Mechanismus prověřování bezpečnosti dodavatelského řetězce (BDŘ)

Součást návrhu novely zákona o kybernetické bezpečnosti
ve stavu k 12. dubna 2023

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

12. Dubna 2023, Praha

TLP:CLEAR

Oddělení národních strategií a politik a
Odbor regulace

Co je mechanismus prověřování BDŘ?

Vnitrostátní systém **vyhodnocování a omezování rizikových dodavatelů ICT** do strategicky nejvýznamnější infrastruktury státu.

Mechanismus prověřování BDŘ přinese zejména:

- posílení informovanosti povinných osob a státu o dodavatelích
- možnost státu omezit využití nejrizikovějších dodavatelů

O přípravě mechanismu do podoby zákona rozhodla BRS v červnu 2022, problematikou BDŘ se stát ale zabývá již několik let.

Omezení rizikových dodavatelů ale **nedopadnou na všechny** a **neznamenají okamžitou výměny** infrastruktury!

Upozornění

Podoba mechanismu prověřování BDŘ představená v této prezentaci odpovídá návrhu zákona po neformální veřejné konzultaci dle stavu k 12. dubnu 2023.

Výsledná podoba nebo podmínky, za jakých bude mechanismus zaveden, nemusí obsahu této prezentace odpovídat.

Proč je mechanismus prověřování BDŘ součástí ZKB?

Společný předmět regulace

- **bezpečnost** (důvěrnost, dostupnost, integrita)
  nejvýznamnější ICT infrastruktury státu a veřejných služeb

Společná dotčená infrastruktura

- **povinné subjekty** a aktiva mechanismu prověřování BDŘ jsou
  podmnožinou regulace ZKB

Společné prostředky a informace

- **totožné instituty** (technické a programové prostředky, varování, řízení aktiv, řízení dodavatelů aj.)
- **totožné či související informace** (poznatky o KBI, prověřování dodavatelů CC, monitoring a analýza KB rizik a hrozeb aj.)

Souvislost mechanismu prověřování BDŘ s NIS2

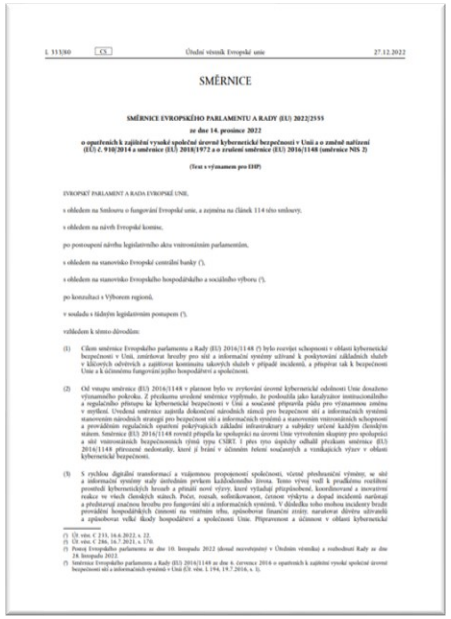
Mechanismus i transpozice NIS2 budou součástí **nového zákona o kybernetické bezpečnosti**.

Hlavní společné oblasti úpravy

- Proces určování povinných osob
- Vymezení regulovaných služeb
- Zavádění bezpečnostních opatření a protiopatření
- Kontrola

Zmocnění dle čl. 22 NIS2 nesouvisí s vnitrostátním mechanismem, ale míří k podobnému cíli.

Požadavek zavést **NIS2** vychází **z práva EU**.



SMĚRNICE

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555

ze dne 14. prosince 2022

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

(Text s významem pro EHP)

USNESENÍ
BEZPEČNOSTNÍ RADY STÁTU
ze dne 21. června 2022 č. 41

k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu

Bezpečnostní rada státu

I. **bere na vědomí** materiál „Bezpečnost dodavatelských řetězců strategické infrastruktury státu", č. j. 28261/2022-UVCR;

II. **vybírá** přístup A – Prověřování dodavatelů dle aktuální bezpečnostní situace z materiálu uvedeného v bodě I tohoto usnesení k dalšímu rozpracování do podoby návrhu zákona;

III. **ukládá** řediteli Národního úřadu pro kybernetickou a informační bezpečnost, aby předložil vládě prostřednictvím předsedy vlády a předsedy Bezpečnostní rady státu do 31. května 2023 návrh zákona zpracovaný na základě bodu II tohoto usnesení, který bude předložen namísto věcného záměru zákona o posuzování bezpečnostní spolehlivosti dodavatelů do strategicky významné infrastruktury elektronických komunikací zařazeného do Plánu legislativních prací vlády na zbývající část roku 2022 na základě usnesení Bezpečnostní rady státu ze dne 19. října 2021 č. 33;

IV. **zrušuje** bod II usnesení Bezpečnostní rady státu ze dne 19. října 2021 č. 33.

Provedou:
předseda vlády a předseda Bezpečnostní rady státu,
ředitel Národního úřadu pro kybernetickou a informační bezpečnost

prof. PhDr. Petr Fiala, Ph.D., LL.M. v. r.
předseda vlády
a předseda Bezpečnostní rady státu

Požadavek zavést **mechanismus prověřování BDŘ** vychází **z vnitrostátního politického rozhodnutí**.

Na koho mechanismus prověřování BDŘ dopadne?

Strategicky významné služby a jejich **poskytovatelé**

- infrastruktura s největším dopadem na veřejné služby a závislostí na ICT
- vychází především z kritické informační infrastruktury (KII) a poskytovatelů základní služby (PZS)
- jde o podmnožinu PRS v režimu vyšších povinností – **cca 150 subjektů**

Služby v odvětvích:

- veřejná správa
- energetika
- doprava
- digitální infrastruktura a služby
- další v případě možnosti závažného dopadu na bezpečnost České republiky nebo vnitřní či veřejný pořádek

Na koho mechanismus prověřování BDŘ dopadne?

Regulované služby dotčené mechanismem prověřování BDŘ

Veřejná správa

- výkon svěřených pravomocí
  (ústřední orgány státní správy, správní úřady s celostátní působností, ČNB aj.)

Energetika – elektřina

- výroba elektřiny
  (výrobna s instalovaným výkonem od 100 MW)
- provoz přenosové soustavy elektřiny
- provoz distribuční soustavy elektřiny
  (kapacita nejméně 220 MW)

Energetika – ropa a ropné produkty

- provoz ropovodu
- provoz produktovodu

Energetika – plynárenství

- provoz přepravní soustavy plynu
- provoz distribuční soustavy plynu

Letecká doprava

- řízení letového provozu nad vzdušným prostorem České republiky
- letové navigační služby
  (s působností v celé ČR)

Drážní doprava

- stavění vlakových cest na celostátní úrovni

Digitální infrastruktura a služby

- poskytování veřejně dostupné služby elektronických komunikací
  (operátoři s nejméně 350 000 aktivními SIM na maloobchodním trhu nebo 100 000 aktivními pevnými internetovými přípojkami v ČR)
- zajišťování veřejné komunikační sítě elektronických komunikací
  (operátoři s nejméně 350 000 aktivními SIM na maloobchodním trhu nebo 100 000 aktivními pevnými internetovými přípojkami v ČR)
- správa a provoz registru internetových domén nejvyšší úrovně
- poskytování služby cloud computingu
  (poskytovatel státního cloud computingu)

Na koho mechanismus prověřování BDŘ dopadne?

NIS2:

Okruh odvětví regulovaných NIS2 je uveden v přílohách I a II.

- Směrnicí je regulováno cca 60 služeb v 18 odvětvích.
- Nové služby v regulaci ZKB dle NIS2.

BDŘ:

Vybrané služby + konkrétní kritéria.

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 poskytovatele 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 stavění vlakových cest

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.

Úkoly státu a povinných osob

Na straně povinných osob:

- **určit kritickou část stanoveného rozsahu** (vysoká a kritická aktiva + aktiva zajišťující nepominutelné funkce)
- **s přiměřeným úsilím zjišťovat informace o dodavatelích** bezpečnostně významných dodávek
- **informovat o dodavatelích NÚKIB**
- **respektovat varování a přímé omezení rizikových dodavatelů**

Na straně státu:

- vést evidenci dodavatelů
- zjišťovat informace vlastními prostředky
- prověřovat konkrétní dodavatele
- vydávat varování a omezovat rizikové dodavatele
- kontrolovat plnění povinností

Krok č. 1 mechanismu: Zjištění a vyhodnocení hrozby

Prověřováni budou **současní** a **potenciální dodavatelé** bezpečnostně významných dodávek.

Zjišťována bude

- **kybernetická hrozba spojená s dodavatelem**
- **ohrožení bezpečnosti ČR obecně**
- **ohrožení vnitřního či veřejného pořádku**

ve spojení s dodavatelem a **v důsledku naplnění kritérií rizikovosti dodavatele**.

Jde o činnost na straně státu bez přímého dopadu na poskytovatele služeb nebo dodavatele – ten má až možné následné omezení.

Krok č. 2 mechanismu: Omezení rizikového dodavatele

V závislosti na zjištěních z prověřování NÚKIB:

- nekoná nic
- vydá **varování o kybernetické hrozbě nebo zranitelnosti spojené s dodavatelem**
- vydá **opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele**
- případně koná jinak dle zákona

Omezení podrobně: forma opatření obecné povahy

Opatření obecné povahy

- před zveřejněním **orgány státu projednají návrh** OOP
- zveřejněný návrh OOP mohou **připomínkovat dotčené osoby** (tzn. povinné osoby i dotčení dodavatelé)
- s přihlédnutím k **životnímu cyklu investice** stanoví OOP **přiměřenou lhůtu** k zavedení povinností
- omezení zavádí **poskytovatelé strategicky významných služeb** pouze ve vztahu k **bezpečnostně významným dodávkám** dodavatele označeného v OOP
- z omezení je možné udělit v samostatném řízení zahájeném na žádost nebo z moci úřední **výjimku**
- **proti OOP lze uplatnit podnět k přezkumu nebo správní žalobu**

Odhadovaný harmonogram

Klíčové fáze	Začátek	Konec
Zadání úkolu BRS	21. červen 2022	
Příprava návrhu	červen 2022	leden 2023
Konzultace návrhu se státem	listopad 2022	leden 2023
Konzultace návrhu s širokou veřejností	26. leden 2023	12. březen 2023
Zapracování podnětů a finalizace návrhu	13. březen 2023	květen 2023
MPŘ + vypořádání	květen 2023	Q3 2023
Legislativní proces	Q3 2023	Q3 2024
Účinnost a možné zahájení prověřování	Q4 2024	
První povinnosti hlášení dodavatelů	Q4 2025	

Děkujeme za pozornost!

Oddělení národních strategií a politik a

Odbor regulace (regulace@nukib.cz)