Zákon o kybernetickej bezpečnosti

Identifikácia a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

- účinný dňom 1. apríla 2018
- transponoval smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informačných systémov v Únii
- upravuje práva a povinnosti osôb ako aj právomoc a pôsobnosť orgánov verejnej moci stanovením minimálnych požiadaviek na štandardné zabezpečenie významných informačných systémov v SR
- minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti v tomto zákone nebránia uplatňovať prísnejšie bezpečnostné opatrenia
- hlavným cieľom je ochrana a funkčnosť kybernetického priestoru

Organizácia, pôsobnosť a povinnosti orgánov verejnej moci § 4

1. Národný bezpečnostný úrad

2. Ústredný orgán

3. Iný orgán štátnej správy

Organizácia orgánov verejnej moci

1. Ústredné orgány štátnej správy – § 4 písm. a) b)

Národný bezpečnostný úrad, Ministerstvo dopravy a výstavby SR, Ministerstvo financií SR, Ministerstvo hospodárstva SR, Ministerstvo obrany SR, Ministerstvo vnútra SR, Ministerstvo zdravotníctva SR, Ministerstvo životného prostredia SR, Slovenská informačná služba, Úrad podpredsedu vlády SR pre investície a informatizáciu a Vojenské obranné spravodajstvo

2. Iné orgány štátnej správy – § 4 písm. c)

Ministerstvá a ostatné ústredné orgány štátnej správy, Generálna prokuratúra SR, Najvyšší kontrolný úrad SR, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov SR, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti

Jednotný informačný systém kybernetickej bezpečnosti § 8

- slúži na riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT
- určený na spracovanie a vyhodnocovanie údajov a informácií o stave kybernetickej bezpečnosti
- obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania
- pozostáva z verejnej a neverejnej časti – **verejná časť s obsahom podľa § 8 ods. 2 dostupná na www.nbu.gov.sk/kyberneticka-bezpecnost**
- prístup k nemu je bezodplatný a prebieha v reálnom čase

Organizácia jednotiek CSIRT

- Národná jednotka CSIRT
- Vládna jednotka CSIRT
- Jednotka CSIRT v pôsobnosti Ústredného orgánu

Národná jednotka CSIRT

- pôsobnosť pre celú SR

- plní úlohu ústredného orgánu v prípade, ak si ústredný orgán nezriadi jednotku CSIRT a ani neuzatvorí zmluvu na využívanie jednotky CSIRT iného ústredného orgánu

Sieť jednotiek CSIRT - § 11, 13, 15

Vládna jednotka CSIRT

- zriaďuje sa v pôsobnosti Úradu podpredsedu vlády SR pre investície a informatizáciu pre podsektor informačné systémy verejnej správy

Úlohy jednotky CSIRT

- vykonávanie preventívnych služieb a reaktívnych služieb

Akreditácia jednotky CSIRT

- zhodu s podmienkami akreditácie posudzuje úrad

Základná služba – tri druhy

1. v zmysle transpozície smernice NIS- služba, ktorá je uvedená v prílohe č. 1 zákona a ktorá spĺňa identifikačné kritéria podľa návrhu vyhlášky

2. ako informačný systém verejnej správy - identifikuje sa na základe dohody s ústredným orgánom, do ktorého sektor informačných systémov verejnej správy spadá (Úrad podpredsedu vlády SR pre investície a informatizáciu)

3. ako prvok kritickej infraštruktúry

Základná služba (1) – identifikačné kritériá

Dopadové kritériá	Návrh vyhlášky
počet používateľov využívajúcich základnú službu	obmedzenie alebo narušenie druhu služby postihujúce viac ako 15 000 osôb
závislosť ostatných sektorov podľa prílohy č. 1 základnej služby	obmedzenie alebo narušenie inej základnej služby, alebo obmedzenie alebo narušenie prevádzky prvku kritickej infraštruktúry
vplyv, ktorý by mohli mať kybernetické bezpečnostné incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti a záujmy štátu alebo na bezpečnosť štátu	hospodárska strata vyššia ako 0,1 % HDP
trhový podiel prevádzkovateľa služby	nedostupnosť druhu služby pre viac ako 1 600 osôb, ktorá nie je nahraditeľná iným spôsobom bez vynaloženia neprimeraných nákladov
geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť	obete na životoch s hraničnou hodnotou viac ako 10 mŕtvych alebo 1 000 zranených osôb vyžadujúcich lekárske ošetrenie
význam prevádzkovateľa základnej služby z hľadiska zachovania kontinuity poskytovania služby	narušenie verejnej bezpečnosti vo významnej časti správneho obvodu obce s rozšírenou pôsobnosťou, ktoré by mohlo vyžadovať vykonanie záchranných a likvidačných prác zložkami integrovaného záchranného systému

Špecifické sektorové kritéria

- faktory špecifické pre jednotlivé odvetvia
- napríklad

Odvetvie	Špecifické kritérium
dodávatelia energie	objem produkcie elektrickej energie na celoštátnej úrovni alebo podiel na tejto produkcii
dodávatelia ropy	objem za deň
letecká doprava vrátane letísk a leteckých prepravcov, železničnej dopravy a námorných prístavov	podiel na celoštátnej preprave a počet cestujúcich alebo operácií nákladnej dopravy za rok
infraštruktúra bankového alebo finančného trhu	jej systémový význam vyplývajúci z celkového objemu aktív alebo pomeru tohto celkového objemu aktív k HDP
zdravotníctvo	počet pacientov, ktorí sú v starostlivosti daného poskytovateľa za rok

- určené v návrhu vyhlášky

Základná služba (1)

Základná služba podľa § 3 písm. k) prvý bod

- spĺňa aspoň jedno dopadové kritérium a jedno špecifické sektorové kritérium, ak je uvedené
- prekročenie kritérií prevádzkovateľ oznamuje úradu do 30 dní od zistenia
- oznámenie - § 17 ods. 5
- úrad zaradí službu do zoznamu základných služieb a prevádzkovateľa do registra prevádzkovateľov základných služieb - zariadenie úrad oznámi (JISKB, schránka)

Prekročenie špecifických sektorových kritérií bez prekročenia dopadových kritérií

- oznamuje prevádzkovateľ služby spôsobom podľa § 17 ods. 5
- úrad nezaradí do zoznamu základných služieb
- slúži ako dôležitý poznatok pre úrad pri prehodnocovaní kritérií

Základná služba (2) a (3)

Základná služba ako informačný systém verejnej správy - § 3 písm. k) bod 2

- úrad zaradí takúto základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra základných služieb v spolupráci a po dohode s príslušným ústredným orgánom

- neskúma sa prekročenie identifikačných kritérií

Základná služba ako prvok kritickej infraštruktúry- § 3 písm. k) bod 3

- úrad automaticky zaradí takúto základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb

- neskúma sa prekročenie identifikačných kritérií

Prevádzkovateľ základnej služby – povinnosti - § 19

- prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté – v bezpečnostnej dokumentácii - § 20 ods. 5

Všeobecné bezpečnostné opatrenia

- v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov
- v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti
- pre všetky siete a informačné systémy

Sektorové bezpečnostné opatrenia

- špecifická kategorizácia sietí a informačných systémov v pôsobnosti ústredného orgánu
- v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti
- pre osobitné siete a informačné systémy
- splnomocnenie na vydanie vykonávacieho predpisu – úrad a ústredný orgán - § 32 ods. 2

Prevádzkovateľ základnej služby – povinnosti - § 19

- v prípade uzatvorenia zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
- informovať podnik na poskytovanie elektronických komunikačných služieb alebo sietí, ku ktorému je sieť alebo informačný systém základnej služby pripojený o tom, že je povinný plniť úlohy na úseku kybernetickej bezpečnosti **(dňom zaradenia do registra)**
- hlásiť, riešiť kybernetický bezpečnostný incident, spolupracovať s úradom a ústredným orgánom **(bezodkladne)**
- v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka
- hlásiť zmeny v údajoch podľa § 17 ods. 5 **(do 30 dní odo dňa ich vzniku)**

Digitálna služba, poskytovateľ digitálnej služby a zaradenie do zoznamu digitálnych služieb

Digitálna služba

- Online trhovisko
- Internetový vyhľadávač
- Cloud computing

Poskytovateľ digitálnej služby - 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

Zaradenie do zoznamu a registra

- na základe oznámenia (§ 21 ods. 1) poskytovateľom digitálnej služby
- úrad aj na základe vlastného zistenia

Úrad zaradenie služby do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb oznámi poskytovateľovi tejto služby

Povinnosti poskytovateľa digitálnej služby - § 21, 22, 23

- prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia – v zmysle vykonávacieho nariadenia Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 a vyčleniť personálne, materiálno-technické, časové a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby

- hlásiť a riešiť kybernetický bezpečnostný incident a spolupracovať s úradom pri riešení hláseného bezpečnostného incidentu

- uzatvoriť s prevádzkovateľom základnej služby zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby poskytovania digitálnej služby

- zástupca poskytovateľa digitálnej služby – písomne poverená osoba so sídlom v SR alebo EÚ - § 23

Hlásenie kybernetických bezpečnostných incidentov - § 24

Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

- strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému
- obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby
- vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
- ohrozenie bezpečnosti informácií

Kategórie závažných kybernetických bezpečnostných incidentov

- kategória I. stupňa
- kategória II. stupňa
- kategória III. stupňa

Hlásenie kybernetických bezpečnostných incidentov - § 24

Kybernetický bezpečnostný incident je identifikovaný ako **závažný kybernetický bezpečnostný incident**, ak spĺňa aspoň jedno identifikačné kritérium pre kategóriu závažného kybernetického incidentu – určené v návrhu vyhlášky

identifikačné kritérium	**kategória I. stupňa**	**kategória II. stupňa**	**kategória III. stupňa**
počet používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetických bezpečnostným incidentom	15 000	35 000	50 000
dĺžka trvania kybernetického bezpečnostného incidentu podľa percenta času uvedeného v pravidlách o úrovni poskytovaných služieb, ktoré patria pre jednotlivé služby	viac ako 40 % času	viac ako 60 % času	viac ako 75 % času
geografické rozšírenie kybernetického bezpečnostného incidentu	najmenej okres	najmenej kraj	celá SR
stupeň narušenia fungovania základnej služby alebo digitálnej služby	čiastočná	úplná	úplná bez náhrady
rozsah vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu	hospodárska strata počet zranených (mŕtvych) vplyv na verejný poriadok	hospodárska strata počet zranených (mŕtvych) vplyv na verejný poriadok	hospodárska strata počet zranených (mŕtvych) vplyv na verejný poriadok

Hlásenie kybernetických bezpečnostných incidentov - § 24, 25

Prevádzkovateľ základnej služby

- hlási každý závažný kybernetický incident – identifikovaná kategória (I, II, III) podľa vyhlášky
- bezodkladne

Poskytovateľ digitálnej služby

- hlási každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa vykonávacieho nariadenia Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov a parametrov na posudzovanie toho, či má incident závažný vplyv (Ú. v. EÚ L 26, 31. 1. 2018)
- bezodkladne po jeho zistení
- prostredníctvom jednotného informačného systému kybernetickej bezpečnosti

Hlásenie kybernetických bezpečnostných incidentov - § 24, 25

Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby

- môže uzatvoriť s úradom písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov (automatické hlásenie incidentov)

Audit - § 29

- prevádzkovateľ základnej služby
- preverením účinnosti prijatých bezpečnostných opatrení
- v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad
- vykonáva orgán posudzovania zhody, ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti
- úrad môže kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby, alebo požiadať orgán posudzovania zhody, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom

Prechodné ustanovenia - § 34

1. Základná služba 1 - **(§ 3 písm. k) bod 1)**

a) do 6 mesiacov oznámiť prekročenie identifikačných kritérií (najneskôr do októbra 2018)
b) do 2 rokov prijať bezpečnostné opatrenia (do apríla 2020)
c) do 2 rokov (do apríla 2020) uzavrie s dodávateľom zmluvu o zabezpečení bezpečnostných opatrení (§ 19 ods. 2)
d) do 3 rokov odo dňa 9. novembra 2018 predloží záverečnú správu o výsledkoch auditu (do 9. novembra 2021)

Prechodné ustanovenia § 34

2. Základná služba 2 – **(§ 3 písm. k) bod 2)**

- **zaradená do zoznamu po dohode s ústredným orgánom – do konca apríla zaslané oznámenia**
- **platia termíny podľa b) až d)**

3. Základná služba 3 – **(§ 3 písm. k) bod 3)**

- **zaradená do zoznamu automaticky úradom – do konca apríla zaslané oznámenia**
- **platia termíny podľa b) až d)**

regulacia@nbu.gov.sk

ĎAKUJEM ZA POZORNOSŤ