zlín.

statutární město Zlín
náměstí Míru 12 • 760 01 Zlín

S00JP0104I43

OBJEDNÁVKA č.: O260200219

ze dne: 01.09.2020

Objednatel:

statutární město Zlín
Městská policie Zlín
náměstí Míru 12
76001 Zlín

IČO: 00283924
DIČ: CZ00283924

Dodavatel:

Univerzita Tomáše Bati ve Zlíně - Fakulta aplikovaně...

Nad Stráněmi 4511
76005 Zlín

IČO: 70883521
DIČ: CZ70883521

Bankovní spojení: Česká spořitelna, a.s., pobočka Zlín
č. účtu: příjmový 3048982/0800, výdajový 3048982/0800
Vyřizuje: Sovadina Lukáš ing.
Tel./Mail: [redacted] /

1. Předmět plnění

Objednáváme u Vás:
automatizovaný penetrační test LAN segmentů (MP Zlín) - viz příloha

2. Cena plnění (včetně DPH)

Kč 91 960,00

3. Termín plnění

30.09.2020

4. Ostatní (platební podmínky, odpovědnost za vady, záruky, sankce apod.)

Objednatel i dodavatel berou na vědomí, že tato objednávka vyžaduje ke své účinnosti uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registr smluv (zákon o registru smluv), ve znění pozdějších předpisů. Za účelem splnění povinnosti uveřejnění této objednávky se statutární město Zlín zavazuje, že ji do registru smluv zašle neprodleně, nejdéle však do 30 dnů od jejího vystavení. (jedná se o objednávky s hodnotou předmětu plnění vyšší než 50 000 Kč bez DPH)

Doložka dle § 41 odst. 1 zákona č. 128/2000 Sb., o obcích	
Schváleno orgánem obce:	*Rada města Zlína*
datum a číslo usnesení:	*16.12.2019, č. usn. 75/25R/2019*

zlín. statutární město Zlín 1
[redacted]
IČ 002 e Zlín Zlín 1 3924

Kladnič [redacted] A
ředitel [redacted] lín

SOUHLASÍM
JIŘÍ KOVÁŘ
[redacted]

Automatizovaný penetrační test zaměřený LAN segmenty používané MP Zlín

- Identifikace běžících služeb a zpracování seznamu známých zranitelností.
- Testy autentizačních procesů používaných na serveru.
- Testy odolnosti serveru vůči útokům vedených na služby serveru, tak i na hostovanou aplikaci.
- Testovány budou zranitelnosti dle OWASP top TEN:
  - A01: Injection
  - A02: Broken Authentication and Session Management
  - A03: Sensitive Data Exposure
  - A04: Insecure Direct Object References
  - A05: Security Misconfiguration
  - A06: Sensitive Data Exposure
  - A07: Missing Function Level Access Control
  - A08: Insecure Deserialization
  - A09: Using Known Vulnerable Components
  - A10: Unvalidated Redirects and Forwards
- Testy budou probíhat pomocí metody z vnitřní sítě MP Zlín.
- Omezení počtu segmentů v ceně kalkulace – max. 5 rozsahů Class C (5 x 256 IP)
- Ověření zabezpečení WAN portů přes veřejný Internet (v kalkulaci max. 5 WAN portů).
- Ověření možností sniffingu na infrastruktuře.

1. 9. 2020

[redacted]