Paneurópske právnické listy
ISSN: 2644-450X (online)

Ročník/Volume: **1**
Číslo/Number: **1**
Rok/Year: **2018**

Kybernetická bezpečnosť vo svetle novej legislatívy

Cyber security in light of new legislation

Mgr. Dagmar Yoder, Mgr. Lenka Caunerová
advokátska kancelária Deloitte Legal s.r.o.

Anotácia

Cieľom článku je priblíženie základnej charakteristiky novej legislatívy v oblasti kybernetickej bezpečnosti. Článok zahŕňa prehľad vývoja legislatívy na európskej, ako aj národnej úrovni a vysvetľuje základné povinnosti, ktoré prináša do praxe.

Annotation

The aim of the article is to provide a brief characteristics of the new legislation concerning cyber security. The article includes an overview of the evolution of legislation at both European and national level and explains the elementary duties it brings into practice.

Kľúčové slová

Kybernetická bezpečnosť

Key words

Cyber security

Paneurópske právnické listy
ISSN: 2644-450X (online)

Ročník/Volume: **1**
Číslo/Number: **1**
Rok/Year: **2018**

V súlade so schválenou Koncepciou kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 bol prijatý zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o kybernetickej bezpečnosti“), ktorý 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“). Zákon bol pripravený Národným bezpečnostným úradom ako ústredným orgánom štátnej správy pre kybernetickú bezpečnosť.

V súlade so smernicou NIS sa Zákon o kybernetickej bezpečnosti zameriava na siete a informačné systémy, ktoré hrajú zásadnú úlohu pri slobodnom pohybe informácií. Siete a informačné systémy sú v mnohých prípadoch priamo napojené na internetovú sieť. Ohrozenie ich bezpečnosti je preto spôsobilé predstavovať zásadné riziko nielen z lokálneho, ale aj celoeurópskeho, či dokonca svetového pohľadu. Bezpečnosť sietí a informačných systémov môže predovšetkým v prípadoch medzinárodných spoločností ohroziť bezpečnostnú stabilitu systémov v iných členských štátoch 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 systémov 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.

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 v rámci prijatých opatrení zohľadnili svoje vnútroštátne špecifiká a každý členský štát v tomto smere transponoval smernicu NIS s ohľadom na reálne, skutočné riziká vyskytujúce sa v spoločnosti.

Medzi hlavné oblasti úpravy Zákona o kybernetickej bezpečnosti 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 povinností Prevádzkovateľa základnej služby a Poskytovateľa digitálnej služby,
– organizácie a pôsobnosti jednotiek CSIRT a ich akreditácie,
– systému zabezpečenia kybernetickej bezpečnosti a minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti,
– kontroly a auditu.

Paneurópske právnické listy
ISSN: 2644-450X (online)

Ročník/Volume: **1**
Číslo/Number: **1**
Rok/Year: **2018**

Z pohľadu povinností vyplývajúcich zo Zákona o kybernetickej bezpečnosti je pre subjekty pôsobiace na trhu kľúčové identifikovať svoje postavenie z pohľadu Prevádzkovateľa základnej služby resp. Poskytovateľa digitálnej služby.

Prevádzkovateľ základnej služby

Prevádzkovateľom základnej služby je orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu, ktorá je klasifikovaná ako základná služba. Základnou službou je služba, ktorá je zaradená v zozname základných služieb a
a) závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore,
b) informačným systémom verejnej správy, alebo
c) je prvkom kritickej infraštruktúry.
Zoznam základných služieb tvorí prílohu k Zákonu o kybernetickej bezpečnosti a obsahuje napr. sektor bankovníctva, dopravy, digitálnej infraštruktúry, energetiky, priemyslu, zdravotníctva a pod.

Poskytovateľ digitálnej služby

Poskytovateľom digitálnej služby je v zmysle Zákona o kybernetickej bezpečnosti právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur.

Digitálnou službou je v zmysle príloh Zákona o kybernetickej bezpečnosti

a. *Online trhovisko* – Ide o digitálnu službu, ktorá umožňuje spotrebiteľom alebo podnikateľom uzatvárať online kúpne zmluvy alebo zmluvy o službách s podnikateľmi buď na webovom sídle online trhoviska, alebo na webovom sídle podnikateľa, ktoré využíva počítačové služby poskytované online trhoviskom.

b. *Internetový vyhľadávač* – Je digitálnou službou, ktorá umožňuje používateľom vyhľadávať v zásade na všetkých webových sídlach alebo na webových sídlach v konkrétnom jazyku informácie o akejkoľvek téme na základe kľúčového slova, vety alebo iných zadaných údajov, pričom jeho výsledkom sú linky, prostredníctvom ktorých možno nájsť informácie súvisiace s požadovaným obsahom,

c. *Služba v oblasti cloud computingu* – Je digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať.

Povinnosti a hlásenie incidentov

Každý subjekt, ktorý sa identifikuje ako Prevádzkovateľ základnej služby je povinný:

- Prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia.
- Uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s dodávateľom zodpovedným za prevádzku sietí a informačných systémov.
- Riešiť incident, hlásiť závažný incident, spolupracovať s úradom pri riešení hláseného incidentu, zabezpečiť dôkazy a určiť kontaktnú osobu pre hlásenia

Úrad môže za nedodržanie povinnosti uložiť pokutu od 300 EUR až do výšky 1% celkového ročného obratu za predchádzajúci účtovný rok, najviac však 300 000 EUR.

Použité informačné zdroje:

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
Dôvodová správa k Zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti
Smernica 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
Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020