V Liptovskom Mikuláši, dňa 25.3.2020

Odporúčania umožňujúce dodržanie princípov verejného obstarávania pri plnení povinností prevádzkovateľa základnej služby v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti.

Mestá obce a VÚC za účelom splnenia povinností prevádzkovateľa základnej služby v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti (ďalej v texte len ako „ZoKB“) budú realizovať kroky, ktoré im umožnia úspešne splniť organizačno - právne opatrenia a technické opatrenia tak, aby boli v stanovenom termíne schopné predložiť kontrolnému orgánu - Národnému bezpečnostnému úradu pozitívny záverečný audit vypracovaný certifikovaným audítorom. Finančné prostriedky, ktoré budú musieť samosprávy vynaložiť na dosiahnutie súladu so ZoKB by mali byť použité účelne a hospodárne, tak aby nebolo možné v budúcnosti spochybniť oprávnenosť nákladov vynaložených na dosiahnutie súladu so ZoKB. Správne zvolený postup by mohol umožniť obciam aj efektívne a hlavne rýchlo reagovať aj na budúce výzvy umožňujúce financovanie opatrení v oblasti kybernetickej bezpečnosti z európskych štrukturálnych a investičných fondov.

Vzhľadom na skutočnosť, že samosprávy sa pri plnení svojich úloh dostávajú do pozície verejného obstarávateľa v zmysle § 7 ods. 1 písm. b) alebo písm. c) zákona č. 343/2015 Z. z. v platnom znení o verejnom obstarávaní (ďalej v texte len ako „ZVO“) je nevyhnutne potrebné, aby pri obstarávaní služieb a tovarov postupovali účelne a efektívne a dodržiavali základné princípy verejného obstarávania. Zároveň si pri verejnom obstarávaní povinní postupovať aj v zmysle príslušných ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe (ďalej v texte len ako „zákon o ITVS“) a to najmä v súvislosti s povinnosťami upravenými v § 15 zákona o ITVS. S ohľadom na vyššie uvedené odporúčame realizáciu nasledujúcich na seba nadväzujúcich krokov:

Krok I. GAP (rozdielová) analýza
Posúdenie súladu aktuálneho stavu spoločnosti z pohľadu ZoKB a vykonávacích vyhlášok. V prípade ak sa spoločnosť rozhodne vykonať GAP analýzu prostredníctvom externého dodávateľa odporúčame aby bez ohľadu na zvolený postup obstarávania samosprávy vyžadovali od externého dodávateľa aby preukázal, že disponuje vo svojom tíme osobou ktorá je certifikovaný Lead audítor na ISO 27 000 a že vie preukázať aspoň 2 pozitívne referencie na už ním doteraz vykonané GAP analýzy. Posúdenie súladu sa týka oblastí: právnej, organizačnej, procesnej a technickej. Výsledkom GAP analýzy sú odporúčania na vykonanie nápravných opatrení, ktorých následná realizácia zabezpečí súlad samosprávy so ZoKB a teda aj pozitívny výsledok záverečného auditu.

Krok II. Štúdia realizovateľnosti
Návrh optimálnej architektúry riešenia technických opatrení a s tým spojený návrh alternatívnych ekonomických postupov ako dosiahnuť implementáciu návrhu architektonického riešenia. Štúdia realizovateľnosti pritom vychádza z výstupov (odporúčaní, nápravných opatrení) z kroku I.. Veľkým prínosom štúdie realizovateľnosti je okrem kvalifikovaného podkladu na rozhodnutie vedenia samosprávy o ďalšom ekonomickom postupe pri dosahovaní súladu so ZoKB aj stanovenie kvalifikovaného odhadu výšky nákladov potrebných na realizáciu alternatívnych ekonomických postupov. Štúdia realizovateľnosti sa tak zároveň stáva aj odborným podkladom do verejného obstarávania na určenie správnej výšky predpokladanej hodnoty zákazky. Vykonaním štúdie realizovateľnosti sa tak samospráva do budúcna vyhne v následnom procese verejného obstarávania aj prípadným námietkam neúspešných uchádzačov (napr. mimoriadne nízka ponuka) či kontrolným zisteniam zo strany Úradu pre Verejné obstarávanie (napr. nesprávne stanovená výška PHZ). Obsahom štúdie realizovateľnosti sú interné informácie o aktuálnom i očakávanom stave bezpečnostnej infraštruktúry samosprávy a preto je s ňou potrebné nakladať ako s dôvernými informáciami, ktoré nie sú voľne prístupné verejnosti, ale len vedeniu a vybranému okruhu zamestnancov samosprávy. V prípade ak sa samospráva rozhodne vykonať štúdiu realizovateľnosti prostredníctvom externého dodávateľa odporúčame aby bez ohľadu na zvolený postup obstarávania samosprávy vyžadovali od externého dodávateľa aby preukázal, že je držiteľom ISMS 27 000, že disponuje vo svojom tíme osobou ktorá je Solution architektom informačnej bezpečnosti

Cluster Kybernetickej Bezpečnosti
so sídlom: Nábrežie Janka Kráľa 967/14, 031 01 Liptovský Mikuláš, Slovenská republika
bankové spojenie: ČSOB, a.s., IBAN: SK SK58 7500 0000 0040 2603 7061,
e - mail: info@clusterkb.sk; gsm: + 421 907 136 800, IČO // ID number: 51 749 416

certifikovaným na SIEM riešenia a sieťovú bezpečnosť (NTA/NBA) a ktorá vie zároveň preukázať aspoň 1 pozitívnu referenciu na už ňou doteraz vykonanú štúdiu realizovateľnosti.

Krok III. realizácia technických opatrení

Na základe rozhodnutia vedenia samosprávy sa spustí proces verejného obstarávania, ktorého cieľom bude realizácia navrhnutej architektúry riešenia (v zmysle kroku II) na základe zvoleného pre samosprávu najvhodnejšieho ekonomického potupu (nákup tovaru, obstaranie služby, či mix tovarov a služieb). Bez ohľadu na to či pôjde o podlimitnú alebo nadlimitnú zákazku, verejné obstarávanie odporúčame realizovať formou užšej súťaže podľa § 92 a nasl. ZVO a to tak, že najprv prihlásení uchádzači preukážu svoje ekonomické postavenie a odbornú spôsobilosť na úspešné zrealizovanie predmetu zákazky (podmienky účasti) a následne uchádzači, ktorí splnili kvalifikačné kritériá uzavrú so spoločnosťou dohodu o mlčanlivosti. Po jej podpise im spoločnosť sprístupní štúdiu realizovateľnosti, na základe obsahu ktorej uchádzači predložia svoje ekonomické ponuky. Kritériom úspechu v tomto štádiu užšej súťaže pritom bude ekonomicky najvýhodnejšia ponuka - najnižšia cena. Výsledkom takto zvoleného postupu bude úspešné verejné obstarávanie, na základe ktorého zákazku zrealizuje za ekonomicky preukázateľne výhodných podmienok kvalifikovaný zmluvný partner disponujúci dostatočnými skúsenosťami a tímom odborníkov, čo je základným predpokladom pre dosiahnutie súladu so ZoKB pri plnení technických opatrení.

V prípade potreby doplňujúcich informácií prosím neváhajte kontaktovať zástupcov členov Clustra Kybernetickej Bezpečnosti:

Milan Brach, hbr advokáti s.r.o., milan.brach@hbra.sk +421 903 417 862
(právne otázky a otázky k verejnému obstarávaniu)

Ján Lichvár, AXENTA s.r.o., lichvar@axenta.sk +421 907 136 800
(technické otázky)