**PREDKLADACIA SPRÁVA**

Národný bezpečnostný úrad, ako ústredný organ štátnej správy pre kybernetickú bezpečnosť, pripravil na základe schváleného programového vyhlásenia vlády Slovenskej republiky na roky 2016-2020 a v súlade so schválenou Koncepciou kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 a Akčným plánom realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 návrh zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“), ktorým do národného právneho poriadku transponuje smernicu Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“).

Smernica NIS predstavuje prvú celoeurópsku legislatívnu úpravu v oblasti kybernetickej bezpečnosti, ktorá sa zameriava na posilnenie právomocí príslušných vnútroštátnych orgánov, zvyšuje ich vzájomnú koordináciu a predstavuje bezpečnostné podmienky pre kľúčové sektory.

Smernica NIS najmä:

* zavádza bezpečnostní požiadavky a požiadavky na hlásenie kybernetických bezpečnostných incidentov pre prevádzkovateľa základných služieb a pre poskytovateľa digitálnych služieb,
* ukladá členským státom povinnosť určiť vnútroštátne príslušné orgány, jednotné kontaktné miesta a bezpečnostné tímy jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“),
* ukladá členským štátom povinnosť prijať národnú stratégiu kybernetickej bezpečnosti,
* ustanovuje skupinu pre spoluprácu, za účelom podpory strategickej spolupráce a výmeny informácii medzi členskými štátmi a budovania vzájomnej dôvery,
* stavuje sieť jednotiek CSIRT, ktorej účelom je prispievať k budovaniu dôvery medzi členskými štátmi a podporovať účinnú spoluprácu.

Cieľom návrhu zákona je vytvoriť funkčný legislatívny rámec nutný pre efektívnu realizáciu kľúčových opatrení pre bezpečnosť národného kybernetického priestoru, ktorý transponuje priority a požiadavky, ktoré boli vytvorené na európskej úrovni a prijaté všeobecným konsenzom prostredníctvom smernice NIS.

Príprave návrhu zákona predchádzala široká odborná diskusia. Národný bezpečnostný úrad v rámci príprav organizoval celonárodné workshopy a stretnutia na tému transpozície smernice NIS do národného právneho poriadku a predsedal Stredourópskej platforme pre kybernetickú bezpečnosť. Návrh zákona bol vypracovaný aj na základe podnetov a po konzultáciách s orgánmi verejnej moci, ktoré sa k navrhovaným zmenám a oblastiam úprav vyjadrili formou pripomienok, ako aj na základe podnetov a diskusií so zástupcami odbornej verejnosti.

Medzi hlavné oblasti úpravy návrhu zákona patrí oblasť

* organizácie a pôsobnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
* národnej stratégie kybernetickej bezpečnosti,
* jednotného informačného systému kybernetickej bezpečnosti,
* postavenia a povinnosti prevádzkovateľa základných služieb a poskytovateľa digitálnych služieb,
* organizácie a pôsobnosť jednotiek CSIRT,
* systému zabezpečenia kybernetickej bezpečnosti a minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti,
* vzdelávania budovania bezpečnostného povedomia a
* kontroly a auditu.

Okrem uvedených okruhov návrh zákona rieši aj niektoré ďalšie požiadavky smernice NIS, ako je napríklad plnenie notifikačných povinností, nahlasovanie kybernetických bezpečnostných incidentov ako aj dobrovoľné nahlasovanie kybernetických bezpečnostných incidentov a svojimi ustanoveniami podporuje výskum a vzdelávanie, ako aj zvyšovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti.

Návrh zákona v jednotlivých článkoch novelizuje právne predpisy, ktorých zmena je z dôvodu dostatočnej transpozície nevyhnutná.

Návrh zákona komplexným spôsobom poníma problematiku riešenia a zabezpečovania kybernetickej bezpečnosti. Vytvára konkurenčné prostredie v oblasti zamestnávania kvalifikovaných pracovníkov na strane štátu, sústreďuje oznamovanie bezpečnostných incidentov v jednom informačno-komunikačnom bode a štandardizuje bezpečnostné požiadavky v celoslovenskom meradle v súlade s medzinárodnými štandardmi, čím prispieva v harmonizácii problematiky zabezpečovania kybernetickej bezpečnosti v európskom prostredí.

Návrh zákona v nevyhnutne potrebnej miere vypĺňa právnu medzeru v súvislosti s kybernetickou obranou novelizovaním príslušných zákonov na úseku zabezpečenia obrany štátu v predpokladaných situáciách. Kybernetická bezpečnosť obsiahnutá v navrhovanom zákone o kybernetickej bezpečnosti a navrhovaná úprava kybernetickej obrany tak vytvorí efektívny rámec pre preventívne a aj reaktívne opatrenia.

Vzhľadom na predpokladanú dĺžku legislatívneho procesu a berúc do úvahy potrebnú legisvakanciu sa navrhuje, aby zákon nadobudol účinnosť 1. marca 2018. Ustanovenia, ktoré zakladajú povinnosti, vyžadujúce si prípravu a implementáciu sa navrhujú ustanoviť s odloženou účinnosťou.

Návrh zákona je v súlade s Ústavou Slovenskej republiky, ústavnými zákonmi, nálezmi Ústavného súdu Slovenskej republiky, so zákonmi, ako aj s medzinárodnými zmluvami, ktorými je Slovenská republika viazaná a s predpismi Európskej únie.

Návrh zákona nie je predmetom vnútrokomunitárneho pripomienkového konania.

Prijatie navrhovaného zákona nemá sociálne vplyvy, ani vplyvy na životné prostredie ani na služby verejnej správy pre občana, bude mať pozitívne vplyvy na informatizáciu spoločnosti, avšak bude mať negatívne vplyvy na podnikateľské prostredie a na rozpočet verejnej správy.