I. PREDMET ŽIADOSTI

„Vzhľadom na to, že v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov má prevádzkovateľ základnej služby povinnosť prijať bezpečnostné opatrenia podľa § 20, dovoľujem si Vás požiadať o stanovisko k otázke určenia manažéra kybernetickej bezpečnosti podľa § 5 písm. a) vyhlášky č. 362/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení:

1. *Aké má mať manažér postavenie v rámci orgánu štátnej správy?*
2. *Má byť štátnym zamestnancom/vykonávať prácu vo verejnom záujme v rámci orgánu štátnej správy alebo môže ísť o externú osobu? Je prípadne možné uzavrieť s manažérom kybernetickej bezpečnosti dohodu podľa IX. časti Zákonníka práce?*
3. *Aké sú požiadavky na odborné a iné znalosti manažéra kybernetickej bezpečnosti podľa § 5 písm. a) bod 4? Na aký osobitný predpis tento bod odkazuje?“*

II. APLIKOVANÉ PRÁVNE PREDPISY

Podľa § 20 ods. 3 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej iba ako „zákon“) bezpečnostné opatrenia sa prijímajú pre oblasť organizácie informačnej bezpečnosti.

Podľa § 5 písm. a) vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“) na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej zásada

a) určenia manažéra kybernetickej bezpečnosti, ktorý
    1. má možnosť predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby,
    2. zabezpečuje aplikáciu bezpečnostných opatrení v systéme riadenia kybernetickej bezpečnosti,
    3. je nezávislí od riadenia prevádzky a vývoja služieb informačných technológií a
    4. spĺňa znalostné štandardy na funkciu manažéra kybernetickej bezpečnosti podľa osobitného predpisu

III. METODICKÉ USMERNENIE

K otázke č. 1 uvádzame, že manažérom kybernetickej bezpečnosti je osoba s preukázanou odbornou spôsobilosťou, ktorej bezpečnostnou úlohou je zodpovednosť za organizovanie systému riadenia kybernetickej bezpečnosti. Zákon a ani vyhláška č. 362/2018 Z. z. explicitne neupravuje postavenie manažéra kybernetickej bezpečnosti v rámci orgánu štátnej správy. Osoba manažéra kybernetickej bezpečnosti je však spájaná s jeho zodpovednosťou voči štatutárnemu orgánu prevádzkovateľa základnej služby. Manažér kybernetickej bezpečnosti, z povahy výkonu svojich úloh, by mal byť osobou s dostatočnou znalosťou vnútorných procesov prevádzkovateľa základnej služby.

K otázke č. 2 uvádzame, že zákon a ani vyhláška č. 362/2018 Z. z. neustanovuje, či má manažér kybernetickej bezpečnosti byť štátnym zamestnancom alebo vykonávať prácu vo verejnom záujme, alebo či môže ísť o externého pracovníka.

Manažér kybernetickej bezpečnosti je však jedným zo základných nástrojov tvorby bezpečnostných opatrení prevádzkovateľa základnej služby a ich aplikácie. Manažér

kybernetickej bezpečnosti je profesionálny riadiaci prvok kybernetickej bezpečnosti prevádzkovateľa základnej služby, ktorý pre efektívnej riadenie potrebuje poznať vnútorné prostredie organizácie a aktíva prevádzkovateľa základnej služby. V uvedenom kontexte je preto možné odporučiť, aby osoba manažéra kybernetickej bezpečnosti, vzhľadom na vysokú mieru požadovanej zodpovednosti a dôvernosti, bola interným zamestnancom prevádzkovateľa základnej služby.

K otázke č. 3 uvádzame, že všeobecne záväzný právny predpis, ktorým úrad ustanoví bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti (§ 32 ods. 1 písm. d) zákona), je v súčasnosti v štádiu prípravy a bude zverejnený na portály Slov-lex.

IV. POUČENIE

Na záver upozorňujeme, že tieto odpovede na konkrétne otázky nepredstavujú právne záväzný výklad zákona, ani individuálny správny akt s konštitutívnymi účinkami.