Nový zákon o kybernetické bezpečnosti

Zpráva o aktuálním stavu

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Konference egovernment 20:10
5. září 2023
TLP: CLEAR

Adam Kučínský
ředitel
odbor regulace

Shrnutí návrhu zákona

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

Základem změn je nově přicházející **směrnice NIS2** (= viz dále), ale také potřeba zákon o kybernetické bezpečnosti aktualizovat.

Do návrhu zákona jsou promítnuty také vnitrostátní instituty a požadavky.

Směrnice obecně je legislativní akt Evropské unie, který není* sám o sobě aplikovatelný **(= musí nejdříve vzniknout národní úprava).**

Národní úřad pro kybernetickou a informační bezpečnost **připravil návrh nového zákona o kybernetické bezpečnosti.**

Návrh zákona je v meziresortním připomínkovém řízení.

Nová pravidla by měla platit v druhé polovině roku 2024 (do 17. října 2024 podle požadavku směrnice NIS2).

*zpravidla

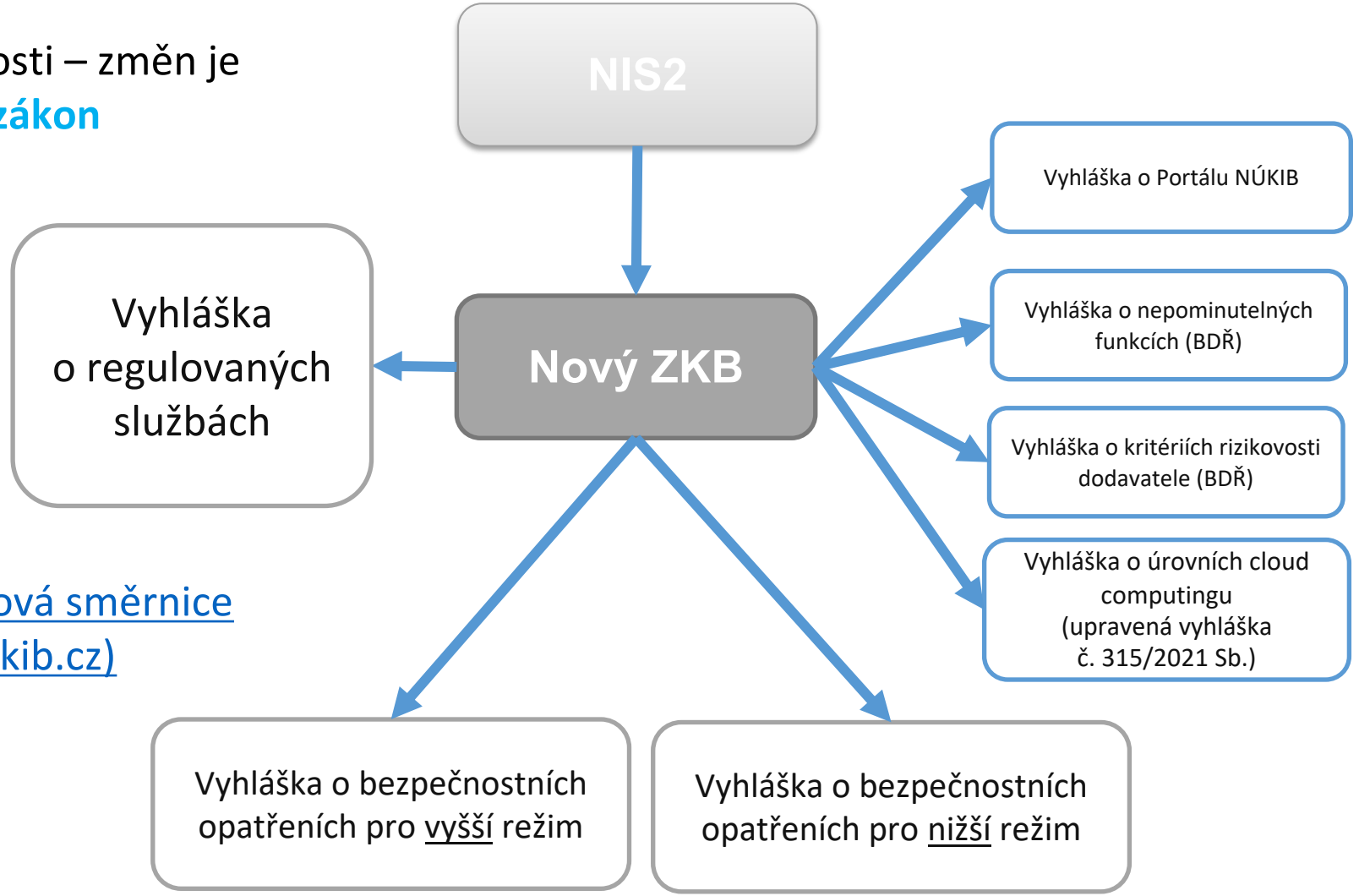
Nový zákon o kybernetické bezpečnosti (NZKB) v MPŘ

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

= zcela nová úprava – cca 70 paragrafů

Verze v mez. připomínkovém řízení má aktuálně navíc **7 vyhlášek.**

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



Nový ZKB – hlavní body

Nový zákon dopadne na minimálně 6 000 organizací

- jde téměř výhradně o požadavek směrnice
- reguluje přes **105 služeb v 18 odvětvích** (energetika, zdravotnictví, bankovnictví, doprava, veřejná správa, digitální infrastruktura,…)
- hlavním kritériem pro zahrnutí do regulace je **velikost subjektu** (daná počtem zaměstnanců nebo jeho finanční situací)
- mění se také přístup k rozsahu regulace – **nevybírají se konkrétní systémy, ale celé služby**
- do regulace se nově navrhuje **zařadit obce**

Regulované organizace zákon nově označuje jako tzv. poskytovatele regulované služby a rozděluje je do dvou režimů – nižších povinností a vyšších povinností

- podle režimu mají stanovené povinnosti

Vznikají úplně nové instituty

- zajištění dostupnosti regulované služby nebo mechanismus prověřování bezpečnosti dodavatelského řetězce

Mění se některé stávající instituty

- stav kybernetického nebezpečí, (proti)opatření, konkrétní lhůty pro hlášení incidentů, sankce,…

Nový ZKB – shrnutí povinností

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** – podle režimu v kterém je služba určena (vyšší/nižší)
- **informovat zákazníky** o incidentech a hrozbách
- **provádět protiopatření**
- **plnit povinnosti z tzv. Mechanismu bezpečnosti dodavatelského řetězce** u vybraných (strategicky významných) služeb
- **zajistit dostupnost z České republiky** u vybraných (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

Mechanismus bezpečnosti dodavatelského řetězce

Nová oblast, nevyplývá ze směrnice NIS2, ale z národního rozhodnutí

- platí **pouze pro vybrané organizace v režimu vyšších povinností (a to nikoli všech)**
- organizace v rámci této povinnosti **musí nahlásit dodavatele**
- **budou prověřováni dodavatelé do kritické části systému** = aktiva s hodnotou 3 a 4 (vysoká/kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu
- **stát prověří to, zda dodavatel není hrozbou pro bezpečnost ČR, zájmy ČR, vnitřní a veřejnou bezpečnost**
  - NÚKIB k tomu vyžaduje informace a součinnost řady orgánů (PČR, SLUŽBY, FAU, NSZ, MPO, MV, NBÚ, ÚOHS…)
- **NÚKIB může vydat zákaz dodavatele použít nebo upozornění na riziko** (je řešitelné bezpečnostním opatřením)
- **lze udělit výjimku** (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu apod.)
  - k vyřazení již dodaných technologií nemusí dojít hned – **počítá se s přechodnými lhůtami**
- hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby

Cíl mechanismu = stát musí mít mechanismus jak řešit závislost nedůvěryhodných dodavatelích z důvodů zachování suverenity

Zajištění dostupnosti regulovaných služeb

Návrh zajištění dostupnosti

- **poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu ve stanoveném čase a kvalitě z území České republiky**
- poskytovatel strategicky významné služby je povinen **prověřovat schopnost zajištění poskytování z České republiky nejméně jednou za dva roky**
- přechodná lhůta jeden rok od určení
- **stanovený čas a kvalitu a nezbytný rozsah služby stanoví poskytovatel regulované služby**

Východiska návrhu

- zajištění dostupnosti směruje na službu, nikoli nutně na její dílčí aktiva (a už vůbec ne na všechna)
- zajištění dostupnosti služby je možné i mimo kyberprostor
- kvalita služby může být snížena – míru snížení si definuje sám poskytovatel v BCM
- úroveň služby může být snížena – míru snížení si definuje sám poskytovatel v BCM
- rozsah služby může je dle připomínek subjektů nutno omezit/definovat, aby byla právní jistota

Cíl zajištění dostupnosti = kritické služby musíme být schopni zajistit alespoň omezeně z České republiky, abychom byli připraveni na mimořádné situace v zahraničí

Komunikace návrhů a zapojení veřejnosti

V srpnu 2022 spuštěn **informační web věnovaný směrnici NIS2 a nové regulaci**

Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)*

Představení problematiky na desítkách konferencí a bilaterálních jednání se zástupci úřadů a soukromého sektoru

Osloveno a komunikováno **s více než 28 svazy, oborovými sdruženími a komorami**

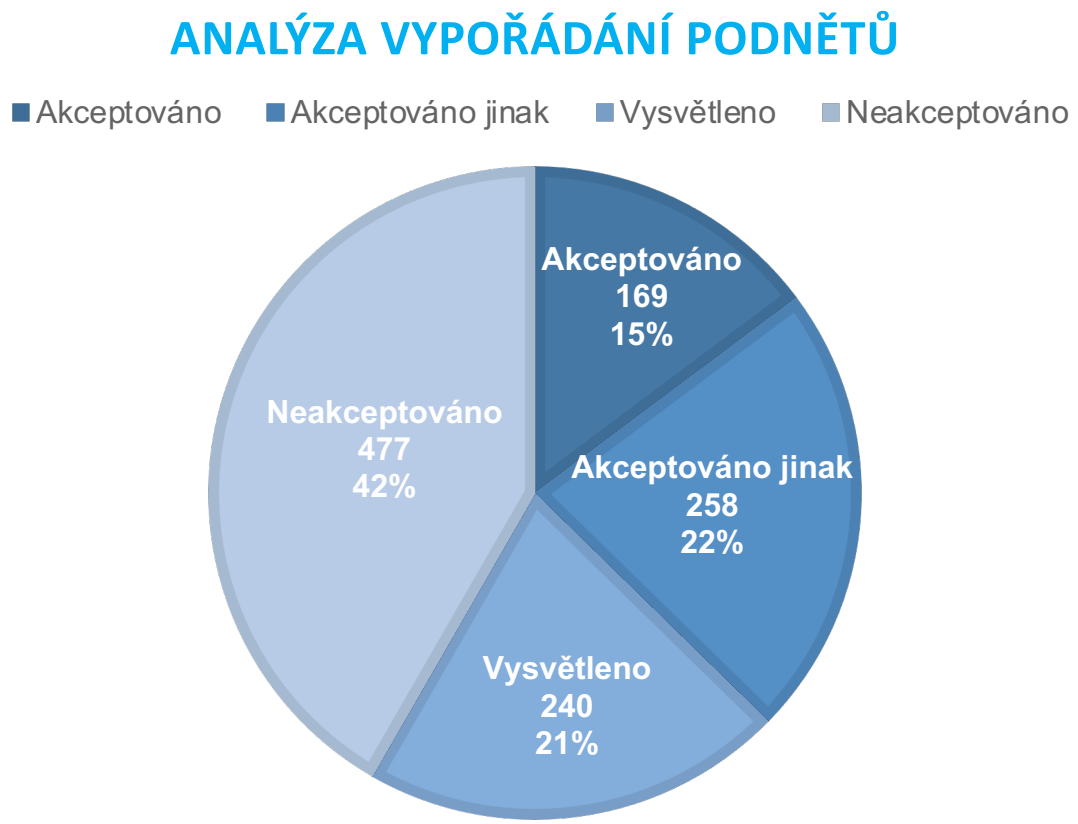
Provedena veřejná konzultace a připomínkování návrhů ze strany veřejnosti

- 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)

* na webu je přes 270 000 přístupů

Veřejné konzultace

V rámci veřejných konzultací bylo od 26. ledna do 12. března **zasláno 1144 podnětů od odborné veřejnosti, soukromého sektoru i veřejné správy**



- **Akceptováno** – podnět byl zapracován do návrhu zákona či doprovodných dokumentů (RIA, důvodová zpráva, návrhy vyhlášek);
- **Akceptováno jinak** – podnět byl v návrhu zákona či doprovodných dokumentech zohledněn jinak;
- **Vysvětleno** – podnět byl shledán spíše jako dotaz nebo konstatování, tudíž byl vysvětlen či okomentován;
- **Neakceptováno** – podnět nebylo možné zapracovat do návrhu zákona či doprovodných materiálů.

Veřejné konzultace – hlavní změny

- Formulační změny, zpřehlednění a zpřesnění textu
- Nastavení inspektorů → **zrušení institutu inspektorů**
- Obsah vyhlášky o bezpečnostních opatřeních pro režim nižších povinností

  → **zeštíhlení, zjednodušení – do MPŘ byla následně předložena zcela přepracovaná verze**
- Lokalizace informací a dat při zpracování v zahraničí → **zcela přepracováno, nově zajištění dostupnosti strategicky významných služeb z České republiky**
- Určovací a identifikační kritéria ve vyhlášce → **přesun určovacích kritérií, určení změny režimu do zákona a výčet odvětví pro identifikaci přímo v zákoně**
- Zákon rozdělen na dva → **hlavní zákon a změnový zákon (měnící jiné předpisy)**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce
- Stav kybernetického nebezpečí → **koncepční změny, provázání s krizovým řízením**

Meziresortní připomínkové řízení

Oficiální meziresortní připomínkové řízení bylo zahájeno 19. června 2023 a ukončeno 26. července 2023
(původní lhůta na připomínky stanovená do 19. července byla prodloužena)

NÚKIB obdržel vyšší stovky připomínek

- připomínky zaslalo **41 řádných připomínkových míst**
- dalších **11 organizací zaslalo své připomínky i bez toho, aby byli osloveni** (ale jejich připomínky byly také přijaty a řešeny)

Písemné návrhy vypořádání připomínek budou rozesílány v průběhu září

Nejčastější připomínkované oblasti

- legislativně-technické úpravy, obsah doprovodných materiálů, definice apod.
- mechanismus bezpečnosti dodavatelského řetězce a zajištění dostupnosti strategicky významné služby
- nastavení vztahu zákon – vyhlášky
- pravomoci Úřadu a Národního CERT
- stav kybernetického nebezpečí

Dílčí vyhodnocení připomínek v MPŘ

Definice

- připomínkovány některé definice (např. aktiva, významný dopad/hrozba/incident), požadováno doplnění dalších definic

Kritéria regulované služby

- nastavení vztahu zákon – určovací vyhláška, je podle některých připomínek protiústavní
- jinými slovy – zákon dostatečně nevymezuje některé instituty a nechává to na vyhláškách
- požadavky na neregulování některých služeb – např. obcí III. typu nebo vědeckých institucí

Rozsah a evidence aktiv

- nesouhlas s požadavkem evidovat všechna primární aktiva

Kontaktní údaje a incidenty

- požadavek na to, aby vyšší režim nehlásil všechny incidenty, požadavek na prodloužení lhůty pro hlášení z 24 na 72 hodin

(Proti)opatření

- dílčí připomínky k reaktivnímu protiopatření nebo např. požadavek, aby institut varování nebyl

Dílčí vyhodnocení připomínek v MPŘ

Mechanismus prověřování bezpečnosti dodavatelského řetězce

- požadavky na zrušení institutu
- nedostatečné vyhodnocení nákladů
- nedostatečně projednáno
- kompenzace – stát by měl platit náhrady
- přechodné lhůty – mají být delší
- zapojení sektorových regulátorů
- měla by to dělat vláda
- zúžení rozsahu dotčených aktiv – jen core, transportní a přístupové vrstvy ne
- pevné stanovení hloubky dodavatelského řetězce, který se bude prověřovat

Zajištění dostupnost strategicky významné služby

- nejasnosti ohledně toho kterých služeb se to týká
- obavy ohledně využívání cloudu

Projednávání mechanismu – časová osa

Červen 2022 – Listopad 2022

- Konference výboru pro bezpečnost *"Bezpečnost dodavatelského řetězce v sítích elektronických komunikací a další strategické infrastruktuře ČR"*
- Seminář *„Výstavba telekomunikačních sítí"*
- AKI summit 2022
- Konference CEVRO Institut

Prosinec 2022

- Seminář NÚKIB k bezpečnosti dodavatelského řetězce

Duben 2023

- Ministerstvo financí, ČAEK

Květen 2023

- UK Embassy – za účasti zástupců soukromého sektoru
- Svaz průmyslu a dopravy, Hospodářská komora ČR

Červen 2023

- NSS – jednání s předsedou Nejvyššího správního soudu

V průběhu roku 2023 řadě jednání na úrovni Hospodářské komory České republiky, Svazu průmyslu a dopravy a dalších.

Dílčí vyhodnocení připomínek v MPŘ

Přestupky a další sankce

- vyvratitelná domněnka společenské škodlivosti
- vynětí územních samosprávných celků ze sankcí
- snížení pokut státní správě

Zabezpečení ISVS podle vyhlášky o nižším režimu

Financování

Legislativní připomínky

- doplnění důvodových zpráv
- formální úpravy
- zmocnění k vyhláškám

Stav kybernetického nebezpečí

- zejména otázky stran návaznosti na krizové stavy

Dílčí vyhodnocení připomínek v MPŘ

Nedostatečné vyčíslení nákladů

NÚKIB se snažil náklady vyčíslit (i historicky), naráží to však na problémy

- nejednotná výchozí úroveň zabezpečení
- diametrální odlišnosti v architektuře, rozsahu i složitosti systémů
- složité vymezení, co vše do nákladů počítat

I přes to se NÚKIB opět snažil náklady vyčíslit – vytvořena metodika a dotazník a zrealizováno šetření

- metodika vycházela z obdobných metodik v minulosti, z legislativních pravidel, Metodiky měření administrativní zátěže podnikatelů (MPO) a dalších zdrojů
- stanoven poměrně jednoduchý dotazník a návod jak do vyplnit
- ještě před realizací průzkumu diskutováno a připomínkováno ze strany jednoho z ministerstev, Svazu měst a obcí ČR a Svazu průmyslu a dopravy
- skrze tyto organizace také proběhla distribuce finálního dotazníku

Úřadu se vrátilo 13 dotazníků z čehož bylo – 0 obcí, 1 velký podnik, 12 zaslalo jedno z ministerstev a jeho podřízené organizace

Nový ZKB – další předpokládané kroky

Mezirezortní připomínkové řízení (MPŘ) – červenec až září 2023

- aktuálně probíhá

Legislativní rada vlády – říjen až prosinec 2023

Poslanecká sněmovna, Senát, prezident – začátek roku 2024

Vydání zákona říjen 2024 (konec transpoziční lhůty)

Vyhlášky budou mít samostatný legislativní proces, který bude spuštěn v roce 2024

Děkuji za pozornost

regulace@nukib.cz