Novela zákona o kybernetické bezpečnosti

Jaroslav Šmíd
náměstek ředitele

Národní úřad pro kybernetickou a informační bezpečnost

Transpozice směrnice NIS v ČR

- Přijetí úpravy do 21 měsíců od vstupu směrnice v platnost – do května 2018
- Nutná novela již účinného zákona o kybernetické bezpečnosti

Příprava novely

- Březen 2016 – počátek přípravných prací
- pracovní skupiny na úrovni resortů a odborné veřejnosti

Legislativní proces

- 4.Q 2016 - schváleno vládou
- 2.Q 2017 schváleno sněmovnou a senátem

Platnost a účinnost

- Účinnost transpoziční novely od 1. 8. 2017
- Následují prováděcí právní předpisy

Zákon o kybernetické bezpečnosti – změny v r. 2017

- **ZKB byl v r. 2017 novelizován ve dvou liniích:**
  - **„Velká novela“ – transpozice směrnice NIS**
    - **Novela účinná od 1. 8. 2017** (Novela cestou zákona č. 205/2017 Sb.)
    - **Úpravy ZKB:** nové definice (§ 2), nové povinné osoby (§ 3), Vznik „Národního úřadu pro kybernetickou a informační bezpečnost“, změny správních deliktů (§ 25)…
  - **„Malá novela“ – změna novelou zákona č. 365/2000 Sb., o ISVS**
    - **Novela účinná od 1. 7. 2017** (Novela cestou z. č. 104/2017)
    - **Úpravy ZKB:** nový pojem provozovatel IS/KS (§ 2 písm. g), ustanovení o vlastnictví dat (§ 6a), hlášení incidentů provozovatelem (§ 8/4), pravomoc nařízení předání dat (§ 15a), změny správních deliktů (§ 25),

Nové povinné osoby

- **Nové povinné osoby:**
  - **Provozovatel základní služby (PZS), informační systém základní služby (ISZS)**
    - Systémy klíčové pro zajišťování některých hospodářských a ekonomických činností
  - **Poskytovatel digitální služby (PDS)**
    - Zajišťuje služby cloudu, internetového vyhledávače, e-commerce
  - **Provozovatel informačního/komunikačního systému KII/VIS/PZS**
    - *„zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“ = klíčový dodavatel*
    - *Zařazen do povinných osob* – zavádí bezpečnostní opatření tam, kde je nemůže zavést správce
    - Důvod úpravy: problémy se zabezpečením dodavatelů,

Struktura povinných podle ZKB – stav od 1. 8. 2017

- §3 ZKB

a) poskytovatelé služeb elektronických komunikací, subjekt zajišťující sít elektronických komunikací b) orgán nebo osoba zajišťující významnou síť **h) Poskytovatel digitálních služeb**	NÁRODNÍ CERT *CZ.NIC*
c) správce **a provozovatel** IS KII d) správce **a provozovatel** KS KII e) správce **a provozovatel** VIS **f) správce a provozovatel IS základní služby** **g) provozovatel základní služby**	VLÁDNÍ CERT *NÚKIB*

* Tučně jsou vyznačeny změny

Definice podle zákona o kybernetické bezpečnosti (ZKB)

- **Základní služba** = služba, jejíž poskytování **je závislé na sítích nebo informačních systémech** a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví:

  1. energetika
  2. doprava
  3. bankovnictví
  4. infrastruktura finančních trhů
  5. zdravotnictví
  6. vodní hospodářství
  7. digitální infrastruktura
  8. chemický průmysl

- **Informační systém základní služby** = systém, na jehož fungování je závislé poskytování základní služby
- **provozovatel základní služby** = orgán nebo osoba, která je odpovědná za poskytování základní služby a která je určena NÚKIB

Provozovatel základních služeb (PZS) - obecně

- Kritéria stanoví prováděcí vyhláška k ZKB
- PZS určí NUKIB podle dopadových a odvětvových kritérií NÚKIB
- Dopadová a odvětvová kritéria
  - Odvětvová kritéria kopírují přílohu II. NIS (+ některá další přidána)
  - Dopadová kritéria respektují požadavky směrnice (čl. 6 NIS) a zohledňují národní podmínky
- Kritéria nastavena ve spolupráci se soukromou sférou a regulátory
  - Pracovní skupina (13 podskupin – celkem cca 100 odborníků)
- Kritéria nastavena tak, aby regulace pokryla pouze systémy nezbytné pro zajištění služeb
  (ne fakturační, marketingové systémy ani např. bankomaty)
- Předpokládaná účinnost vyhlášky a začátek určování – únor 2018

Určování provozovatelů základních služeb (PZS) - kritéria

1. **Definice ZKB**
   - Závislost na IS/KS (článek 5 odst. 2 NIS)
   - Poskytuje službu ve vymezených odvětvích (příloha II. NIS)

2. **Odvětvová kritéria (3 úrovně)**
   - Druh služby
   - Druh subjektu (příloha II. NIS)
   - Speciální kritéria druhu subjektu (článek 6 odst. 2 NIS)

3. **Dopadová kritéria**
   - Dopad kybernetického bezpečnostní incidentu v informačním/komunikačním systému (článek 6 NIS)

Pro určení je třeba naplnit všechny tři podmínky

Schéma systému kritérií pro určení PZS a ISZS

- Odvětvová kritéria mají 3 úrovně
- Je posuzováno zda, je naplní subjekt - **organizace**
- Postupuje se od obecného ke speciálnímu

Druh služby
- Výroba elektřiny

Druh subjektu
- Výrobce elektřiny

Speciální kritéria druhu subjektu
- Výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW

Odvětvová kritéria - Posuzuje se subjekt
ÚROVEŇ ORGANIZACE

- Dopadová kritéria – je posuzováno, zda je naplní **IS/KS**

Dopad kyber. bezp. incidentu
- Dopadová kritéria

Dopadová kritéria
Posuzuje se dopad KBI v systému subjektu
ÚROVEŇ SYSTÉMU

Určení PZS a IS ZS

Subjekt naplnil odvětvová kritéria a posuzovaný systém dopadová kritéria

Provozovatel základních služeb (PZS) – odvětvová kritéria

- Energetika
  - Elektřina, plyn, ropa, teplárenství *
- Doprava
  - Letecká, železniční, vodní, silniční
- Bankovnictví
- Infrastruktura finančních trhů
- Zdravotnictví
- Vodní hospodářství
  - Pitná voda, nakládání s odpadní vodou *
- Digitální infrastruktura
- Chemický průmysl *

+ Specifická kritéria v jednotlivých odvětvích (minimální výkon, kapacita apod.)

* **Přidáno nad rámec požadavků NIS**

Provozovatel základních služeb – dopadová kritéria (ČR) I.

- Posuzuje se dopad incidentu v informačním/komunikačním systému
- Incident v informačním/komunikačním systémů muže způsobit:
  I. závažné omezení či narušení druhu služby postihující více než 25 000* nebo 50 000* nebo 500 000* osob,
     - Odpovídá dopadu dle článku 6 odst. 1 písm. a) NIS
  II. závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,
     - Odpovídá dopadu dle článku 6 odst. 1 písm. b) NIS
     - Zároveň umožňuje určit provozovatele, který je důležitý pro jiný stát EU (čl. 5 odst. 4 NIS).
  III. hospodářskou ztrátu vyšší než 0,25 % HDP,
     - Odpovídá dopadu dle článku 6 odst. 1 písm. c), d) NIS

* V závislosti na specificích jednotlivých odvětví se tyto hodnoty liší

Provozovatel základní služby – dopadová kritéria (ČR) II.

IV. nedostupnost definovaného druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,

- Odpovídá dopadu dle článku 6 odst. 1 písm. f) NIS

V. oběti na životech s mezní hodnotou více než 100 nebo 200* mrtvých nebo 1 000 zraněných osob vyžadujících lékařské ošetření,

- Odpovídá dopadu dle článku 6 odst. 1 písm. c) NIS

VI. narušení veřejné bezpečnosti na významné části správního území obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací základními a ostatními složkami integrovaného záchranného systému, nebo

- Odpovídá dopadu dle článku 6 odst. 1 písm. a), c), e) NIS

VII. kompromitaci citlivých údajů o více než 200 000 osobách

- Odpovídá dopadu dle článku 6 odst. 1 písm. c) NIS

* V závislosti na specifických jednotlivých odvětví se tyto hodnoty liší

Úprava vztahů s poskytovatelem cloud computingu

- KII, VIS a PZS, kteří jsou orgánem veřejné moci, jsou povinni s poskytovatelem cloud computingu smluvně ošetřit vlastnictví dat a možnost jejich kontroly
- Dále zákon stanoví povinné náležitosti smluv v této oblasti :
  a) respektování bezpečnostní politiky KII/VIS/PZS
  b) stanovení úrovně poskytovaných služeb,
  c) systém schvalování subdodavatelů služby cloud computingu,
  d) specifikace podmínek ukončení smlouvy z pohledu bezpečnosti,
  e) řízení kontinuity činností v souvislosti s poskytovanou službou,
  f) určení vlastníka uchovávaných dat,
  g) dohoda o důvěrnosti,
  h) stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,
  i) pravidla zákaznického auditu
  j) povinnost informovat odběratele služeb o incidentech
- Důvod: často velmi problematické smlouvy v oblasti IT ve státní správě

Provozovatel informačního/komunikačního systému

- Nová povinná osoba v ZKB: *„zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“* = klíčový dodavatel
- Identifikace:
  - Správce může pověřit jiného provozem KII/VIS, pokud to nevylučuje jiný zákon
  - Odpovědnost za identifikaci provozovatele má správce
  - Způsob identifikace zákon nedefinuje – lze dovodit ze smluvního vztahu
  - Správce informuje dodavatele, že se stává provozovatelem
  - Provozovatel musí plnit ZKB v nezbytném rozsahu
- Povinnosti
  - Provozovatel zavádí povinnosti ze ZKB tam, kde je nemůže zavést správce a tam, kde to po něm správce vyžaduje
  - Za toto provozovateli náleží náhrada nákladů

Hlášení incidentů

- Všechny povinné osoby vyjma poskytovatelů služeb el. komunikací musí hlásit incidenty, čímž není dotčena povinnost z GDPR,
- Zavedena možnost přenést hlášení incidentu ze správce na provozovatele KII/VIS
  - Pokud Úřadu hlásí incident provozovatel, musí zároveň informovat správce
- Zavedena možnost dobrovolného hlášení incidentů Vládnímu CERTu nebo Národnímu CERTu i pro jiné než povinné osoby
- § 12 odst. 3: Právo NÚKIB informovat veřejnost o incidentu
- V případě že existuje veřejný zájem na tom aby byly zveřejněny informace o incidentu má Úřad právo informovat nebo dotčené osobě uložit aby tak učila sama
  - Krajní možnost omezená veřejným zájmem a konzultací s dotčeným subjektem

Předávání dat, přístup k informacím

- Zavádí se pravomoc NÚKIB uložit v případě hrozícího incidentu provozovateli systému předat data, provozní údaje a informace spojené se IS/KS
  - Na návrh správce KII/VIS
  - Povinné náležitosti návrhu: odůvodnění, popis přechozích jednání mezi správcem a provozovatelem, možné následky nepředání dat, údajů a informací
- Prolomení zákona o svobodném přístupu k informacím (§ 10a ZKB)
  - Neposkytují se informace jejich zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření
  - Informace, které jsou vedené v evidenci incidentů
  - Je třeba stanovit co je informací, jejíž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti => klasifikace informací (podle vyhlášky č. 316/2014 Sb.)

Přestupky

- Zavedení nových přestupků, doplnění nových povinných osob
- Změna výše sankcí za přestupky – zvyšují se pokuty
  - Z 100 000 Kč na 1 000 000/5 000 000 Kč
  - Spodní hranice pokut nestanovena

Povinnost	Sankce
Neplnění nápravných opatření , rozhodnutí, nepředání dat	až 1 000 000
Nebude mít smluvně ošetřené vlastnictví, ničení a předání dat	až 1 000 000
Nehlásí incidenty, neplnění rozhodnutí,	až 1000 000
Nezavede bezpečnostní opatření	až 5 000 000
Hlášení kontaktních údajů	Až 10 000
Nepředá data, nezničí data/nespolupracuje při určování	až 200 000

Stav implementace požadavků NIS v ČR – k 1. 9. 2017

Směrnice NIS 2017	ZKB před novelou 2015 - 2017	ZKB po novele 2017 ->
Národní strategie bezpečnosti sítí a informací	✓	✓
Zavádí požadavky na bezpečnost a oznamování incidentů	✓	✓
Ustavuje síť skupin pro reakci na incidenty (CSIRT)	✓	✓
Povinnost zřídit vnitrostátní orgány, které budou mít bezpečnost sítí a IS v gesci	✓	✓
Určit jednotné kontaktní místo v regulované oblasti	✓	✓
Určení PZS	⚠ *	✓
Určení PDS	✗ **	✓

* Zavedeno částečně – kritická informační infrastruktura

** Nezavedeno

Výzva č. 10 – Kybernetická bezpečnost

- **Operační program:** Integrovaný regionální operační program
- **Prioritní osa:** Dobrá správa území a zefektivnění veřejných institucí
- **Specifický cíl - 3.2** : Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT.
- **Oprávnění žadatelé:** Organizační složky státu, příspěvkové organizace organizačních složek státu, státní organizace a státní podniky. Kraje, organizace zřizované nebo zakládané kraji, obce (kromě Prahy a jejích částí), organizace zřizované nebo zakládané obcemi (kromě Prahy a jejích částí).
- **Ukončení příjmu žádostí o podporu:** 22. 11. 2017

Výzva č. 10 – Kybernetická bezpečnost

- Výzva se týká zvýšení odolnosti systémů kritické informační infrastruktury, tzv. významných informačních systémů a informačních systémů poskytovatelů základní služby veřejné správy proti kybernetickým hrozbám. Hlavní podporovanou aktivitou jsou technická opatření vedoucí k zabezpečení vyjmenovaných informačních systémů. Budou podporována opatření jako například fyzická bezpečnost (např. kamerové systémy, protipožární opatření apod.), nástroj pro ověřování identity uživatelů (správa uživatelských hesel), nástroj pro zaznamenávání činnosti kritické informační infrastruktury , významných informačních systémů a informačních systémů základní služby, jejich uživatelů a administrátorů.
- **Podrobnosti k Výzvě:** https://www.strukturalni-fondy.cz/cs/Microsites/IROP/Vyzvy/Vyzva-c-10-Kyberneticka-bezpecnost

Děkuji Vám za pozornost

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost