Technická specifikace díla

Provedení GAP analýzy bezpečnostních opatření informačních a komunikačních systémů Dopravního podniku Ostrava a.s. Cílem je určení správné kategorie podle připravované novely zákona o kybernetické bezpečnosti a národní implementace směrnice NIS2, identifikovat nesoulady s připravovanou novelou zákona o kybernetické bezpečnosti, vyhláškou o bezpečnostních opatřeních poskytovatele (dále jen vyhláška), případně dalších 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) a vytvořit katalog aktiv pro efektivní řízení kybernetické bezpečnosti.

1. Požadavky na provedení:

Určení kategorie organizace:

- **Analýza legislativy:** Přezkoumání připravovaných právních předpisů a jejich požadavků na různé kategorie subjektů.
- **Posouzení činností organizace:** Hodnocení rolí, odpovědností a služeb Dopravního podniku Ostrava a.s. ve vztahu k nové legislativě.
- **Stanovení kategorie**: Formální určení, zda Dopravní podnik Ostrava a.s. spadá do kategorie s vyššími nebo nižšími povinnostmi, včetně zdůvodnění a dopadů této klasifikace na organizaci.

Vytvoření katalogu aktiv:

- **Identifikace aktiv:** Vytvoření komplexního seznamu všech klíčových aktiv, jako jsou IT systémy, sítě, aplikace a další kritické komponenty, které jsou zásadní pro kybernetickou bezpečnost organizace.
- **Hodnocení hodnoty a klasifikace aktiv:** Posouzení důležitosti každého aktiva, včetně jeho kritičnosti, citlivosti a dopadu na provoz.
- **Přiřazení odpovědných osob:** Určení odpovědných pracovníků za správu a ochranu jednotlivých aktiv.

GAP analýza:

- **Rozsah analýzy**:
    - **Organizační opatření:** Přezkoumání existujících bezpečnostních politik, směrnic a postupů.
    - **Technická opatření:** Analýza technické infrastruktury, systémů a aplikací z hlediska zabezpečení.
    - **Procesní opatření:** Hodnocení procesů pro řízení rizik, řešení incidentů a kontinuitu činností.

- **Metodologie**:
    - Využití mezinárodně uznávaných standardů (např. ISO/IEC 27001).
    - Porovnání stávajícího stavu s požadavky legislativy dle určené kategorie.

Návrh nápravných opatření:

- **Specifičnost**: Opatření musí být konkrétní, aplikovatelná a reflektovat připravované legislativní změny.
- **Prioritizace**: Stanovení priorit na základě rizikovosti a náročnosti implementace, s ohledem na termíny legislativních změn.
- **Časový harmonogram**: Návrh reálných termínů pro realizaci opatření, včetně časového plánu pro splnění nových legislativních požadavků.
- **Odhad nákladů**: Orientační finanční náročnost jednotlivých opatření, včetně investic potřebných pro splnění nových požadavků

2. Výstupy projektu

- **Katalog aktiv**:
    - Kompletní přehled klíčových aktiv včetně jejich klasifikace, hodnocení hodnoty a odpovědných osob.
- **Zpráva o určení kategorie**:
    - Detailní analýza a zdůvodnění zařazení DPO a.s. do příslušné kategorie.
    - Dopady určené kategorie na povinnosti DPO a.s.
- **Zpráva z GAP analýzy**:
    - Detailní popis zjištěného stavu.
    - Identifikace nesouladů s konkrétními paragrafy aktuální i připravované legislativy.
    - Posouzení rizik spojených s identifikovanými nesoulady.
- **Návrh nápravných opatření**:
    - Seznam doporučených opatření s detailním popisem.
    - Prioritizace a časový plán implementace s ohledem na legislativní termíny.
    - Odhad potřebných zdrojů (personálních, finančních).
- **Prezentace výsledků**:
    - Shrnutí klíčových zjištění a doporučení.
    - Diskuze o strategiích implementace.

3. Časový harmonogram

- **Zahájení projektu**: do 1 týdne od podpisu smlouvy
- **Sběr dat a analýza**: 1-2 týdny
- **Vypracování zprávy a návrh opatření**: 2 týdny
- **Prezentace výsledků**: do 1 týdne od vypracování zprávy
- **Ukončení projektu**: bezodkladně po prezentaci a akceptaci výsledků