POŽADAVKY NA ANALÝZU

Název veřejné zakázky	**Analýza stavu kybernetické bezpečnosti v jihočeských nemocnicích**

Obecné požadavky

- výstupy naplní požadavky Vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti (dále jen VoKB) a budou obsahovat všechny náležitosti dle § 5 Řízení rizik této vyhlášky
- analýza zahrne v dostatečném detailu všechny jihočeské nemocnice, prvotní hloubková analýza bude provedena formou řízených analytických workshopů s cílem identifikace nejvýznačnějších potenciálních rizik
- analýza bude pokrývat veškeré aspekty nutné pro zajištění informační a kybernetické bezpečnosti nemocnice
- výstupy provedené analýzy musí být dále porovnatelné do takové míry, aby mohlo být na jejich základě dosaženo další úrovně vyhodnocení při sjednocení postupů napříč jihočeskými nemocnicemi
- požadujeme konzultanty se zaměřením na znalost problematiky organizace a řízení (včetně legislativy) na úrovni konkrétních procesů nezbytných pro zajištění informační a kybernetické bezpečnosti, a expertní znalost bezpečnostní architektury na úrovni konkrétního nastavení jednotlivých IT nástrojů nezbytných pro zajištění informační a kybernetické bezpečnosti

Seznámení s prostředím Objednatele

- předmětem seznámení budou informační a komunikačními systémy a technologie, dále s procesy a dokumentace Objednatele, které se vztahují k oblasti kybernetické bezpečnosti a řízení rizik
- požadujeme pohled legislativní, organizační, procesní, architektonický až na úroveň konkrétních užívaných technologií a s nimi spjatých pracovních postupů

Posouzení aktuálního stavu kybernetické bezpečnosti Objednatele

- požadujeme komplexní popis včetně posouzení aktuálního stavu systému řízení bezpečnosti informací a kybernetické bezpečnosti a aktuálního stavu technických opatření kybernetické bezpečnosti
- pro posouzení skutečného stavu informační a kybernetické bezpečnosti ve všech nemocnicích bude použit přístup postavený na analýze míry konkrétních rizik
- každý nesoulad s dobrou praxí bude hlouběji analyzován, rozčleněn na detailní nálezy a každý takový nález bude ohodnocen mírou rizika dle VoKB
- výstupem bude popis a hodnocení zjištěného aktuálního stavu organizačních a technických bezpečnostních opatření a přehled zjištěných nedostatků v zajištění kybernetické bezpečnosti proti požadavkům Zákona o kybernetické bezpečnosti a VoKB

Vypracování návrhu aktivit ke zlepšení kybernetické bezpečnosti

- včetně návrhu na provedení investic do informačních a komunikačních systémů a technologií Objednatele za účelem posílení úrovně kybernetické bezpečnosti
- výstupem bude popis budoucího stavu systému řízení bezpečnosti informací a přehled doporučených technických bezpečnostních opatření v provozu chráněných aktiv
- jednotlivé oblasti budou posouzeny ve smyslu současné úrovně zralosti i návrhu zralosti cílové včetně odůvodnění, pro posuzování zralostí bude použit jednoduchý model (např. CMMI), zamýšlený posun v úrovni zralostí jednotlivých oblastí během implementace strategie bude navržen v granularitě let
- rizika budou jednoznačně pojmenována jazykem srozumitelným managementu jednotlivých nemocnic
- 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) zahrnující veškeré investiční a provozní náklady, pracnost na realizaci a personální náklady na provoz
- 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 (RFI)

Provedení prioritizace aktivit a návrh celkového harmonogramu provedení opatření ke zvýšení úrovně kybernetické bezpečnosti u Objednatele

- výstupem bude seznam všech aktivit s určením jejich priorit, vzájemných závislostí, doporučení na čas jejich zahájení a odhad jejich trvání
- pro jednotlivá navržená opatření bude provedena analýza nákladů a přínosů zohledňující celkové 3leté náklady na opatření a míru spjatého rizika
- z analýzy bude pro každou oblast patrné, jaká opatření mají nejvyšší účinnost ve smyslu snížení bezpečnostního rizika a měla by být realizována přednostně
- plán implementace navržených opatření sloučí jednotlivá opatření do realizovatelných celků (projektů, procesních změn apod.) v časové granularitě kvartálů na období jednoho až tří let
- 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 nemocnicemi

Popis jednotlivých jihočeských nemocnic z hlediska ICT

Nemocnice České Budějovice, a.s.

Celkový počet uživatelů	3500
Počet zaměstnanců IT oddělení	9
Počet zaměstnanců v oblasti kyberbezpečnosti	1
Počet koncových stanic	1400
Počet serverů	150
Počet aktivních prvků	350
Počet aplikací	500

Nemocnice Český Krumlov, a.s.

Celkový počet uživatelů	450

Počet zaměstnanců IT oddělení	2
Počet zaměstnanců v oblasti kyberbezpečnosti	0
Počet koncových stanic	252
Počet serverů	22
Počet aktivních prvků	25
Počet aplikací	40

Nemocnice Dačice, a.s.

Celkový počet uživatelů	68
Počet zaměstnanců IT oddělení	1
Počet zaměstnanců v oblasti kyberbezpečnosti	0
Počet koncových stanic	52
Počet serverů	6
Počet aktivních prvků	10
Počet aplikací	6

Nemocnice Jindřichův Hradec, a.s.

Celkový počet uživatelů	800
Počet zaměstnanců IT oddělení	v současnosti 5 (příprava na nový NIS, jinak 4)
Počet zaměstnanců v oblasti kyberbezpečnosti	0 (nikdo nedělá pouze kyberbezpečnost)
Počet koncových stanic	430
Počet serverů	15 fyzických (včetně hostitelských) + 15 virtuálních
Počet aktivních prvků	25 (switche LAN) + 15 (switche kamerového systému a oddělené pac. wifi s cca 50 AP)
Počet aplikací	30

Nemocnice Písek, a.s.

Celkový počet uživatelů	550
Počet zaměstnanců IT oddělení	3
Počet zaměstnanců v oblasti kyberbezpečnosti	1
Počet koncových stanic	470
Počet serverů	45 virtuálních
Počet aktivních prvků	56
Počet aplikací	25

Nemocnice Prachatice, a.s.

Celkový počet uživatelů	250
Počet zaměstnanců IT oddělení	3
Počet zaměstnanců v oblasti kyberbezpečnosti	0
Počet koncových stanic	250
Počet serverů	32 VM / 10 HW
Počet aktivních prvků	Cca 26 významných
Počet aplikací	Do 30 významných

Nemocnice Strakonice, a.s.

Celkový počet uživatelů	507
Počet zaměstnanců IT oddělení	3
Počet zaměstnanců v oblasti kyberbezpečnosti	2
Počet koncových stanic	365
Počet serverů	25
Počet aktivních prvků	32
Počet aplikací	40

Nemocnice Tábor, a.s.

Celkový počet uživatelů	1100
Počet zaměstnanců IT oddělení	5
Počet zaměstnanců v oblasti kyberbezpečnosti	0
Počet koncových stanic	600
Počet serverů	30 virtuálních/8 fyzických
Počet aktivních prvků	65
Počet aplikací	30 +