Legislativa kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Dne 29. srpna 2014 vstoupil v platnost s účinností od 1. ledna 2015 zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zpracovává příslušné předpisy Evropské unie (jedná se o transpozici směrnice NIS) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

Hlavním cílem zákona je:

- stanovit základní úroveň bezpečnostních opatření,
- zlepšit detekci kybernetických bezpečnostních incidentů,
- zavést hlášení kybernetických bezpečnostních incidentů,
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť.

V roce 2017 proběhly dvě obsahově významné novely zákona o kybernetické bezpečnosti, a to prostřednictvím zákona č. 104/2017 Sb. s účinností od 1. července a zákona č. 205/2017 Sb. s účinností od 1. srpna 2017. K aktuálnímu datu proběhly ještě následující novelizace tohoto zákona – novelizace zákonem č. 183/2017 Sb., zákonem 35/2018 Sb., zákonem č. 111/2019 Sb. a aktuálně poslední novelizace zákonem č. 12/2020 Sb.

Aktuální znění zákona je účinné od 1. února 2020.

Zákon je dostupný na stránkách NÚKIB pod tímto odkazem:

Zákon o kybernetické bezpečnosti

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)

Dne 6. července 2016 byla uveřejněna směrnice Evropského parlamentu a Rady (EU) 2016/1148 (dále jen „směrnice NIS“). **Tato směrnice má za cíl harmonizovat právní úpravu členských států v oblasti bezpečnosti sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti s cílem zlepšení fungování vnitřního trhu.**

Některé povinnosti, které směrnice NIS ukládá, jsou v České republice zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcími předpisy již řešeny.

Směrnice NIS mimo jiné rozšiřuje okruh subjektů, pro které budou stanoveny povinnosti v oblasti ochrany a prevence před kybernetickými bezpečnostními incidenty – jedná se o tzv. provozovatele základní služby a poskytovatele digitálních služeb (internetové vyhledávače, cloud computing a online tržiště). Požadavky směrnice zapracovává novela zákona o kybernetické bezpečnosti cestou zákona č. 205/2017 Sb. s účinností od 1. srpna 2017 (viz příslušná sekce stránek NÚKIB).

Transpoziční lhůta pro směrnici NIS je stanovena do 9. května 2018.

Směrnice NIS je dostupná na oficiálních stránkách EU pod tímto odkazem:

Směrnice NIS

Vyhláška o kybernetické bezpečnosti

Tato vyhláška zapracovává Směrnici NIS a pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby anebo informační systémy nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu,
- způsob likvidace dat, provozních údajů, informací a jejich kopií.

Dostupné verze vyhlášek:

Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti.

Nová vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti.

Nová vyhláška o kybernetické bezpečnosti byla zveřejněna ve Sbírce zákonů pod označením *"Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)".*

Vyhláška č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.

Dne 19. prosince 2014 vstoupila v platnost vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích. **Vyhláška stanoví významné informační systémy a kritéria pro jejich určení.**

V roce 2020 byla přijata novela vyhlášky, která má za cíl zpřesnit kritéria pro určení toho, zda je daný informační systém významný. Nabytí účinnosti celého znění vyhlášky je rozloženo do tří období (měnit se bude znění § 2, první období nastává 1. ledna 2021). Kompletní znění nabude účinnosti dne 1. ledna 2023. Konsolidovaný text vyhlášky včetně znázornění jednotlivých „vln" nabývání účinnosti § 2 je k dispozici zde:

Vyhláška č. 360/2020 Sb.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Nařízení vlády je platné od 30. prosince 2010. Nařízení vlády definuje průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury. V příloze k nařízení vlády je definováno 9 odvětví, včetně jednotlivých odvětvových kritérií pro určení prvku kritické infrastruktury.

Toto nařízení vlády nabylo účinnosti 1. ledna 2011. V souvislosti se zahrnutím oblasti kybernetické bezpečnosti do odvětvových kritérií proběhla novela nařízením vlády č. 315/2014 Sb., s účinnosti od 1. ledna 2015.

Nařízení vlády je dostupné na stránkách NÚKIB pod tímto odkazem:

Nařízení vlády o kritériích pro určení prvku kritické infrastruktury
(vč. kritické informační infrastruktury)

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Dne 15. prosince 2017 byla ve Sbírce zákonů České republiky vydána nová vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

Vyhlášku zpracoval Národní úřad pro kybernetickou a informační bezpečnost ve spolupráci s odbornou veřejností. Vyhláška zapracovává požadavky Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS).

Vyhláška upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti.

Vyhláška nabyla účinnosti dne 1. února 2018.

Vyhláška byla rozeslána stejnopisem částky Sbírky zákonu České republiky č. 157/2017 dne 15. prosince 2017. Tato částka Sbírky zákonů České republiky je dostupná zde:

Vyhláška č. 437/2017 Sb.

Důvodová zpráva k vyhlášce a připomínky uplatněné v rámci meziresortního připomínkového řízení jsou dostupné zde (v sekci verze materiálu – Verze pro jednání vlády nebo LRV):

Důvodová zpráva k vyhlášce č. 437/2017 Sb.

Podpůrné materiály a další informace k problematice určování provozovatele základní služby a informačního systému základní služby naleznete zde:

Podpůrné materiály a další informace

Od 1. ledna 2021 je účinné nové znění vyhlášky, kterým se v odvětví zdravotnictví mění dvě stávající kritéria a doplňují dvě nová kritéria (změna se týká speciálních kritérií druhu subjektu). Konsolidovaný text vyhlášky je k dispozici zde:

Nové znění vyhlášky č. 437/2017 Sb.

Prováděcí nařízení EK ke Směrnici NIS, které stanoví bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb

Dne 31. ledna 2018 zveřejnila Evropská komise prováděcí nařízení komise (EU) 2018/151, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (Směrnice NIS). **Toto prováděcí nařízení obsahuje bližší upřesnění bezpečnostních opatření, které musí poskytovatelé digitálních služeb (§ 3 písm. h) podle ZKB) zohledňovat při řízení bezpečnostních rizik**, jimž jsou vystaveny sítě a informační systémy, a dále bližší upřesnění parametrů pro posuzování toho, zda je dopad incidentu významný. **Toto prováděcí nařízení je účinné od 10. května 2018 a je přímo aplikovatelné.** Pro poskytovatele digitálních služeb je tedy závazné.

Prováděcí nařízení je dostupné na oficiálních stránkách EU pod tímto odkazem:

Prováděcí nařízení