

STANOVISKO REPUBLIKOVEJ ÚNIE ZAMESTNÁVATEĽOV

Vyhľadávka Národného bezpečnostného úradu, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti

<https://www.slov-lex.sk/legislativne-procesy/SK/LP/2022/323>

Materiál v pripomienkovom konaní do 23.06.2022

Stručný popis podstaty materiálu najmä jeho relevancie z pohľadu RÚZ

Materiál bol predložený do medzirezortného pripomienkového Národným bezpečnostným úradom SR na základe § 32 ods. 1 písm. d) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Cieľom a obsahom materiálu je najmä:

Účelom návrhu vyhlášky je vykonať zákon spôsobom, aby boli určené minimálne odborné znalosti pre jednotlivých používateľov sietí a informačných systémov vykonávajúcich činnosti a úlohy v oblasti kybernetickej bezpečnosti

Návrh vyhlášky má nadobudnúť účinnosť dňa 01.08.2022

Postoj RÚZ k materiálu

Účelom návrhu vyhlášky je vykonať zákon spôsobom, aby boli určené minimálne odborné znalosti pre jednotlivých používateľov sietí a informačných systémov. RÚZ k návrhu predkladá nižšie uvedené pripomienky. Navrhované požiadavky odbornej spôsobilosti sú nastavené príliš striktné a sú spôsobilé zároveň obmedziť prístup inak kvalifikovaným a odborne zdatným zamestnancom k trhu práce v oblasti kybernetickej bezpečnosti/IT bezpečnosti.

Pripomienky RÚZ k predkladanému materiálu

1. Zásadná pripomienka k návrhu ako celku

Navrhujeme všeobecné ustanovenie, ktoré bude počítat so situáciou, že v rámci jednej organizácie/spoločnosti môže byť znalostná požiadavka na určitý typ pozície zdieľaná resp. tvorená viacerými odbornými útvarmi, ktoré vo svojom celku resp. symbióze príslušné znalostné štandardy spĺňajú a nemusí to byť v rámci jednej konkrétnej pozície. Napr. v rámci firmy pracovníci jedného IT security oddelenia sa špecializujú každý špecificky na určité typy hrozieb (takáto špecializácia a diverzifikácia v konečnom dôsledku má ešte lepší efekt ako napĺňanie požiadaviek jedným zamestnancom).

Návrh doplnenia § 2 ods. 4: „(4) Znalostné štandardy pre určitú rolu môžu byť v rámci jednej organizácie spĺňané aj kolektívne, napríklad zdieľaním príslušných znalostí v rámci jedného alebo viacerých útvarov“.

2. Zásadná pripomienka k návrhu ako celku

Jednotlivé požiadavky na znalostné štandardy v oblasti kybernetickej bezpečnosti nie celkom vhodne reagujú na skutočné praktické požiadavky na zabezpečenie kybernetickej bezpečnosti, a to najmä z dôvodu ich formalistickej koncepcie. Príkladom je u konkrétnej pozície (napr. odborný zamestnanec) požiadavka na znalosť všetkých aktuálnych typov hrozieb, kryptografických mechanizmov resp. základov trestného práva. Prax však vyžaduje skôr bezproblémovú orientáciu v príslušných témach, praktické zručnosti, schopnosť chápať súvislosti a ich podstatu, prípadne schopnosť si potrebné informácie zabezpečiť medzi špecializovanými útvarmi alebo v rámci kolektívu. Takto prísne formálne kladené znalostné požiadavky sú spôsobilé zároveň obmedziť prístup inak kvalifikovaným a odborne zdatným zamestnancom k trhu práce v oblasti kybernetickej bezpečnosti/IT bezpečnosti a môžu spôsobiť personálne výpadky príslušným zamestnávateľom čo môže mať v konečnom dôsledku negatívny dopad na dosiahnutie účelu zákona o kybernetickej bezpečnosti.

V tomto zmysle navrhujeme upraviť popis znalostných požiadaviek v rámci rolí: odborný zamestnanec, špecialista kybernetickej bezpečnosti, manažér kybernetickej bezpečnosti, výkon operatívnych činností a architekt kybernetickej

bezpečnosti, špecialista riadenia rizík, tester kybernetickej bezpečnosti, architekt kybernetickej bezpečnosti, špecialista pre riešenie kybernetických incidentov.

Zdroj:

<https://www.slov-lex.sk/legislativne-procesy/SK/LP/2022/323>