Specifikace předmětu veřejné zakázky

A. Seznámení se s IT prostředím zadavatele a příslušných příspěvkových organizací

Předmětem seznámení formou řízených analytických workshopů budou veškeré informační a komunikačními systémy a technologie, tomu odpovídající procesy a dokumentace objednatele, které se vztahují k oblasti kybernetické bezpečnosti a řízení rizik.

Analýza bude pokrývat veškeré aspekty nutné pro zajištění informační a kybernetické bezpečnosti příslušných příspěvkových organizací. Zadavatel požaduje pohled legislativní, organizační, procesní, architektonický až na úroveň konkrétních užívaných technologií a s nimi spjatých pracovních postupů s cílem optimalizace využití možností dohledového centra ze strany Kybernetického operačního centra Jihomoravského kraje (dále jen „KOC JMK“) pro zvýšení úrovně informační a kybernetické bezpečnosti předmětných organizací.

B. Posouzení aktuálního stavu kybernetické bezpečnosti příspěvkových organizací

Zadavatel požaduje komplexní popis včetně posouzení aktuálního stavu systému řízení bezpečnosti informací a kybernetické bezpečnosti a aktuálního stavu technických opatření kybernetické bezpečnosti v souvislosti s požadavky platné legislativy ČR.

Zadavatel požaduje, aby pro posouzení skutečného stavu informační a kybernetické bezpečnosti v příslušných příspěvkových organizacích vybraný dodavatel použil přístup postavený na analýze míry konkrétních rizik.

Zadavatel požaduje soupis aktuálně předávaných logů do KOC JMK, soupis dalších logů, které je možné předávat do KOC JMK za účelem zvýšení kybernetické bezpečnosti příspěvkové organizace s využitím stávajících technologií a postupů.

Součástí analýzy bude také posouzení míry využití stávajících technologií a SW nástrojů z hlediska jejich efektivity a potenciálu pro zvýšení kybernetické bezpečnosti příspěvkové organizace (např. expertním nastavením funkcí).

Zadavatel požaduje, aby každý nesoulad s dobrou praxí vybraný dodavatel hlouběji zanalyzoval, rozčlenil na detailní nálezy a každý takový nález ohodnotil mírou rizika dle vyhlášky o kybernetické bezpečnosti.

Výstupem této části předmětu veřejné zakázky bude popis a hodnocení zjištěného aktuálního stavu organizačních a technických bezpečnostních opatření a přehled zjištěných nedostatků v zajištění kybernetické bezpečnosti proti požadavkům zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

C. Vypracování návrhu aktivit ke zlepšení stavu kybernetické bezpečnosti příspěvkových organizací

Zadavatel požaduje vypracování **návrhu aktivit ke zlepšení kybernetické bezpečnosti cestou optimalizace využití stávajících technologií a SW nástrojů a zvýšení jejich efektivity**.

Výstupem této části předmětu veřejné zakázky dále bude popis budoucího stavu systému řízení bezpečnosti informací a přehled doporučených technických bezpečnostních opatření v provozu chráněných aktiv, přičemž:

a. Rizika budou jednoznačně pojmenována jazykem srozumitelným managementu jednotlivých příspěvkových organizací,
b. Ke každému riziku budou navržena doporučená opatření tak, aby byla adresována všechna zjištěná rizika, u každého opatření bude určen vliv opatření na snížení jednotlivých rizik a budou expertním odhadem vyčísleny 3leté celkové náklady TCO (Total Cost of Ownership - celkové náklady spojené s vlastnictvím) zahrnující veškeré investiční a provozní náklady, pracnost na realizaci a personální náklady na provoz,
c. Pro opatření ke snížení nejvýznamnějších rizik, u kterých je nutný nákup nových technologií, bude připraven soupis technických parametrů tak, aby bylo možné co nejrychleji zahájit hledání vhodných řešení.

D. Provedení prioritizace aktivit a návrh celkového harmonogramu provedení opatření ke zvýšení úrovně kybernetické bezpečnosti příspěvkových organizací

Výstupem této části předmětu veřejné bude seznam všech aktivit s určením jejich priorit, vzájemných závislostí, doporučení na čas jejich zahájení a odhad jejich trvání, přičemž:

a. Pro jednotlivá navržená opatření bude provedena analýza nákladů a přínosů zohledňující celkové 3leté náklady na opatření a míru spjatého rizika,
b. Z analýzy bude pro každou oblast patrné, jaká opatření mají nejvyšší účinnost ve smyslu snížení bezpečnostního rizika a měla by být realizována přednostně,
c. Plán implementace navržených opatření sloučí jednotlivá opatření do realizovatelných celků (projektů, procesních změn apod.) v časové granularitě kvartálů na období jednoho až tří let,
d. Zavedení opatření budou naplánována metodou, jež zajistí co nejrychlejší snížení nejvýznamnějších rizik a zároveň zohlední vazby a návaznosti mezi projekty a potenciální synergické efekty společných aktivit napříč příspěvkovými organizacemi.