Právní výzvy v oblasti kybernetické bezpečnosti

Mgr. Petra Vráblíková

advokát

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

- Účinný od 1. 1. 2015
- Prováděcí předpisy:
  - vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
  - Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
  - Usnesení vlády č. 105/2015, č. 382/2015…

Zákon č. 104/2017 Sb., kterým se mění zákon č. 365/200 Sb., o informačních systémech veřejné správy

- Nové povinnosti soukromých osob i správců IS VS
- Nové sankce
- Včetně novely zákona o kybernetické bezpečnosti, směřující k:
  - vztažení úpravy na provozovatele ISVS
  - Zavedení nových povinností provozovatele – zejména vždy předat data správci ISVS bez ohledu na autorská práva k systému, na jeho pokyn kopii dat zničit a umožnit dohled nad průběhem ničení dat
  - Povinnost je vynutitelná prostřednictvím Úřadu, sankce se zvyšují o řád

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

Základní principy směrnice

- Harmonizace standardů kybernetické bezpečnosti
- Povinnost přijmout strategii kybernetické bezpečnosti
- Povinnost mít CSIRT tým
- Povinnost spolupracovat s ostatními státy při řešení incidentů
  - Na úrovni technické
  - Na úrovni strategické
- Povinnost zavést řízení rizik a zlepšit sdílení informací mezi soukromým a veřejným sektorem.

Vládní návrh novely KBZ (dnes v Senátu)

Působnost zákona se rozšiřuje na:

- tzv. základní služby v oblasti energetiky, dopravy, zdravotnictví, bankovnictví, finanční trhy, vodní hospodářství, chemický průmysl a digitální infrastrukturu a jejich informační systémy
  - Provozovatele základní služby
  - Správce a provozovatele informačních systémů základní služby

- Digitální služby a jejich poskytovatele
  - online tržiště
  - internetové vyhledávače
  - cloud computing

Povinnosti provozovatelů základních služeb:

- Informovat správce nebo provozovatele IS VS o jejich určení jakožto provozovatele ZS
- Oznámit NBÚ významný dopad kybernetického bezpečnostního incidentu na kontinuitu poskytování ZS
- Informovat o probíhajícím kybernetickém bezpečnostním incidentu veřejnost na základě rozhodnutí NBÚ
- Poskytnout kontaktní údaje

Povinnosti provozovatelů digitálních služeb

- Povinnost implementovat bezpečnostní opatření v míře přiměřené k řízení bezpečnostních rizik, jimž jsou vystaveny jejich IS
- Povinnost hlášení kybernetických incidentů s významným dopadem na poskytování digitálních služeb
- Povinnost hlášení kontaktních údajů
- Povinnost spolupráce s národním CERT a NBÚ

Obě skupiny

- Povinnost podřídit se výkonu státní správy CERT a NBU
  - povinnost podřídit se reaktivním a ochranným opatřením
  - Plnění povinností za stavu kybernetického nebezpečí (pouze provozovatelé základních služeb)
  - Povinnost podřídit se kontrole (u provozovatelů digitálních služeb pouze ex post)

Další změny:

- Nad rámec směrnice
  - Povinnost ukládat svá data pouze na cloudech garantujících přístupnost informací a dat pro správce KII, VIS a ISZS (pokud jsou OVM)
  - Regulace vztahu mezi provozovateli ZS a správci IS ZS
  - Striktní vymezení obsahu veřejnoprávních smluv o provozu IS
  - Doplnění kontrolních a sankčních pravomocí NBÚ

GDPR cirkus

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

+ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.
+ Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

Směrnice NIS

- Pouze subjekty poskytující služby **v kritické infrastruktuře státu**
- Umožňuje **přenos odpovědnosti** za bezpečnostní opatření mezi správcem/provozovatelem
- Týká se pouze **ochranných a reaktivních opatření proti** kybernetickým ohrožením

GDPR

- Platná **pro každou organizaci** nabízející zboží nebo služby v rámci členských států EU a manipulující s osobními údaji subjektů IT.
- Bezpečnostních opatření musí být implementovány **do technických a organizačních procesů a postupů již od počátku jejich přípravy**

Děkuji za pozornost

Mgr. Petra Vráblíková

advokát

Karlštejnská 518, 252 29 Lety

vrablikova.petra@gmail.com