Príloha č.2

**Externý výkon funkcie manažéra kybernetickej bezpečnosti**

**Požiadavky – špecifikácia manažéra KB – aktivity vykonávajúce manažérom KB**

Rola Manažéra kybernetickej bezpečnosti má oporu v § 17d vyhlášky NBÚ č. 362/2018 Z. z., ktorý stanovuje obsah bezpečnostných opatrení pre oblasť podľa § 20 ods. 3 písm. a) zákona.

Manažér kybernetickej bezpečnosti je zodpovedný za predchádzanie kybernetickým bezpečnostným incidentom a minimalizovanie vplyvu kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služieb organizácie.

Manažér kybernetickej bezpečnosti musí spĺňať znalostné štandardy na funkciu Manažéra kybernetickej bezpečnosti a musí byť nezávislý od riadenia prevádzky a vývoja IT služieb.

Profil Manažéra kybernetickej bezpečnosti je zhrnutý v tabuľke nižšie (z neho sú potom vyvodené jeho zodpovednosti a právomoci).´

|  |  |
| --- | --- |
| Oblasť: | Charakteristika: |
| Mandát | Zodpovednosť za operatívne riadenie oblasti kybernetickej bezpečnosti |
| Rozsah činnosti / zodpovednosť | Riadenie oblasti kybernetickej bezpečnosti a jej monitorovanie pre všetky IS v správe organizácie ako poskytovateľa základnej služby |
| Rozhodovacie právomoci | Návrh odporúčaní a konceptov pre implementáciu dostatočných kontrolných mechanizmov a procesov pre oblasť riadenia a monitorovania kybernetickej bezpečnosti |
| Eskalácia / reportovanie | Manažér kybernetickej bezpečnosti reportuje a eskaluje prípadné problémy priamo Bezpečnostnému výboru |

Manažér kybernetickej a informačnej bezpečnosti najmä:

* spolupracuje pri príprave východiskového strategického dokumentu, ktorý určuje prístup k zabezpečovaniu kybernetickej bezpečnosti, t. j. dokumentu „Stratégia kybernetickej bezpečnosti“ a zodpovedá za jej pravidelnú revíziu a aktualizáciu,
* spolupracuje na vyhodnocovaní bezpečnostných cieľov v súlade a v periodicite definovanej dokumentom „Stratégia kybernetickej bezpečnosti“,
* tvorí návrhy politík, smerníc a pravidiel pre oblasť kybernetickej bezpečnosti,
* spolupracuje na príprave rozpočtu pre kybernetickú bezpečnosť,
* spolupracuje pri analýze rizík a pri jej aktualizácii (riziká týkajúce sa kybernetickej bezpečnosti),
* v rámci procesu klasifikácie a evidencie informácii posudzuje odôvodnenia spracovateľov informácií a odsúhlasuje zverejnenie informácií v súlade so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov),
* predkladá návrhy a oznamuje informácie v oblasti kybernetickej bezpečnosti priamo Bezpečnostnému výboru,
* spolupracuje pri implementácii nových technických riešení (IT architektúra, riadenie zmien, riadenie projektov a pod.) z pohľadu vplyvu na oblasť kybernetickej bezpečnosti,
* dohliada na prijímanie, dodržiavanie a preverovanie účinnosti prijatých opatrení v oblasti kybernetickej bezpečnosti,
* spolupracuje pri uzatváraní zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti s externým dodávateľom, ktorý poskytuje služby týkajúce sa vývoja, implementácie a prevádzky IS v správe organizácie,
* vykonáva pravidelné audity kybernetickej bezpečnosti v zmysle legislatívnych alebo interných plánov, prípadne vykonáva mimoriadne audity podľa potreby (napr. v prípade podozrenia na kybernetický bezpečnostný incident),
* zaisťuje, že ak dôjde ku kybernetickým bezpečnostným incidentom alebo narušeniu dôvernosti, integrity alebo dostupnosti informačných aktív, tieto incidenty sa vyriešia pohotovo a účinne budú ohlásené v súlade s platnou legislatívou,
* zaisťuje, že budú prijaté opatrenia minimalizujúce možnosť opakovania kybernetických bezpečnostných incidentov.

Manažér kybernetickej a informačnej bezpečnosti taktiež spolupracuje s inými útvarmi v nasledovných oblastiach:

* vyšetrovanie a forenzné analýzy,
* sociálne a personálne aspekty (napr. tzv. „background checks“),
* IT architektúra (najmä z pohľadu kybernetickej bezpečnosti),
* bezpečnostné nástroje,
* kontroly plnenia bezpečnostných opatrení,
* riadenie prístupových práv,
* riadenie zmien a projektov,
* konfiguračný manažment,
* riadenie rizík v oblasti kybernetickej bezpečnosti, identifikácia možných dopadov relevantných hrozieb a pravdepodobnosti ich uplatnenia,
* analýzy funkčného dopadu,
* riadenie vzťahov s dodávateľmi v kontexte dodržiavania pravidiel kybernetickej bezpečnosti,
* stanovovanie a kontrola dodržiavania pravidiel kybernetickej bezpečnosti zo strany zamestnancov a dodávateľov,
* zvyšovanie povedomia o kybernetickej bezpečnosti a zaškoľovanie/preškoľovanie všetkých zamestnancov a dodávateľov,
* inovácie v oblasti kybernetickej bezpečnosti.

Manažér kybernetickej a informačnej bezpečnosti je ďalej povinný:

* aktívne spolupracovať s Bezpečnostným výborom a plniť úlohy predsedu Bezpečnostného výboru,
* pravidelne reportovať stav a výkonnosť kybernetickej bezpečnosti Bezpečnostnému výboru,
* riadiť riešenie kybernetických bezpečnostných incidentov,
* bezodkladne hlásiť závažný kybernetický bezpečnostný incident prostredníctvom jednotného informačného systému kybernetickej bezpečnosti,
* spolupracovať s Národným bezpečnostným úradom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj vlastné informácie dôležité pre riešenie kybernetického bezpečnostného incidentu,
* v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
* oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka,
* oznámiť a preukázať Národnému bezpečnostnému úradu vykonanie reaktívneho opatrenia a jeho výsledok, v prípade ak bolo prijaté reaktívne opatrenie,
* informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy s treťou stranou stalo nemožným.

Manažér kybernetickej a informačnej bezpečnosti má právo od iných organizačných útvarov žiadať:

* doplňujúce informácie,
* logy,
* akúkoľvek súvisiacu podpornú dokumentáciu,
* umožnenie kontroly dodržiavania prijatých bezpečnostných opatrení kybernetickej bezpečnosti.

Manažér kybernetickej a informačnej bezpečnosti je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií.

**Požiadavky – časový výkon manažéra KB**

* Predpokladaný počet ČH za kalendárny mesiac 56, čo predstavuje 7 pracovných dní v štandardnej dĺžke 8 h pracovného dňa.
* ČH – predstavuje jednu človekohodinu aktívneho výkonu činností manažéra kybernetickej bezpečnosti.
* 56 ČH / mesiac na dobu 24 mesiacov
* **Spolu 1344 ČH**