**Dôvodová správa**

1. **Všeobecná časť**

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“).

Siete a informačné systémy hrajú zásadnú úlohu pri slobodnom pohybe a často sú prepojované a spájané internetom, ako globálnym nástrojom. Narušenie siete a informačných systémov v jednom členskom štáte sa preto dotýka ďalších členských štátov a celej Európskej únie. Odolnosť sietí a stabilita informačného systému je preto základným predpokladom hladkého a nerušeného fungovania vnútorného trhu Európskej únie a predpokladom dôveryhodnej medzinárodnej spolupráce.

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.

Cieľom smernice NIS je zaručiť spoločnú bezpečnosť sietí a informačných systém v rámci Európskej únie, prostredníctvom zvýšenia bezpečnosti internetu a súkromných sietí a informačných systémov, na ktorých je do značnej miery postavené fungovanie hospodárskych a spoločenských záujmov.

Významným subjektom na poli kybernetickej bezpečnosti v Európskej únii je Európska agentúra pre bezpečnosť sietí a informácií (ENISA), ktorá prispieva k zabezpečovaniu vysokého stupňa bezpečnosti a v spolupráci s európskymi krajinami vytvára spoločnú kultúru bezpečností sietí a informačných systémov v Európskej únii.

Povinnosti členských štátov vyplývajúce zo smernice NIS sú nastavené na najnižšej prijateľnej úrovni nevyhnutnej k dosiahnutiu požadovanej pripravenosti a k zabezpečeniu medzištátnej spolupráce založenej na dôvere. Členské štáty môžu v rámci prijatých opatrení zohľadňovať svoje vnútroštátne špecifiká a každý členský štát v tomto smere transponuje smernicu NIS s ohľadom na reálne, skutočné riziká vyskytujúce sa v spoločnosti.

Smernica NIS najmä:

* zavádza bezpečnostné požiadavky a požiadavky na hlásenie kybernetických bezpečnostných incidentov pre prevádzkovateľa základných služieb (ďalej len „PZS“) a pre poskytovateľa digitálnych služieb (ďalej len „PDS“),
* 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, s cieľom podporovať strategickú spoluprácu a výmenu informácii medzi členskými štátmi a budovať vzájomnú dôveru,
* stanovuje sieť jednotiek CSIRT, ktorej účelom je prispievať k budovaniu dôvery medzi členskými štátmi a podporovať účinnú spoluprácu.

Nasledovná tabuľka uvádza konkrétne hlavné úlohy vyplývajúce zo smernice NIS a ich transponovanie do návrhu zákona:

|  |  |  |
| --- | --- | --- |
| **Úloha vyplývajúca zo smernice NIS** | **Transponovaná** | **Kde v návrhu zákona** |
| Vypracovať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov (čl. 7) | áno | § 7 |
| Definovať aspoň jeden zodpovedný orgán (čl. 8 ods. 1) | áno | § 5 ods. 1 písm. a) |
| Definovať kontaktné miesto (čl. 8 ods. 3) | áno | § 5 ods. 1 písm. e) |
| Vytvoriť aspoň jednu jednotku CSIRT (čl. 9 ods. 1) | áno | § 6, 11 a 13  |
| Identifikovať PZS (čl. 5) | áno | § 17 |
| Nahlasovať kybernetické bezpečnostné incidenty (čl. 14)  | áno | § 24, 25 a 26 |
| Zabezpečiť členstvo v skupine pre spoluprácu a v skupine jednotiek CSIRT (čl. 11, čl. 12) | áno | § 5 písm. g) |

Hlavným legislatívnym východiskom návrhu zákona je Stratégia pre informačnú bezpečnosť v Slovenskej republike (Uznesenie vlády SR č. 270/2008), Legislatívny zámer zákona o informačnej bezpečnosti (Uznesenie vlády SR č. 136/2010) a Uznesenie vlády SR č. 328/2015 ku Koncepcii kybernetickej bezpečnosti.

V nadväznosti na Legislatívny zámer návrhu zákona o informačnej bezpečnosti, v ktorom boli stanovené okrem čiastkových cieľov dva základné okruhy problémov, a to zaistenie ochrany pre informačné systémy verejnej správy a vytvorenie všeobecného právneho rámca pre ochranu celého digitálneho priestoru Slovenskej republiky, je aj v súlade s naplnenými cieľmi smernice NIS možné konštatovať, že návrh zákona o kybernetickej bezpečnosti komplexne a vyčerpávajúcim spôsobom rieši všetky relevantné otázky.

Príprave návrhu zákona predchádzala široká odborná diskusia. Národný bezpečnostný úrad v rámci príprav organizoval workshopy na tému transpozície smernice NIS do národného právneho poriadku, prebiehali konzultácie s akademickou obcou aj odbornou verejnosťou, boli zriadené príslušné pracovné skupiny. Zákon bol teda vypracovaný aj na základe podnetov a po konzultáciách s orgánmi verejnej moci, ktoré sa k navrhovaným zmenám a oblastiam úprav vyjadrili, ako aj na základe podnetov a diskusií so zástupcami odbornej verejnosti.

Cieľom návrhu zákona je vytvoriť funkčný legislatívny rámec nevyhnutný 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.

Medzi hlavné oblasti úpravy návrhu zákona v nadväznosti na smernicu NIS patrí oblasť

* organizácie a pôsobnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
* národnej stratégie kybernetickej bezpečnosti,
* jednotného informačného systému kybernetickej bezpečnosti,
* postavenia a povinnosti PZS a PDS,
* organizáciu a pôsobnosť jednotiek CSIRT a ich akreditáciu,
* systému zabezpečenia kybernetickej bezpečnosti a minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti,
* kontroly a auditu.

Okrem uvedených okruhov návrh zákona rieši aj niektoré ďalšie požiadavky smernice NIS, ako je napríklad vymedzenie medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti, plnenie notifikačných povinností, nahlasovanie kybernetických bezpečnostných incidentov ako aj dobrovoľné nahlasovanie kybernetických bezpečnostných incidentov, 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. Ide najmä o zákon č. 45/2011  Z. z. o kritickej infraštruktúre, zákon č. 351/2011  Z. z. o elektronických komunikáciách v znení neskorších predpisov a zákon č. 319/2002  Z. z. o obrane Slovenskej republiky v znení neskorších predpisov a zákon č. 321/2002  Z. z. o ozbrojených silách Slovenskej republiky v znení neskorších predpisov. Návrh zákona komplexným spôsobom rieši odmeňovanie zamestnancov na strane štátu tak, aby bol štát schopný zamestnať odborníkov v oblasti kybernetickej bezpečnosti a tým konkurovať súkromným zamestnávateľom. V súvislosti so zavedením nového správneho poplatku rovnako dochádza k doplneniu zákona č. 145/1995  Z. z. o správnych poplatkoch v znení neskorších predpisov.

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.

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.