NOVELA ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

V pátek dne 14. července 2017 byla ve Sbírce zákonů vyhlášena novela zákona o kybernetické bezpečnosti. Novela účinná od 1. srpna 2018 podstatně rozšiřuje okruh osob, které podle tohoto zákona musejí postupovat, a stanoví jim řadu nových povinností.

PŘEHLED ZMĚN

Novela v první řadě provádí směrnici 2016/1148/EU o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v EU. Nejzásadnější novinky lze rozdělit do několika oblastí, z nichž za nejvýznamnější lze považovat:

- nové povinnosti správců a provozovatelů informačního systému základní služby a provozovatelů základní služby,
- zcela nové zakotvení povinností pro poskytovatele digitální služby,
- nové povinnosti pro orgány veřejné moci ve vztahu k uzavírání smluv v IT a
- zřízení Národního úřadu pro kybernetickou a informační bezpečnost („Úřad“) se sídlem v Brně, který je ústředním správním úřadem pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací.

ZÁKLADNÍ SLUŽBY

To jsou služby poskytované v závislosti na sítích elektronických komunikací nebo informačních systémech, jejichž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z odvětví, které zákonodárce považuje za klíčová (např. energetika, doprava, bankovnictví, chemický průmysl). **Úřad do 9. listopadu 2018 určí osoby poskytující základní služby, které budou muset dodržovat přísnější bezpečností opatření** ukládané zákonem o kybernetické bezpečnosti anebo Úřadem. Osoby, které Úřad neurčí, budou moci fungovat v mírnějším režimu.

Se základními službami pak úzce souvisí zákonem upravené informační systémy, na kterých může být fungování základních služeb závislé. Správcům a provozovatelům takových informačních systémů a provozovatelům základních služeb zákon o kybernetické bezpečnosti nově ukládá povinnosti v oblasti kybernetické bezpečnosti, které spočívají zejména v zavedení bezpečnostních opatření a informační povinnosti v případě výskytu kybernetických bezpečnostních incidentů.

POSKYTOVATELÉ DIGITÁLNÍ SLUŽBY

Významnou novinkou je **zavedení povinností pro poskytovatele digitální služby, kterou se rozumí služba informační společnosti spočívající v provozování online tržiště, internetového vyhledávače anebo služeb cloud computingu**. Zákon se vztahuje na poskytovatele digitální služby, kteří jsou právnickými osobami a nejsou mikropodniky a malými podniky (tj. mají více jak 50 zaměstnanců a 10 milionů EUR roční obrat). Poskytovatelé digitální služby budou mít povinnost zřídit si v České republice svého zástupce v případě poskytování služby v Česku (pokud nemají zástupce v EU), přijmout bezpečnostní opatření ve smyslu zákona, hlásit vybrané významné ky-

bernetické bezpečnostní incidenty CZ.NIC a Úřadu, evidovat takové incidenty, případně na základě rozhodnutí Úřadu informovat veřejnost o výskytu kybernetického bezpečnostního incidentu a jeho dopadech. Za porušení uvedených povinností hrozí poskytovateli digitálních služeb pokuta až do výše 1 milionu korun českých.

ORGÁNY VEŘEJNÉ MOCI

Orgány veřejné moci mají s novelou zákona, mimo stávající povinnosti, také povinnost si ve smlouvách s poskytovateli digitálních služeb cloud computingu zajistit, že budou dodržována bezpečnostní pravidla stanovená Úřadem. Zákon také stanovuje nezbytné náležitosti, které musejí takové smlouvy obsahovat, a obecná pravidla, která by měla být řešena v rámci bezpečnostních opatření zakotvených ve smlouvách s poskytovateli digitálních služeb cloud computingu. Obecně zákon zpřísnil požadavky na zabezpečení a výběr dodavatelů informačních systémů a požadavky na smluvní dokumentaci vážící se k vybraným systémům a službám. Všechny smluvní vztahy, které nesplňují požadavky dle zákona o kybernetické bezpečnosti, musejí být uvedeny do souladu s novými požadavky zákona do 1. srpna 2018, což může pro mnohé, zejména tedy orgány veřejné moci, znamenat **úpravu uzavřených smluv anebo uzavření smluv nových**.

ÚŘAD

V neposlední řadě dochází ke zřízení Úřadu a udělení mu pravomocí vydávat obecné bezpečnostní standardy, udělovat konkrétní doporučení anebo rozhodnutí či vydávat opatření obecné povahy za účelem zvýšení kybernetické bezpečnosti u jednotlivých dotčených osob a poskytovatelů služeb. Zároveň je Úřad jedním z povinných míst, kam se budou hlásit kybernetické bezpečnostní incidenty. Bude zároveň oprávněn udělovat pokuty za nesplnění povinností dle zákona, a to až do výše 5 milionů korun.

Havel, Holásek & Partners s.r.o., advokátní kancelář

NÚKIB ZAHÁJIL ČINNOST

V Brně 1. srpna oficiálně zahájil činnost Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který se novelou zákona vyčlenil z Národního bezpečnostního úřadu (NBÚ). Nyní má 118 zaměstnanců, v budoucnu by jich mohlo být asi 400.

Pod NBÚ mělo dosud kybernetickou bezpečnost na starosti Národní centrum kybernetické bezpečnosti (NCKB), které se nyní spolu s dalšími částmi NBÚ vydělilo do NÚKIB. Mezi vyčleněné části patří například ochrana utajovaných informací v informačních a komunikačních systémech, kryptografická ochrana a neveřejná služba v rámci družicového systému Galileo.

NÚKIB by měl například zajišťovat podporu v případě kybernetických útoků. Součástí práce týmu lidí bude i prevence, tedy aby systémy informační infrastruktury odpovídaly současným bezpečnostním kritériím.

Kybernetické útoky na kritickou či důležitou informační infrastrukturu jsou v posledních letech na vzestupu. Vládní tým GovCERT eviduje zhruba 100 bezpečnostních incidentů měsíčně. Útoky mohou ohrozit klíčové služby státu, zajištění bezpečnosti a jeho obranyschopnost, ale také soukromé podniky a každodenní život obyvatel.