Příloha č. 1 výzvy: Technická specifikace předmětu plnění

Předmětem plnění této veřejné zakázky jsou činnosti v oblasti technických opatření kybernetické a informační bezpečnosti. Konkrétně se jedná o níže uvedené projekty a činnosti:

a) **Architekt kybernetické bezpečnosti**
b) **Identifikace a hodnocení aktiv a rizik**
c) **Zvyšování bezpečnostního povědomí**
d) **Zvládání bezpečnostních incidentů**
e) **GAP analýza nového ZoKB**

Plnění níže uvedených činností bude vždy probíhat na základě schválené rozsahu v člověkodnech, kdy bude dodavatel seznámen se všemi informacemi, podklady a skutečnostmi pro odhad náročnosti činností. Tyto budou vždy, před započetím činností, schváleny ze strany UK.

Celkový předpokládaný rozsah činností za všechny níže uvedené položky je 130 člověkodnů, přičemž 1 člověkoden = 8 hodin práce.

a) Architekt kybernetické bezpečnosti

Požadujeme dodávku role Architekta kybernetické bezpečnosti dle platného zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Předpokládaný rozsah činností je 50 člověkodnů.

Předmětem činností bude zejména:

- Definování vhodných technických opatření na základě identifikovaných rizik.
- Návrh vhodné architektury současné počítačové sítě z pohledu technických opatření vedoucích k zajištění kybernetické bezpečnosti.
- Návrh vhodné architektury připravovaných projektů a záměrů z pohledu technických opatření vedoucích k zajištění kybernetické bezpečnosti.
- Návrh vhodného nastavení bezpečnostních nástrojů.
- Součinnost při vyhodnocování kybernetických incidentů.

b) Identifikace a hodnocení aktiv a rizik

Obsahem je poskytování odborných činností spočívajících v kompletním dokončení identifikace a hodnocení aktiv a rizik.

Předpokládaný rozsah činností je 25 člověkodnů.

Konkrétně se bude jednat o následující činnosti:

- Na základě již existujících výstupů dojde k jejich kompletní revizi a dopracování do požadovaného stavu v souladu s požadavky ZoKB.
- Vypracování seznamu rizik.
- Společně s ÚVT dojde k vydefinování technických opatření v rámci plánu zvládání rizik.
- Společně s ÚVT dojde k dopracování prohlášení o aplikovatelnosti.
- Vytvoření závěrečné zprávy o identifikaci, hodnocení aktiv a rizik.
- Vytvoření prezentace pro VŘKB.

Výstupní dokumentace:

- Seznam rizik.
- Plán zvládání rizik.
- Prohlášení o aplikovatelnosti.
- Zpráva o identifikaci a hodnocení aktiv a rizik.
- Prezentace pro vedení VŘKB.

c) Zvyšování bezpečnostního povědomí

Obsahem je poskytování odborných činností spočívajících ve zvyšování bezpečnostního povědomí zaměstnanců UK.

Předpokládaný rozsah činností je 15 člověkodnů.

Konkrétně se bude jednat o následující činnosti:

- Bezpečnostní příručka pro zaměstnance:
    - Revize připomínek a workshop se zástupci jednotlivých fakult (5 fakult),
    - Zapracování všech obdržených připomínek od zástupců jednotlivých fakult,
    - Zpracování nové verze dokumentu,
    - Představení a revize připomínek od zástupců jednotlivých fakult,
    - Druhá revize připomínek od zástupců jednotlivých fakult,
    - Vytvoření finální verze dokumentu,
    - Vytvoření prezentace pro VŘKB.
- Vytvoření plánu rozvoje bezpečnostního povědomí.
- Vytvoření seriálu kybernetické bezpečnosti pro prezentaci jednotlivých oblastí Bezpečnostní příručky pro zaměstnance

Výstupní dokumentace:

- Bezpečnostní příručka pro zaměstnance UK.
- Prezentace pro VŘKB.
- Plán rozvoje bezpečnostního povědomí.
- Seriál kybernetické bezpečnosti.

d) Zvládání bezpečnostních incidentů

Obsahem je provedení analýzy současného stavu procesů, kybernetických bezpečnostních nástrojů a osob, které jsou zapojeny do procesu zvládání bezpečnostních incidentů. Na základě provedené analýzy bude vypracována směrnice zvládání bezpečnostních incidentů a předložen seznam doporučení. Dokumenty zajistí rychlejší a efektivnější zvládání případných kybernetických bezpečnostních incidentů.

Předpokládaný rozsah činností je 30 člověkodnů.

Konkrétně se bude jednat o následující činnosti:

- Analýza nastavení a využívání nástroje SIEM.
- Analýza nastavení procesů a možností reakcí CSIRT CUNI.
- Vytvoření směrnice zvládání bezpečnostních incidentů pro prostředí rektorátu, na základě získaných informací.

- Vytvoření prezentace pro VŘKB.

Výstupní dokumentace:

- Zpráva o nastavení a využívání SIEM včetně doporučení ke zlepšení.
- Zpráva o reakčních schopnostech CSIRT CUNI včetně doporučení.
- Prezentace zprávy o využívání SIEM a CSIRT CUNI.
- Směrnice zvládání bezpečnostních incidentů.
- Prezentace pro VŘKB.

e) GAP analýza nového ZoKB

Obsahem je provedení (rozdílové) GAP analýzy vůči požadavkům nového ZoKB. Tato část předpokládá realizaci ke konci roku 2024, kdy by již mělo být známo konkrétní znění nového zákona. V případě, že nové znění zákona v době realizace ještě nebude k dispozici, bude GAP analýza prováděna vůči poslední verzi, kterou Národní úřad pro kybernetickou a informační bezpečnost odeslal Legislativní radě vlády.

Předpokládaný rozsah činností je 10 člověkodnů.

Konkrétně se bude jednat o následující činnosti:

- Provedení společného Workshopu s odpovědnými osobami.
- Zpracování výsledné zprávy.
- Vytvoření prezentace.

Výstupní dokumentace:

- Výsledná zpráva GAP analýzy.
- Prezentace pro VŘKB.