Veřejná zakázka

**„Zvýšení kybernetické bezpečnosti města Pelhřimov – část A“**

**Zadavatel:**

**Město Pelhřimov**se sídlem Pelhřimov, Masarykovo náměstí 1, PSČ 393 01   
IČO: 00248801  
DIČ: CZ00248801

Osoba zastupující zadavatele: Ladislav Med, starosta

Detailní specifikace předmětu plnění

# **Rozsah služeb**

Předmětem plnění této části veřejné zakázky je objektivní a nezávislé zmapování aktuálního stavu kybernetické bezpečnosti informačních systémů města, identifikace mezer vůči legislativním požadavkům (ZoKB, NIS 2, GDPR) a následně ověřit technologickou odolnost prostřednictvím cílených penetračních testů, v rozsahu:

**2.1 Vstupní audit a základní analýza**

* Analýza politik, směrnic, procesů a dokumentace systému řízení informační bezpečnosti (ISMS).
* Interview a workshopy s klíčovými pracovníky (IT, management) k popsání aktuálního stavu.
* Provedení základního skenování technické infrastruktury – interní i externí – pro zjištění zranitelností.

**2.2 GAP analýza**

* Porovnání stavu s požadavky ZoKB, NIS 2, GDPR, dobrými standardy (CIS v8, ISO 27001, NIST).
* Identifikace mezer v procesech, technologiích, fyzickém zabezpečení a v dokumentaci.
* Vypracování přehledného reportu s rizikovými ohledy, hodnocením dopadu a prioritizací.
* Navržení konkrétních nápravných opatření (technická i organizační), včetně návrhu úprav dokumentace a doporučení cílového stavu.

**2.3 Penetrační testy**

* Prověření externího perimetru (internetové přístupy, VPN, firewall, veřejné IP služby).
* Interní testování – simulace útoků z vnitřní sítě, testy Wi‑Fi, přístupových práv a bezpečnostního nastavení koncových stanic.
* Testování webových aplikací a veřejných portálů.
* Vypracování detailní Zprávy z penetračních testů: identifikace a detailní popis zranitelností, reprodukce, dopady, urgentnost oprav a doporučení mitigací.

**2.4 Výstupy**

* Kompletní dokument „Vstupní audit a GAP analýza“ s popisem metodiky, zjištění, rizik a doporučení.
* Samostatná Zpráva z penetračního testování s technickými anatomiemi útoků, ukázkami exploitů a navrženými řešeními.
* Přehledný akční plán (Roadmapa) s popisy kroků pro implementaci opatření a stanovenými prioritami.

**3. Standardy, rámce a metodické přístupy**

Zpracování bude vycházet z prověřených přístupů a norem:

* CIS Controls v8, ISO 27001, NIST, ZoKB, NIS 2, GDPR.
* OWASP pro webové aplikace, metodika OWASP Test Guide pro penetrační testy.
* Skenování dle CVSS, rizikové matice.

**Forma předání výstupů:**

* Výstupy budou zpracovány v **českém jazyce**, v elektronické i listinné podobě.
* Elektronická verze bude dodána ve formátu **PDF a DOCX/ODT**, auditní protokoly budou podepsány autorizovaným auditorem.
* Součástí bude i stručné **shrnutí závěrů pro účely dotačního monitoringu**.