DOI: https://doi.org/10.52651/nmb.c.2024.9788080406738.13-22

15. medzinárodná vedecká konferencia ♦15th International Scientific Conference
Národná a medzinárodná bezpečnosť 2024 ♦ National and International Security 2024
17. – 18. 10. 2024, Liptovský Mikuláš

ANALÝZA AKTUÁLNEHO STAVU LEGISLATÍVY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

ANALYSIS OF THE CURRENT STATE OF CYBER SECURITY LEGISLATION

Roman Bartolomej BOROVSKÝ

ABSTRACT

This paper discusses the evolving landscape of cybersecurity, highlighting its critical importance in today's digital world. As cyber threats grow more sophisticated, the need for robust security measures becomes increasingly vital. The paper examines the implementation of the NIS 2 Directive in the Slovak legal framework, emphasizing the challenges and changes introduced by the new cybersecurity legislation. It explores the role of national regulatory bodies, the importance of harmonized standards across the EU, and the implications for both public and private sectors. The findings suggest that while the legislative updates are necessary, effective implementation will require continuous collaboration and methodological clarity.

Keywords: Cybersecurity, NIS 2 Directive, Slovak Cybersecurity Act, Cyber threats

ÚVOD

Na úvod možno uviesť, že kybernetická bezpečnosť je vysoko dynamická a neustále sa meniaca oblasť. Kybernetické hrozby sa totiž dnes vyvíjajú oveľa rýchlejšie ako kedykoľvek predtým, zdokonaľujú sa a stávajú sa sofistikovanejšími. Hackeri a iní aktéri operujúci v kybernetickom priestore využívajú najnovšie technológie a zraniteľnosti systémov, aby získali neoprávnený prístup k citlivým údajom a cenným informáciám. Organizácie aj jednotlivci preto musia byť neustále ostražití a prispôsobovať a aktualizovať svoje bezpečnostné opatrenia. Inak riskujú vážne následky, ako sú finančné straty, poškodenie mena, reputácie alebo dokonca zlyhanie činnosti. Z toho dôvodu je v dnešnej dobe nevyhnutné venovať kybernetickej bezpečnosti stálu pozornosť a investovať do moderných bezpečnostných riešení. Len tak je možné efektívne a účinne čeliť rastúcim kybernetickým hrozbám (Ivančík, 2020a; Gillis, 2024).

Samotná kybernetická bezpečnosť je komplexná disciplína zameraná na ochranu digitálnych informácií, systémov, sietí, dát a informácií pred neoprávneným prístupom, zmenami, zverejnením, narušením, zničením alebo zneužitím. V dnešnom digitálnom svete, kde sú životy jednotlivcov, ale aj celej spoločnosti čoraz viac prepojené s technológiami, je kybernetická bezpečnosť nevyhnutná pre ochranu osobných údajov, finančných informácií, transakcií, procesov, kritickej infraštruktúry atď. (Aslan, 2023; Saxena, 2024; Kelley, 2024)

Hlavnými cieľmi kybernetickej bezpečnosti sú: zachovanie dôvernosti (ochrana informácií pred neoprávneným prístupom, zabezpečenie integrity (ochrana informácií pred neoprávnenými zmenami, zabezpečenie dostupnosti (zaistenie toho, že autorizovaní používatelia majú k informáciám prístup, keď ho potrebujú) (IBM, 2024; Microsoft, 2024; Kaspersky, 2024).

Kybernetická bezpečnosť v nadväznosti na uvedené zahŕňa širokú škálu techník a postupov, ako sú napríklad: ochrana sietí (firewally, VPN, IDS/IPS systémy), ochrana koncových zariadení (antivírusy, firewally, aktualizácie softvéru), ochrana dát (šifrovanie, zálohovanie), riadenie prístupov (autentifikácia, autorizácia), školenie používateľov (zvyšovanie povedomia o kybernetických hrozbách) atď. (De Groot, 2020; Saxena, 2024; Kelley, 2024)

V súlade s vyššie uvedeným možno kybernetickú bezpečnosť definovať ako *„množinu procesov, osvedčených postupov a technologických riešení, ktoré pomáhajú chrániť kritické systémy a siete pred digitálnymi útokmi“* (Microsoft, 2024). Podľa inej definície *„kybernetická bezpečnosť je prax ochrany počítačov, serverov, mobilných zariadení, elektronických systémov, sietí a údajov pred škodlivými útokmi. Je známa aj ako bezpečnosť informačných technológií alebo bezpečnosť elektronických informácií“* (Kaspersky, 2024). A ďalšia definícia hovorí, že *„kybernetická bezpečnosť je umenie ochrany sietí, zariadení a údajov pred neoprávneným prístupom alebo kriminálnym použitím a praxou zabezpečenia dôvernosti, integrity a dostupnosti informácií“* (CISA, 2024).

Kybernetická bezpečnosť sa v dôsledku rastúcej digitalizácie a závislosti spoločnosti na informačných technológiách stáva čoraz dôležitejšou. Zaoberá sa nielen technickými opatreniami, ale aj procesmi a politikami, ktoré zabezpečujú ochranu dát a informácií. Medzi základné princípy kybernetickej bezpečnosti patrí dôvernosť, integrita a dostupnosť dát, súhrnne označované ako „*CIA triáda*“[1]. Dôvernosť znamená ochranu informácií pred neoprávneným prístupom, integrita zaručuje, že údaje neboli zmenené alebo zničené neoprávnenými osobami, a dostupnosť zabezpečuje, že údaje sú prístupné oprávneným osobám, keď sú potrebné (Fieldmann, 2022; OIS, 2024).

Bezpečnosť (z lat. *sēcūritās*) je jednou z najsilnejšie pociťovaných ľudských potrieb. V psychológii uznávanej Maslowovej teórii hierarchie potrieb patrí bezpečnosti a istote druhé miesto hneď za fyziologickými potrebami. Okrem nich sú v hierarchii začlenené aj spoločenské potreby, potreba úcty a uznania a nakoniec potreba sebarealizácie (Ivančík, 2022).

Zaistenie bezpečnosti v kybernetickom priestore je kritické z viacerých dôvodov. Po prvé, kybernetické útoky môžu mať vážne následky pre národnú bezpečnosť, vrátane ohrozenia kritickej infraštruktúry. Po druhé, finančné straty spôsobené kybernetickými útokmi môžu byť obrovské, a to nielen pre jednotlivé organizácie, ale aj pre ekonomiky ako celok. Po tretie, ochrana osobných údajov a súkromia je základným právom, ktoré je potrebné chrániť pred zneužitím (Andress – Winterfeld, 2011; Ivančík, 2020b; Natalucci a kol., 2024).

Legislatívne normy sa vo všeobecnosti snažia o ochranu legitímnych práv a záujmov fyzických a právnických osôb v kontexte predmetu konkrétneho právneho predpisu. Keďže kybernetický priestor je prostredím, v ktorom dochádza okrem iného aj k sociálnej a ekonomickej interakcii na mikroúrovni (jednotlivci) a makroúrovni (nadnárodné koncerny, štáty), je samozrejmé, že vlády a medzinárodné spoločenstvá musia reagovať na potrebu jeho zabezpečenia.

Legislatíva v oblasti kybernetickej bezpečnosti je navrhnutá tak, aby vytvorila systém na efektívne riadenie a reagovanie na kybernetické hrozby. Tieto opatrenia zahŕňajú zákony a nariadenia, ktoré stanovujú povinnosti pre organizácie týkajúce sa ochrany dát, oznamovania incidentov a zabezpečenia informačných systémov. Medzinárodná spolupráca je taktiež kľúčová, pretože kybernetické hrozby často prekračujú národné hranice a vyžadujú koordinovanú odpoveď. Tento príspevok poskytuje podrobnú analýzu navrhovaných zmien

[1] z angl. Confidentiality, Integrity, Availability

v slovenskej legislatíve a ich implementáciu v kontexte pripomienkového konania a kľúčovej smernice Európskej únie.

IMPLEMENTÁCIA SMERNICE NIS 2 A LEGISLATÍVNY RÁMEC EÚ

Implementácia smernice Európskeho Parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (ďalej ako „NIS 2“) vychádza z právneho základu stanoveného v Zmluve o fungovaní Európskej únie (ZFEÚ)[2], konkrétne z článku 114 ZFEÚ.

V rámci legislatívneho procesu EÚ existujú rôzne typy právnych aktov, z ktorých najvýznamnejšími sú nariadenia a smernice. Nariadenia majú všeobecnú platnosť, sú záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch bez potreby ich implementácie do národného práva. To znamená, že nariadenia sú priamo aplikovateľné a ich ustanovenia sa stávajú súčasťou právneho poriadku každého členského štátu od okamihu ich účinnosti.

Na druhej strane, smernice sú záväzné pre členské štáty, pokiaľ ide o výsledok, ktorý sa má dosiahnuť, ale ponechávajú na jednotlivé štáty voľnosť pri výbere formy a metód implementácie. Členské štáty sú povinné prijať vnútroštátne právne predpisy, ktoré zabezpečia dosiahnutie cieľov stanovených v smernici. To znamená, že smernice nepriamo upravujú národné právo prostredníctvom transpozície, pričom spôsob a detaily implementácie môžu byť v rôznych štátoch odlišné.

Medzi ďalšie právne akty EÚ patria rozhodnutia, ktoré sú záväzné v celom rozsahu, ale len pre tie subjekty, ktorým sú adresované, odporúčania a stanoviská, ktoré nie sú právne záväzné, ale poskytujú smerovanie a odporúčania pre legislatívny a politický postup členských štátov alebo iných inštitúcií EÚ.

Smernica NIS 2 vznikla ako odpoveď na rastúce kybernetické hrozby a potrebu zlepšiť reakcie členských štátov na tieto výzvy. Rýchla digitálna transformácia a narastajúca prepojenosť spoločnosti viedli k zvýšeniu počtu, sofistikovanosti a dopadu kybernetických incidentov, čo si vyžiadalo prispôsobené, koordinované a inovatívne riešenia na úrovni celej EÚ.[3] Napriek pokroku dosiahnutému zavedením smernice NIS 1 (Smernica (EÚ) 2016/1148 zo 6. júla 2016) sa pri jej implementácii odhalili významné nedostatky, ktoré bránili efektívnemu riešeniu nových výziev.[4] Preto bola potrebná revízia a aktualizácia regulačného rámca.

Jedným z hlavných problémov, ktoré smernica NIS 2 rieši, je fragmentácia vnútorného trhu, spôsobená rozdielmi v požiadavkách na kybernetickú bezpečnosť medzi členskými štátmi. Tieto rozdiely viedli k zvýšeným nákladom a komplikáciám pre subjekty pôsobiace v rôznych členských štátoch, čo oslabovalo celkovú odolnosť voči kybernetickým hrozbám v rámci celej Únie[5]. Navyše, rozsah pôsobnosti NIS 1 bol považovaný za zastaraný, keďže nezohľadňoval význam všetkých odvetví a služieb pre fungovanie vnútorného trhu[6].

Smernica NIS 2 prináša niekoľko zásadných zmien a vylepšení v porovnaní s predchádzajúcou legislatívou. Rozširuje svoj rozsah pôsobnosti na väčšiu časť hospodárstva,

[2] Lisabonská zmluva, ktorou sa mení a dopĺňa Zmluva o Európskej únii a Zmluva o založení Európskeho spoločenstva (2007/C 306/01) – Konsolidované znenie
[3] Pozri bližšie: Smernica (EÚ) 2022/2555, Preambula bod 3.
[4] Tamtiež, bod 2
[5] Tamtiež, bod 5
[6] Tamtiež, bod 6

čím zabezpečuje komplexné pokrytie odvetví a služieb, ktoré sú kľúčové pre spoločenské a hospodárske činnosti na vnútornom trhu. Jedným z hlavných prínosov je zavedenie jednotných kritérií pre identifikáciu subjektov, ktoré spadajú do pôsobnosti smernice, čím sa eliminuje možnosť rozdielnych prístupov členských štátov pri identifikácii prevádzkovateľov základných služieb[7].

Ďalšou dôležitou zmenou je rozdelenie subjektov do dvoch kategórií – kľúčové subjekty a dôležité subjekty – na základe ich veľkosti a významu v rámci odvetvia. Tento prístup umožňuje lepšie prispôsobenie požiadaviek a dohľadu nad týmito subjektmi, čím sa zabezpečí spravodlivejšia rovnováha medzi rizikom a administratívnou záťažou.[8] Okrem toho smernica posilňuje mechanizmy dohľadu a presadzovania práva, čo by malo viesť k vyššej úrovni kybernetickej bezpečnosti v celej Únii.

NIS 2 tiež zameriava svoju pozornosť na zlepšenie spolupráce medzi členskými štátmi, s cieľom zabezpečenia rýchlejšej a efektívnejšej reakcie na kybernetické hrozby.[9] Tento koordinovaný prístup je kľúčový pre posilnenie kybernetickej odolnosti v celej Európskej únii a pre efektívne riešenie nových a vznikajúcich výziev v oblasti kybernetickej bezpečnosti.

V závere tejto podkapitoly možno uviesť, že „*táto smernica nebráni členským štátom, aby prijali alebo ponechali v platnosti ustanovenia na zaistenie vyššej úrovne kybernetickej bezpečnosti, ak nie sú takéto ustanovenia v rozpore s povinnosťami členských štátov stanovenými v práve Únii*“ (čl. 5 NIS 2), čím sa uplatňuje prístup minimálnej harmonizácie.

ZÁKON O KYBERNETICKEJ BEZPEČNOSTI A JEHO NOVELIZÁCIA

Národný bezpečnostný úrad Slovenskej republiky, konajúci na základe uznesenia vlády č. 55 zo dňa 1. februára 2024, pripravil novelu zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej aj ako „ZKB“). Tento legislatívny návrh je v súlade so schváleným programovým vyhlásením vlády na roky 2023-2027 a Národnou stratégiou kybernetickej bezpečnosti na roky 2021-2025, vrátane jej akčného plánu. Novela má za úlohu implementovať smernicu NIS 2 do slovenského právneho poriadku. Táto smernica má za cieľ posilniť rámec kybernetickej bezpečnosti v celej EÚ, pričom reaguje na nedostatky predchádzajúcej smernice NIS 1. Z dôvodu dĺžky legislatívneho procesu a potrebnú legisvakanciu by mal zákon nadobudnúť účinnosť od 1. januára 2025. [10]

Navrhované zmeny modernizujú existujúcu legislatívu o kybernetickej bezpečnosti, čím zvyšujú národné štandardy a znižujú riziká spojené s rýchlym technologickým pokrokom. Významnou zmenou je nový prístup k identifikácii prevádzkovateľov základných služieb, ktorý prechádza z kritériami založeného identifikačného mechanizmu na priamu identifikáciu subjektov v zákone. Novela taktiež rozširuje pôsobnosť regulácie na nové subjekty, spresňuje hlásenia incidentov a zdôrazňuje dôležitosť riadenia kybernetických rizík v dodávateľských reťazcoch.

Novela zároveň posilňuje úlohy a zodpovednosti manažérov kybernetickej bezpečnosti a dohliada na zvýšenie dozornej činnosti vrátane zavedenia nástrojov na analýzu rizík pre aplikáciu bezpečnostných opatrení. Zákon zostáva v súlade s Ústavou Slovenskej republiky a ďalšími záväznými právnymi rámcami, pričom zároveň reflektuje potreby aplikačnej praxe. Očakáva sa, že navrhovaný zákon bude mať pozitívne aj negatívne vplyvy na podnikateľské

[7] Tamtiež, bod 7
[8] Tamtiež, bod 15
[9] Tamtiež, bod 39 a nasl.
[10] Pozri bližšie: Dôvodová správa k návrhu novely zákona č. 69/2018 Z. z. LP/2020/400

prostredie, najmä vzhľadom na dodatočné náklady spojené s implementáciou jeho opatrení. Podľa predkladateľa však nebudú mať tieto zmeny výrazný vplyv na sociálne aspekty, životné prostredie, verejné služby ani rozpočty verejnej správy.[11]

Novelizácia zákona 69/2018 Z. z. prináša viaceré kľúčové zmeny a doplnky, ktoré sú nevyhnutné pre transpozíciu smernice NIS 2. Medzi hlavné zmeny patrí zavedenie novej definície „kybernetická hrozba“ v súlade s čl. 6 ods. 10 smernice NIS 2, úprava definície „kritická infraštruktúra“ a rozšírenie okruhu subjektov, ktoré sú považované za prevádzkovateľov základných služieb. Okrem toho novela zavádza nové požiadavky na bezpečnostné opatrenia pre prevádzkovateľov základných a kritických služieb a povinnosť hlásenia kybernetických incidentov v súlade so smernicou NIS 2, ktorá kladie dôraz na včasné varovanie a riešenie incidentov. Taktiež sa zlepšujú mechanizmy kontroly a auditu dodržiavania zákona a zavádzajú sa nové sankcie za nedodržanie požiadaviek zákona, čím sa posilňuje jeho vymáhateľnosť.

MEDZIREZORTNÉ PRIPOMIENKOVÉ KONANIE

Navrhované zmeny v zákone sú vyjadrené prostredníctvom 84 novelizačných bodov, ktoré pokrývajú širokú škálu oblastí od definícií, cez bezpečnostné opatrenia až po sankcie. V rámci medzirezortného pripomienkového konania bolo k návrhu vznesených celkom 695 pripomienok, z ktorých 255 bolo označených za zásadné. Tieto pripomienky reflektujú významné obavy a návrhy na zlepšenie, ktoré by mali byť zohľadnené pri finálnom znení novely.[12]

Jednou z opakujúcich sa pripomienok bola potreba zosúladenia národných definícií s terminológiou používanou v európskych predpisoch. Napríklad definícia „kybernetická hrozba“ bola kritizovaná za duplicitnosť a navrhovalo sa, aby odkazovala priamo na nariadenie (EÚ) 2019/881[13] bez potreby detailného vymedzenia v národnom zákone. Tento prístup by pomohol predísť nejasnostiam a zabezpečil by konzistentnosť s európskou legislatívou.

Pripomienky tiež poukázali na potrebu detailnejšej špecifikácie bezpečnostných opatrení a procesu hlásenia incidentov. Napríklad bolo navrhnuté doplnenie nástroja na hodnotenie účinnosti bezpečnostných opatrení do § 8 ods. 2 ZKB, čo je v súlade s požiadavkami smernice NIS 2 na neustále zlepšovanie a monitorovanie kybernetickej bezpečnosti. Novela reflektuje aj pripomienky týkajúce sa potreby zlepšenia jej aplikácie a zavedenia účinných sankcií za porušenie zákona, pričom navrhuje úpravy v § 10a ods. 1 na zahrnutie porušenia povinnosti mlčanlivosti alebo tajomstva podľa osobitného predpisu.

Štatistika pripomienok ukázala, že najaktívnejšími prispievateľmi boli Odbor aproximácie práva sekcie vládnej legislatívy Úradu vlády SR (OAPSVLÚVSR) so 127 pripomienkami (avšak bez zásadných pripomienok), Republiková únia zamestnávateľov (RÚZSR) so 121 pripomienkami (z toho 117 zásadných) a Ministerstvo pôdohospodárstva a rozvoja vidieka SR (MPRVS) so 70 pripomienkami (z toho 5 zásadných). Tieto subjekty sa zameriavali najmä na otázky administratívnej záťaže, nejasností v zákonných definíciách a praktickej aplikovateľnosti navrhovaných zmien.

---

[11] S týmto tvrdením dôvodovej správy nesúhlasíme, nakoľko aj subjekty verejnej správy budú spadať pod účinnosť zákona 69/2018 z. Z. a tým pádom budú musieť vynaložiť dodatočné prostriedky na nové opatrenia. – pozn. autora

[12] Pozri bližšie: LP/2020/400 Zákon, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a ktorým sa menia a dopĺňajú niektoré zákony

[13] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA

Najviac pripomienok sa sústredilo na ustanovenia týkajúce sa povinností prevádzkovateľov základných služieb (§ 17 ZKB), kde sa riešili nejasnosti ohľadom lehôt na splnenie povinností, duplicita povinností a požiadavky na oznamovanie kontinuity služieb. Ďalšie časti zákona, ktoré pritiahli značnú pozornosť, zahŕňali bezpečnostné opatrenia (§ 20), kde sa diskutovalo o poradí a rozsahu týchto opatrení, požiadavkách na certifikované produkty a služby, ako aj o nezávislosti manažérov kybernetickej bezpečnosti. Okrem toho sa výrazne riešilo aj hlásenie kybernetických bezpečnostných incidentov (§ 24), konkrétne rozsah hlásení, definície „rozsiahleho“ a „závažného“ bezpečnostného incidentu a primeranosť prijatých opatrení.

Pripomienkový proces odhalil niekoľko kritických bodov, ktoré je potrebné zvážiť pred prijatím konečnej verzie zákona. Subjekty opakovane poukazovali na potrebu zníženia administratívnej záťaže a zabezpečenia právnej istoty, čo by malo byť prioritou v ďalšom legislatívnom procese. Navrhovaná novela prináša mnoho zmien, ktoré si vyžadujú jasné metodologické usmernenia, aby sa predišlo nejasnostiam a zbytočným komplikáciám v aplikačnej praxi.

V závere podkapitoly je dôležité zdôrazniť, že medzirezortné pripomienkové konanie je kľúčovým nástrojom pre zlepšenie kvality legislatívnych návrhov, pričom umožňuje dotknutým subjektom aktívne sa zapojiť do tvorby zákonov. Tento proces, spolu s adekvátnym zohľadnením pripomienok, môže výrazne prispieť k efektívnejšiemu a praktickejšiemu legislatívnemu rámcu, ktorý nielenže zlepší národnú kybernetickú bezpečnosť, ale aj zabezpečí súlad s európskymi normami a požiadavkami.

IMPLEMENTAČNÉ VÝZVY NOVELY ZÁKONA

Implementácia smernice NIS 2 do navrhovanej novely zákona o kybernetickej bezpečnosti obsahuje viacero oblastí, kde dochádza k nesúladu alebo k nedostatočnej implementácii požiadaviek smernice. Tieto rozdiely môžu mať významné dôsledky pre efektívnosť zákona a jeho praktickú aplikáciu v oblasti kybernetickej bezpečnosti.

Jedným z najvýraznejších rozdielov medzi smernicou NIS 2 a navrhovanou novelou zákona je terminológia. Smernica NIS 2 zavádza nové kategórie subjektov, konkrétne „kľúčové subjekty“ (*essential entities*) a „dôležité subjekty“ (*important entities*), ktoré sú rozdelené na základe ich veľkosti, významu a potenciálneho vplyvu na spoločnosť a ekonomiku. Tento nový klasifikačný systém je uvedený v článku 3 smernice. Na druhej strane, novela slovenského zákona stále používa pojem „prevádzkovatelia základných služieb“ (§ 3 bod 2 novely zákona), čo nezohľadňuje nové kategórie subjektov definované v NIS 2, ale zotrváva pri staršej terminológii NIS 1. Tento rozdiel môže viesť k obmedzenému rozsahu pôsobnosti zákona a vynechaniu niektorých subjektov, ktoré by mali byť regulované podľa NIS 2 ako kľúčové alebo dôležité subjekty.

Smernica NIS 2 kladie veľký dôraz na spoluprácu a zodpovednosti členských štátov, vrátane povinností týkajúcich sa medzinárodnej spolupráce a výmeny informácií, čo podrobne rozoberá v samostatnej III. kapitole. V navrhovanej novelizácii zákona je však táto téma rozdelená medzi viaceré časti. Aj keď novela spomína pôsobnosť národnej jednotky CSIRT v § 6 a pôsobnosť NBÚ v § 9, nie je jasné, či budú splnené všetky potrebné predpoklady na vykonávanie úloh a povinností stanovených smernicou NIS 2. Nedostatočné implementovanie týchto požiadaviek by mohlo oslabiť efektívnosť medzinárodnej spolupráce a reakcie na cezhraničné kybernetické hrozby.

Článok 36 smernice NIS 2 ponecháva na členské štáty stanovenie pravidiel, pokiaľ ide o sankcie za porušenie vnútroštátnych ustanovení prijatých na základe tejto smernice. V tomto

kontexte novela zákona zavádza rozsiahly postup na uplatňovanie nápravných opatrení a sankcií, pričom dohľad nad ich dodržiavaním zabezpečuje Národný bezpečnostný úrad. NBÚ má kompetencie na ukladanie sankcií a prijímanie predbežných opatrení, čo posilňuje vynútiteľnosť pravidiel. Avšak efektivita týchto opatrení bude závisieť na praktickej realizácii dohľadu a dostupnosti zdrojov a kapacít na jeho vykonávanie. Ďalším dôležitým aspektom je jasnosť a prehľadnosť právneho rámca pre subjekty, ktoré sú povinné zákon dodržiavať. Aj keď je právny rámec pre sankcie a nápravné opatrenia v novele detailne rozpracovaný, je kľúčové, aby bol pre dotknuté subjekty zrozumiteľný a jednoducho aplikovateľný. Ak by boli postupy príliš komplikované alebo nejasné, mohlo by to viesť k problémom s dodržiavaním zákona a tým oslabiť jeho účinnosť v praxi.

NIS 2 zároveň výslovne zdôrazňuje potrebu osobitnej podpory a ochrany pre mikropodniky, malé a stredné podniky (MSP), ktoré sú obzvlášť zraniteľné voči kybernetickým rizikám.[14] V navrhovanej novele zákona však chýbajú jasné a konkrétne ustanovenia, ktoré by priamo riešili špecifické potreby a ochranu týchto podnikov. Hoci novela obsahuje všeobecné opatrenia na ochranu subjektov, osobitná pozornosť pre MSP, ako to vyžaduje smernica, v nej nie je dostatočne rozpracovaná, čo môže viesť k nedostatočnej implementácii smernice a tým sťažiť zlepšenie kybernetickej bezpečnosti týchto subjektov.

Na základe uvedených zistení by mala novela zákona prehodnotiť niektoré svoje ustanovenia, aby zabezpečila plnú harmonizáciu s požiadavkami smernice NIS 2. Implementácia smernice do navrhovanej novely vykazuje viaceré nedostatky, ktoré môžu ovplyvniť efektívnosť zákona a jeho praktickú aplikáciu v oblasti kybernetickej bezpečnosti. Je potrebné zvážiť doplnenie pojmov "kľúčové subjekty" a "dôležité subjekty", ktoré reflektujú nové kategórie subjektov zavedené smernicou, presnejšie určiť lehoty na hlásenie incidentov, a posilniť právomoci národnej jednotky CSIRT na zaistenie efektívnej medzinárodnej spolupráce. Rovnako je dôležité zabezpečiť jasné a konkrétne ustanovenia, ktoré by riešili špecifické potreby mikropodnikov, malých a stredných podnikov, aby sa predišlo oslabeniu ich kybernetickej bezpečnosti. Tieto zmeny by prispeli k vytvoreniu robustnejšieho a efektívnejšieho právneho rámca, ktorý by lepšie odrážal súčasné potreby v oblasti kybernetickej bezpečnosti a zabezpečil vysokú úroveň ochrany pre všetky relevantné subjekty.

REGULAČNÉ ORGÁNY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Národný bezpečnostný úrad (NBÚ) hrá kľúčovú úlohu v oblasti kybernetickej bezpečnosti na Slovensku. Tento úrad je centrálnou autoritou pre kybernetickú bezpečnosť a zodpovedá za riadenie, koordináciu a kontrolu činností spojených s ochranou kybernetického priestoru. Jeho kompetencie sú definované zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý stanovuje základné povinnosti pre subjekty pôsobiace v kritických sektoroch. NBÚ určuje bezpečnostné štandardy, vydáva metodické pokyny a usmernenia, ktoré sú záväzné pre všetky zainteresované strany. Navyše, slúži ako kontaktné miesto pre kybernetickú bezpečnosť na národnej úrovni a zaisťuje koordináciu s inými členskými štátmi EÚ a s organizáciami ako NATO.

Efektívna kybernetická bezpečnosť si vyžaduje úzku spoluprácu medzi verejnými a súkromnými subjektmi. ZKB zdôrazňuje potrebu partnerstiev medzi štátnymi orgánmi, ako je NBÚ, a prevádzkovateľmi základných a digitálnych služieb. Títo prevádzkovatelia majú povinnosť zabezpečiť adekvátnu úroveň kybernetickej ochrany a včas informovať NBÚ o prípadných incidentoch. V praxi to znamená, že NBÚ často spolupracuje s týmito subjektmi pri

[14] Bod 56 smernice NIS 2

vypracovávaní bezpečnostných opatrení, poskytovaní školení a výmene informácií o hrozbách a zraniteľnostiach.

NBÚ má tiež právomoc vykonávať kontrolu nad dodržiavaním zákona o kybernetickej bezpečnosti, čo zahŕňa audity, monitoring a neohlásené kontroly. Pri zistení porušenia legislatívnych požiadaviek môže NBÚ uložiť sankcie, ktoré môžu mať formu finančných pokút, nariadení nápravných opatrení alebo pozastavenia prevádzky. Sankcie sú dôležitým nástrojom na zabezpečenie plnenia povinností a prevencie potenciálnych škôd spôsobených kybernetickými útokmi.

Pri porovnaní rôznych prístupov k manažovaniu kybernetickej bezpečnosti v rámci EÚ môžeme popri NBÚ v Slovenskej republike spomenúť Spolkový úrad pre bezpečnosť v informačnej technike (BSI[15]) v Nemecku a Národný úrad pre kybernetickú a informačnú bezpečnosť (NÚKIB) v Českej republike.

V Nemecku je kybernetická bezpečnosť zabezpečovaná už spomenutým Spolkovým úradom pre bezpečnosť v informačnej technike (BSI), ktorý ako federálna inštitúcia disponuje širokými právomocami. BSI nielenže stanovuje bezpečnostné štandardy, ale poskytuje aj podporu pre verejné a súkromné subjekty. Tento prístup sa vyznačuje špecializáciou, ktorá umožňuje koncentrovanie odborných znalostí a technických zdrojov, čo vedie k efektívnejšej ochrane kritických infraštruktúr a rýchlej reakcii na incidenty.[16] Česká republika sa vydala podobnou cestou a v roku 2017 zriadila Národný úrad pre kybernetickú a informačnú bezpečnosť (NÚKIB)[17]. NÚKIB okrem iného spravuje národný bezpečnostný tím CSIRT.CZ a plní povinnosti vyplývajúce z európskej smernice NIS 2. Tento prístup umožňuje väčšiu odbornú hĺbku a flexibilitu pri riešení kybernetických hrozieb, čím prispieva k účinnejšej ochrane digitálnej infraštruktúry.

Na záver podkapitoly možno konštatovať, že každá z týchto krajín zvolila odlišný prístup k riadeniu kybernetickej bezpečnosti. Slovenská republika sa spolieha na centralizovaný model, zatiaľ čo Nemecko a Česká republika preferujú špecializované orgány. Kým centralizovaný model NBÚ prináša výhody v oblasti koordinácie a rýchlosti reakcie, špecializované inštitúcie ako BSI a NÚKIB ponúkajú hlbšiu expertízu a väčšiu flexibilitu pri riešení kybernetických hrozieb. Voľba konkrétneho modelu závisí od národných špecifík a prioritných cieľov v oblasti kybernetickej bezpečnosti.

ZÁVER

Implementácia smernice NIS 2 predstavuje zásadný krok v posilňovaní kybernetickej bezpečnosti v rámci Európskej únie. Smernica prináša niekoľko kľúčových zmien, ktoré reagujú na potreby súčasného digitálneho prostredia a rastúce riziká spojené s kybernetickými hrozbami. Rozšírením pôsobnosti smernice na širšiu škálu hospodárskych sektorov a zavedením jednotných kritérií na identifikáciu subjektov sa zabezpečuje konzistentné pokrytie kľúčových oblastí, ktoré sú nevyhnutné pre fungovanie vnútorného trhu EÚ.

Jednou z hlavných výziev pri implementácii smernice NIS 2 je prekonanie fragmentácie vnútorného trhu spôsobenej rozdielmi v národných legislatívach. Táto fragmentácia bola identifikovaná ako jeden z hlavných problémov už pri implementácii smernice NIS 1, ktorá nebola schopná dostatočne zjednotiť prístupy členských štátov. Smernica NIS 2 preto zavádza

[15] z nem. Bundesamt für Sicherheit in der Informationstechnik
[16] Pozri bližšie: Zweites Gesetzzur Erhöhung der Sicherheit informationstechnischer Systeme zo dňa 27.05.2021
[17] Pozri bližšie: Zákon č. 205/2017 Sb. zo dňa 14.07.2017

harmonizovanejšie a prísnejšie pravidlá, ktoré by mali viesť k vyššej úrovni kybernetickej bezpečnosti v celej Únii.

V Slovenskej republike je transpozícia smernice NIS 2 do národného právneho rámca zabezpečená prostredníctvom novely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Táto novela, pripravená Národným bezpečnostným úradom, reflektuje nielen požiadavky smernice, ale aj potreby vyplývajúce z aplikačnej praxe a rýchleho technologického pokroku. Navrhované zmeny zahŕňajú modernizáciu existujúcej legislatívy, rozšírenie pôsobnosti regulácie na nové subjekty, spresnenie bezpečnostných opatrení a úpravu procesu hlásenia incidentov.

Proces medzirezortného pripomienkového konania bude zohrávať kľúčovú úlohu pri formovaní finálnej podoby novely. Tento postup umožnil dotknutým subjektom, vrátane zástupcov priemyslu a odborných asociácií, vyjadriť svoje pripomienky a návrhy, čo prispeje k vylepšeniu a spresneniu navrhovaných ustanovení. Pripomienkové konanie odhalilo niekoľko kritických bodov, ako napríklad potrebu zosúladenia národných definícií s terminológiou používanou v európskych predpisoch, čo zaručí väčšiu konzistentnosť a efektívnosť legislatívy.

Je však potrebné zdôrazniť, že úspešná implementácia týchto zmien bude závisieť od jasných metodologických usmernení a efektívnej spolupráce medzi verejnými a súkromnými subjektmi. Práve spolupráca medzi štátnymi orgánmi, ako je NBÚ (resp. BSI, či NÚKIB), a prevádzkovateľmi základných a digitálnych služieb je nevyhnutná na zabezpečenie odolnosti voči kybernetickým hrozbám. Dôležitá bude aj podpora malých a stredných podnikov, ktoré často čelia výrazným výzvam v oblasti kybernetickej bezpečnosti.

Záverom možno konštatovať, že smernica NIS 2 a jej transpozícia prostredníctvom novely zákona č. 69/2018 Z. z. predstavujú významný krok smerom k zlepšeniu kybernetickej bezpečnosti na Slovensku. Úspešná implementácia týchto zmien si však bude vyžadovať pokračujúce úsilie, jasné legislatívne ukotvenie a efektívnu spoluprácu všetkých zúčastnených strán. Táto novela nielenže posilní národnú kybernetickú bezpečnosť, ale aj zabezpečí súlad s európskymi normami a požiadavkami, čím prispeje k vyššej odolnosti kybernetického priestoru v celej Európskej únii.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ANDRESS, J – WINTERFELD, S. 2011. Cyberspace Operation. In *Cyber Warfare*, 2011. [online] [cit. 19-08-2024]. Dostupné na internete: <https://www.sciencedirect.com/topics/computer-science/cyberspace-operation>. DOI: https://doi.org/10.1016/B978-1-59749-637-7.00002-2

CISA. 2024. What is Cybersecurity? In *Cybersecurity & Infrastructure Security Agency*, 2024. [online] [cit. 19-08-2024]. Dostupné na internete: <https://www.cisa.gov/news-events/news/what-cybersecurity>.

Dôvodová správa k návrhu novely zákona č. 69/2018 Z. z. LP/2020/400

FIELDMANN, B. 2022. CIA Triad. In *Fortinet*, 2020. [online] [cit. 19-08-2024]. Dostupné na internete: <https://www.fortinet.com/resources/cyberglossary/cia-triad>.

IBM. 2024. What is a cybersecurity? In *IBM*, 2024. [online] [cit. 19-08-2024]. Dostupné na internete: <https://www.ibm.com/topics/cybersecurity>.

IVANČÍK, R. 2020a. Cyber Threats as One of the Most Serious Asymmetric Security Threats in 21st Century. In Košice Security Revue, 2020, roč. 10, č. 1, s. 10-23. ISSN 1338-6956.

IVANČÍK, R. 2020b. Obrana kybernetického priestoru ako jedna z priorít Severoatlantickej aliancie v oblasti kybernetickej bezpečnosti a obrany. In *Aktuálne výzvy kybernetickej*

bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru, 2020, s. 35-46. ISBN 978-80-8040-819-3.

IVANČÍK, R. 2022. *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 240 s. ISBN 978-80-7380-873-0.

KASPERSKY. 2024. What is Cybersecurity? In *Kaspersky Lab*, 2024. [online] [cit. 19-08-2024]. Dostupné na internete: <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>.

Lisabonská zmluva, ktorou sa mení a dopĺňa Zmluva o Európskej únii a Zmluva o založení Európskeho spoločenstva (2007/C 306/01) – Konsolidované znenie

MICROSOFT. 2024. What is Cybersecurity? In *Microsoft*, 2024. [online] [cit. 19-08-2024]. Dostupné na internete: <https://www.microsoft.com/sk-sk/security/business/security-101/what-is-cybersecurity>.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA

NATALUCCI, F. – QURESHI, M. S. – SUNTHEIM, F. 2024. Rising Cyber Threats Pose Serious Concerns for Financial Stability. In *International Monetary Fund*, 2024. [online] [cit. 20-08-2024]. Dostupné na internete: <Rising Cyber Threats Pose Serious Concerns for Financial Stability>.

OIS. 2024. Confidentiality, Integrity, and Availability: The CIA Triad. In *Office of Information Security of the Washington University in St. Louis*, 2024. [online] [cit. 19-08-2024]. Dostupné na internete: <https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/>.

SAXENA, A. 2024. Importance of cyber security: Benefits and Disadvantages. In *Sprinto*, 2024. [online] [cit. 19-08-2024]. Dostupné na internete: <https://sprinto.com/blog/importance-of-cyber-security/>.

Smernica Európskeho Parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii

Zákon č. 205/2017 Sb. ktorým se mení zákon č. 181/2014 Sb., o kybernetické bezpečnosti zo dňa 14.07.2017

Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov č. 69/2018 Z. z. zo dňa 03.01.2018

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme zo dňa 27.05.2021

JUDr. PhDr. Roman Bartolomej Borovský
Zelená stráň 8, 040 14 Košice
rb.borovsky@gmail.com