**Technická specifikace**

Předmětem plnění VZ je poskytnutí služeb ověření účinnosti zavedených bezpečnostních opatření v IS ČOI vůči zákonu č.181/2014 Sb. o kybernetické bezpečnosti. Obsahem poskytnutých služeb Zhotovitele je zpracování diferenční analýzy (GAP analýzy) informačních a komunikačních systémů a technologií České obchodní inspekce, ve které Zhotovitel vyhodnotí shodu bezpečnostních opatření Objednatele s požadavky ZKB. U zjištěných rozdílů navrhne taková opatření, která zajistí soulad se zněním ZKB. Součástí diferenční analýzy bude rámcové posouzení stavu ochrany osobních údajů dle nařízení (EU) 2016/679 - GDPR.

1. **Metodika provedení diferenční analýzy**

Zhotovitel použije pracovní postupy zakládající se na zjišťování stavu současných bezpečnostních opatření oproti požadavkům vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen „Vyhláška o KB“). V tomto smyslu budou analyzovány požadavky ZKB a Vyhlášky o KB vůči reálnému stavu IS ČOI.

Celé vypracování diferenční analýzy bude probíhat ve 3 základních fázích:

* V první fázi proběhne analýza prostředí Objednatele, jejímž cílem je získání potřebných informací pro zpracování diferenční analýzy,
* Ve druhé fázi budou získané informace porovnány s požadavky ZKB. Zhotovitel identifikuje a vyhodnotí zjištěné rozdíly,
* Ve třetí fázi Zhotovitel navrhne nápravná opatření s ohledem na stávající prostředí a požadavky Objednatele.

Ve výsledné zprávě (výstupním dokumentu) Zhotovitel zdokumentuje stávající stav prostředí Objednatele, identifikuje a zhodnotí rozdíly vůči požadavkům ZKB, navrhne bezpečnostní opatření, která zajistí soulad s požadavky ZKB.

1. **Obsah diferenční analýzy**

Požadovaný obsah diferenční analýzy bude zahrnovat:

| **Pol.** | **Činnost** |
| --- | --- |
| **1.** | **Úvod** |
| **2.** | **A: Zákon č.181/2014 Sb. Posouzení zpracované bezpečnostní dokumentace (návrh zpřesnění, doplnění)** |
| 2.1. | Systémová bezpečnostní politika |
| 2.2. | Analýza rizik |
| 2.3. | Politika řízení dodavatelů |
| 2.4. | Rozsah a hranice SŘBD |
| 2.5. | Pravidla nakládání s informacemi |
| 2.6. | Metodika identifikace a vyhodnocení aktiv |
| 2.7. | Metodika identifikace a vyhodnocení rizik |
| 2.8. | Bezpečné chování uživatelů |
| 2.9. | Směrnice pro řízení kybernetických bezpečnostních incidentů |
| **3.** | **Posouzení bezpečnostních nástrojů, opatření implementovaných (v IS ČOI)** |
| 3.1. | Posouzení HW, SW architektury datového centra ČOI |
| 3.2. | Fyzická bezpečnost datového centra ČOI |
| 3.3. | Nástroj pro ochranu integrity komunikačních sítí |
| 3.4. | Nástroj pro ověřování identity uživatelů |
| 3.5. | Nástroj pro řízení přístupových oprávnění |
| 3.6. | Nástroj pro ochranu před škodlivým kódem |
| 3.6. | Nástroj pro zaznamenávání činností VIS, jejich uživatelů a administrátorů |
| 3.7. | Nástroj pro detekci kybernetických bezpečnostních událostí |
| 3.8. | Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí |
| 3.9 | Nástroj pro zajišťování úrovně dostupnosti aplikací |
| **4.** | **Návrh nápravných opatření** |
| 4.1. | Návrh technických opatření |
| 4.2. | Návrh úpravy, doplnění bezpečnostní dokumentace |
| **5.** | **GDPR (základní informace)** |
| 5.1. | GDPR - určení předmětných oblastí (procesů) ČOI s dopadem na ochranu OÚ |
|  | GDPR – zmapování pohybu (dataflow) osobních dat v těchto oblastech  |
| 5.2. | GDPR – kritická místa v těchto dataflow diagramech |
| 5.3. | GDPR – doporučení k zabezpečení (technická, organizační, jiná) těchto kritických míst  |
| 5.4. | GDPR – návrh dalšího postupu |
| **6.** | **Závěr** |

Zhotovitel vypracuje výsledky diferenční analýzy a navržená nápravná opatření ve dvou vyhotoveních:

Dokument č. 1 - v plném rozsahu technických specifikací (určený pro výkonné pracovníky v oblasti
 kybernetické bezpečnosti Objednatele),

Dokument č. 2 - Manažerské shrnutí (určený pro vedení úřadu).

1. **Předpokládaný harmonogram plnění :**
2. Zahájení plnění (realizace projektu) je ke dni účinnosti Smlouvy o zajištění služeb, která bude uzavřena mezi Objednatelem a dodavatelem, jehož nabídka bude vyhodnocena jako nejvhodnější.
3. Předání pracovního dokumentu s výsledky analýzy prostředí Objednatele pro kontrolu plnění stavu projektu. Předání analýzy je nejpozději do 40 dnů od zahájení plnění (kontrolní den č. 1).
4. Předání pracovního dokumentu se zjištěnými rozdíly v prostředí IS ČOI vůči požadavkům ZKB do 60 dnů od zahájení plnění (kontrolní den č. 2).
5. Ukončení plnění předmětu VZ, tj. odevzdání finálního dokumentu diferenční analýzy je nejpozději do 90 dnů od zahájení plnění.
6. Podrobný časový harmonogram bude sestaven a vzájemně odsouhlasen až po zahájení projektu v rámci úvodního jednání v závislosti na dostupnost odpovědných pracovníků Objednatele.