Aktuality NIS2 transpozice do ZKB

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

12. dubna 2023

TLP: GREEN

Petr Kopřiva
vedoucí oddělení regulace cloud computingu

Co potřebujeme vědět na začátku

- *Prezentace má informační a osvětových charakter a informace v ní obsažené se mohou se v čase změnit.*

- Směrnice obecně je legislativní akt Evropské unie, který není* sám o sobě aplikovatelný **(= musí nejdříve vzniknout národní úprava)**
- Kybernetická bezpečnost v České republice **je již nyní regulována** (= je z čeho vycházet)
- Základem změn je nově přicházející **směrnice NIS2** (= viz dále), ale také potřeba zákon o kybernetické bezpečnosti aktualizovat

*zpravidla

Stav směrnice NIS2

- Směrnice byla publikována 27. prosince 2022
- Gestor problematiky (předkladatel návrhu transpozičního zákona) = NÚKIB

- **Transpozice, tj. provedení obsahu směrnice do českého práva je potřeba provést do 17. října 2024.**

Regulované služby (směrnice NIS2)

Směrnice NIS1:

30 služeb v 7 odvětvích

Kritéria dopadu incidentu

⇒ **cca 400 povinných osob**

„Kybernetickou bezpečnost musí řešit pouze ti s nejvyšší mírou dopadu na společnost.“

Směrnice NIS2:

60 služeb v 18 odvětvích

Kritérium velikosti subjektu

⇒ **cca 6000 povinných osob**

„Kybernetickou bezpečnost musí řešit každý, kdo na ní má finance.“

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential“.

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik“ a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik“ a „střední podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important“ (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

Nový ZKB – povinné osoby

- Povinné osoby budou určovány primárně na základě velikosti (střední a velké podniky) a poskytované služby
- Poskytovatel regulované služby
  - Jediná povinná osoba
  - Poskytuje regulovanou službu = služba splňující kritéria stanovená vyhláškou
- Režim poskytovatele regulované služby
  - Stanovuje míru povinností – vyšší režim / nižší režim (vyšší cca 1000 povinných osob, nižší cca 5000)
  - Ke každému režimu bude vyhláška, která bude definovat bezpečnostní opatření
- Naplnění kritérií je povinen hlásit poskytovatel služby = každý si musí vyhodnotit kritéria sám
  - Do 30 dnů od doby, kdy naplnění zjistí, nejpozději do 90 kdy k naplnění došlo
- NÚKIB muže zaregistrovat i sám dozví-li se o naplnění kritérií

Nový zákon o kybernetické bezpečnosti – povinnosti

- Hlavní povinnosti
  - Hlásit kontaktní a další údaje
  - Stanovit rozsah řízení kybernetické bezpečnosti – definuje rozsah regulace v organizaci
  - Zavádět bezpečnosti opatření – podle režimu v kterém je služba určena (vyšší/nižší)
  - Hlásit kybernetické bezpečnostní incidenty
  - Informovat zákazníky o incidentech a hrozbách
  - Provádět protiopatření
  - Plnit povinnosti z Mechanismu řízení bezpečnosti dodavatelského řetězce u vybraných služeb
  - Zajistit dostupnost strategicky významných služeb

- Zákon dále upravuje další oblasti nezbytné pro fungování regulatorního rámce
  - Specifické situace – poskytování informací, stav kybernetického nebezpečí
  - Úprava institucí – NÚKIB, CERT a jejich pravomoci, součinnost dalších orgánů státu
  - Sankce – přestupky, úprava horních limitů sankcí

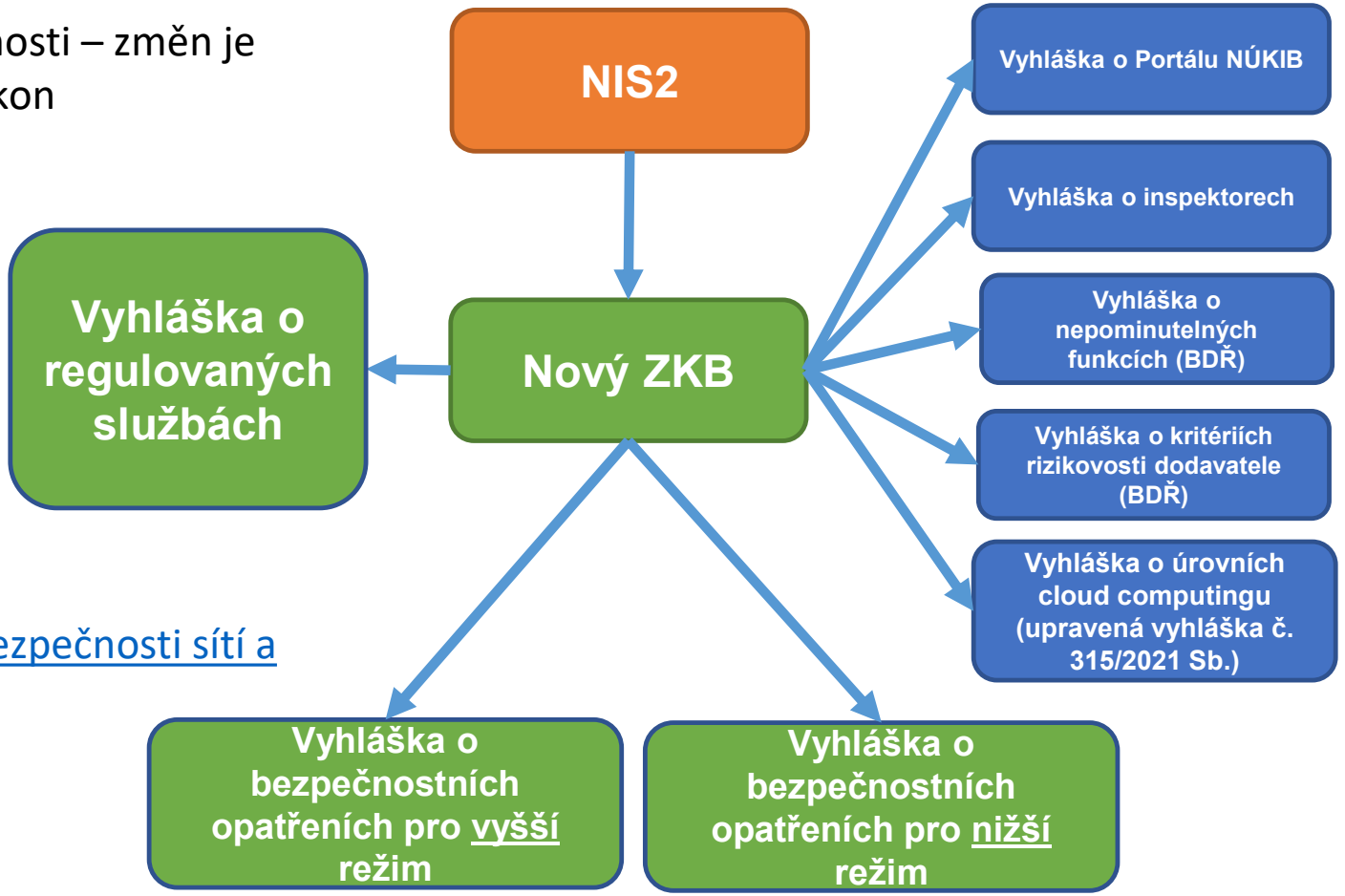
Nový zákon o kybernetické bezpečnosti (NZKB)

Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo třeba vytvořit nový zákon

zcela nová úprava – cca 60 paragrafů

Zveřejněný návrh má aktuálně navíc 8 vyhlášek

Celý návrh zveřejněn zde: [Course: Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)]



NZKB - hlavní dopady na organizace

- **Nové povinné osoby**
  - Primárně **v režimu nižších povinností**:
    - ⇒ Povinnost zaregistrovat se a udat kontaktní údaje NÚKIB
    - ⇒ Základní úroveň bezpečnostních opatření
    - ⇒ Hlášení významných kybernetických incidentů
    - ⇒ Řízení se reaktivními protiopatřeními vydanými NÚKIB

- **Původní subjekty dle ZKB**
  - Primárně v režimu vyšších povinností:
    - ⇒ Bezpečnostní opatření jsou vymezeny službou – může dojít k rozšíření okruhu, na který budou bezpečnost zavádět, ale konkrétní opatření se pro vyšší režim mění pouze minimálně
    - ⇒ NIS2 stanovuje vyšší sankce za porušení – blíže GDPR
    - ⇒ Povinnost samoidentifikace spíše než kontaktování ze strany NÚKIB

Komunikace návrhů – veřejné konzultace

- Veřejná konzultace a zveřejnění prvotních návrhů ZKB pro podněty veřejnosti bylo zahájeno 26. ledna 2023 a ukončeno 12. března 2023
- NÚKIB obdržel podněty od 117 jednotlivých míst (toho bylo 27 obsahově stejných)
- Celkový počet jednotlivých podnětů ve vyšších stovkách, do jednoho tisíce

- Další předpokládané kroky
  - Druhá polovina dubna – rozeslání vypořádání z veřejných konzultaci směrem k autorům podnětů
  - Polovina května – start Mezirezortního připomínkového řízení (MPŘ) – 2Q 2023
    - Oficiální zahájení legislativního procesu
    - Zveřejnění došlých podnětů veřejnosti vč. vypořádání a zveřejnění návrhů předložených do MPŘ
  - Legislativní rada vlády – 3/4Q 2023
  - Poslanecká sněmovna – konec 2023
  - Vydání zákona říjen 2024 (konec transpoziční lhůty)

Veřejné konzultace – hlavní připomínky

- Mechanismus prověřování dodavatelského řetězce
- Nastavení inspektorů
- Obsah vyhlášky o bezpečnostních opatřeních pro režim nižších povinností
- Lokalizace informací a dat při zpracování v zahraničí
- Stav kybernetického nebezpečí
- Vymezení regulovaných služeb
- Výjimka pro zpravodajské služby
- Přestupky a další sankce

Veřejné konzultace – hlavní změny

- Nastavení inspektorů - > zrušení institutu
- Obsah vyhlášky o bezpečnostních opatřeních pro režim nižších povinností - > zeštíhlení, zjednodušení
- Lokalizace informací a dat při zpracování v zahraničí - > zajištění dostupnosti strategicky významných služeb z ČR
- Určovací a identifikační kritéria ve vyhlášce - > přesun určovacích kritérií do zákona + odvětví
- Výjimka pro zpravodajské služby - > přidána obdobně jak nyní v ZKB

Děkuji za pozornost

Dotazy a připomínky k návrhům nových předpisů je možné zasílat na:

regulace@nukib.cz