



Váš dopis zn.	Naše č.j	Vyřizuje / linka	Datum
	MC05 38966/2024	Dubinová Dobromila Bc./257000959 dobromila.dubinova@praha5.cz	1.3.2024

Poskytnutí informací podle § 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

MČ Praha 5, Úřad MČ Praha 5, jako povinný subjekt podle § 14 odstavec 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ“) obdržel dne 20.2.2024 žádost o poskytnutí informací, kterou eviduje pod č.j. MC05 38996/2024 ve znění: „náplň práce manažera kybernetické bezpečnosti, jaká je konkrétní náplň práce, jak vypadá pracovní den manažera kybernetické bezpečnosti?“

V souladu s příslušnými ustanoveními InfZ poskytujeme následující informace:

Na ÚMČ Praha 5 není v rámci systemizace zřízena pracovní pozice manažera kybernetické bezpečnosti. Tato agenda je řešena dohodou o pracovní činnosti (DPC) - zaměstnanec vykonává zejména pracovní činnosti:

Sjednaná činnost/název	Zajišťování činností manažera kybernetické bezpečnosti, zahrnující tvorbu postupů a pravidel pro zajišťování kybernetické bezpečnosti a souvisejících požadavků, plynoucích z doporučení NÚKIB a z platné legislativy.
Rozsah	10 hodin měsíčně (maximálně 120 hodin po dobu platnosti a účinnosti dohody)
Výstup (např.: analýza, protokol, ekonomická studie, monitoring apod.).	Měsíční přehled provedených prací, pro zajištění kybernetické bezpečnosti na pracovištích ÚMČ Praha 5.

Manažer kybernetické bezpečnosti v rozsahu odpovídajícím dohodě o pracovní činnosti (10 hodin měsíčně) zajišťuje tyto konkrétní činnosti:

- koordinuje a dohlíží na plnění požadavků plynoucích z legislativy (ZoKB, z. o ISVS a další)
- koordinuje zavádění a realizaci systému řízení rizik
- dohled a koordinace činností, souvisejících se zajištěním kybernetické bezpečnosti na pracovištích ÚMČ Praha 5
- definuje bezpečnostní požadavky IS používaných na pracovištích ÚMČ Praha 5
- definuje bezpečnostní požadavky při pořízení nových IS pro pracoviště ÚMČ Praha 5

- koordinuje činnosti související s penetračním testováním
- koordinuje vyhodnocování a klasifikaci kybernetických bezpečnostních incidentů a jejich zvládnání
- odpovídá za zajištění odstranění nedostatků zjištěných při kontrolách NÚKIB
- navrhuje a koordinuje úpravy bezpečnostní dokumentace na základě zjištění z auditů kybernetické bezpečnosti
- vyhodnocuje účinnost systému řízení bezpečnosti informací a jejich prováděných nebo plánovaných změn
- navrhuje bezpečnostní opatření a koordinuje jejich implementaci a dodržování
- posuzuje výstupy z penetračních testů
- definuje požadavky na kybernetickou bezpečnost při pořízení nových IS pro pracoviště ÚMČ Praha 5
- definuje požadavky na kybernetickou bezpečnost u IS používaných na pracovištích ÚMČ Praha 5
- dohlíží na platnost exit strategií u smluvní vztahů na provozované IS na pracovištích ÚMČ Praha 5

Pracovní den manažera kybernetické bezpečnosti (MKB)

S ohledem na omezení, plynoucí z DPČ (10 hodin měsíčně) nelze vytvořit snímek pracovního dne jako takového. V souvislosti se zmíněným omezením je role MKB většinou zaměřena na metodickou a konzultační činnost.

Typicky zahrnuje:

- administrativní záležitosti (vyřizování e-mailů a podobně)
- operativní řešení ad-hoc požadavků
- metodickou činnost
- ústní i on-line konzultace k problematice kybernetické a informační bezpečnosti
- sledování informací zveřejňovaných Národním úřadem pro kybernetickou a informační bezpečnost – např. varování o zranitelnostech technologií, používaných v ÚMČ P5 a jejich řešení ve spolupráci s Odborem informatiky
- sledování legislativního procesu v souvislosti s evropskou směrnicí NIS2
- účast na jednáních s externími odborníky
- analýzy reportů z bezpečnostních technologií
- šíření osvěty mezi zaměstnanci
- tvorba a rozesílání varování zaměstnancům ÚMČ P5 v případě, že probíhá nějaká škodlivá kampaň, která by je mohla ohrozit (např. Phishingové kampaně)
- připomínkování dokumentů
- sledování trendů v oblasti kybernetické a informační bezpečnosti v mezinárodním prostředí
- příprava a realizace školení zaměstnanců v oblasti kybernetické bezpečnosti
- trvalá dostupnost pro řešení naléhavých i nenaléhavých záležitostí - mobilní telefon resp. on-line komunikace (MS-Teams apod.).

Podle § 5 odst. 3 InfZ bude informace také do 15 dnů od poskytnutí zveřejněna způsobem umožňujícím dálkový přístup na webových stránkách MČ Praha 5:

<https://www.praha5.cz/povinne-zverejnovane-informace/archiv-poskytnutych-informaci-podle-zakona-c-106-1999-sb/>

JUDr. Kateřina Černá
tajemnice ÚMČ Praha 5