# Doporučení NÚKIB pro výběr dodavatelů do telekomunikačních sítí

# v souvislosti s připravovanou směrnicí NIS 2

Ondřej Malý

5. 5. 2022

# DOPORUČENÍ NÚKIB

- „Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí“
- Cíl: představit odvětví:
  - pohled NÚKIB a dalších vybraných institucí na základní východiska posuzování důvěryhodnosti dodavatelů technologií do 5G sítí,
  - kritéria, která mohou přispět k výběru důvěryhodných dodavatelů:
    - **strategická**
    - obchodní
    - technická

# DŮVĚRYHODNOST DODAVATELŮ DLE NÚKIB - obecně

Co ovlivňuje dle NÚKIB a dalších úřadů „důvěryhodnost dodavatelů:

- **sídlo ve státech**:
  - které mají demokraticky volenou vládu (nezávislá opozice, svobodné volby, fungující princip tzv. brzd a protivah)
  - které mají nezávislý soudní systém
  - jejichž právní předpisy a veřejné politiky se řídí zásadami právního státu
  - dbají na ochranu duševního vlastnictví; dlouhodobě či systematicky neporušují mezinárodní právo
  - nevymezují se proti nim mezinárodní a nadnárodní organizace či aliance, kterých je ČR členem (rezoluce RB OSN/omezující opatření EU)
  - udržují s ČR partnerské vztahy a neprovádí činnosti, které jdou proti základním zájmům ČR nebo jejích spojenců; nepovažují ČR za nepřátelský stát,

# DŮVĚRYHODNOST DODAVATELŮ DLE NÚKIB - obecně

Co ovlivňuje dle NÚKIB a dalších úřadů „důvěryhodnost dodavatelů:

- **není nepatřičně ovlivňován zahraniční vládou či orgánem státní správy** a je s dostatečnou mírou autonomie schopen zajišťovat dostupnost, integritu a důvěryhodnost dat v dodaných technologických řešeních,
- sleduje obchodní cíle, podniká v souladu se zvyklostmi mezinárodního obchodu a nepožívá od státu, v němž má sídlo nebo pod jehož vliv spadá, nepřiměřených výhod (např. státní podporu významně narušující hospodářskou soutěž),
- **naplňuje bezpečnostní standardy,** které jsou v době realizace dodávky na trhu běžné, a je ochoten zavázat se k jejich naplňování i do budoucna.

Výše uvedená východiska nejsou zamýšlena k použití jako kritéria pro hodnocení důvěryhodnosti dodavatelů pro operátory.

# STRATEGICKÁ KRITÉRIA

- **Strategická kritéria zvyšující důvěryhodnost dodavatele jsou zejména:**
  - Dodavatel a jeho ovládající osoby mají **sídlo v členském státě EU či NATO**.
  - Dodavatel má **sídlo ve státě, resp. podléhá pouze právním řádům států, které jsou smluvními stranami mezinárodních smluv o kybernetické bezpečnosti**, mají s ČR platné dohody o spolupráci v oblasti bezpečnosti či podobná ujednání nebo se na ně taková pravidla vztahují. Jedná se zejména o:
    - členské státy EU a státy zajišťující odpovídající ochranu osobních údajů ve smyslu čl. 45 GDPR,
    - státy, které jsou smluvní stranou některé ze smluv o výměně a vzájemné ochraně utajovaných informací s ČR,
    - státy, které jsou smluvní stranou Dohody o vládních zakázkách, či
    - státy, které jsou smluvní stranou tzv. Budapešťské úmluvy o počítačové kriminalitě.
  - Dodavatel má sídlo ve státě, resp. **podléhá pouze právním řádům států, na které veřejně neupozorňují bezpečnostní instituce České republiky** v souvislosti s prováděním zpravodajských či jiných operací, poškozujících zájmy České republiky nebo členských států EU či NATO.
  - Dodavatel je **ochoten zavázat se prohlášením**, že je právně i fakticky schopen odmítnout sdělení či zpřístupnění důvěrných informací od svých zákazníků nebo o svých zákaznících třetím stranám; v případě zákonné informační povinnosti odkazuje dodavatel na příslušná ustanovení v právních předpisech.

# STRATEGICKÁ OPATŘENÍ

- Strategická opatření navazují na sadu opatření EU 5G Toolbox

- Strategické opatření č. 3 (SM03) EU 5G Toolboxu stanovuje, aby členské státy EU přijaly rámec pro hodnocení rizikového profilu relevantních dodavatelů na národní úrovni nebo společně s dalšími členskými státy.

- **Na národní úrovni již probíhají práce na vytvoření mechanismu pro prověřování a hodnocení rizikových dodavatelů – lze předpokládat, že i tento bude rovněž reflektovat strategická kritéria.**

# NÁVRH SMĚRNICE NIS 2

- Cílem NIS 2 je:
  - rozšíření oblasti působnosti aktuálně platné a účinné směrnice NIS s ohledem na rychlou digitální transformaci společnosti,
  - zlepšení odolnosti a schopnosti veřejných i soukromých subjektů a EU jako celku reagovat na incidenty v oblasti kybernetické bezpečnosti,
  - zlepšení kybernetické bezpečnosti v EU a její sjednocení napříč EU.

- Návrh směrnice NIS 2 mají doplnit také nová směrnice o posílení odolnosti kritických subjektů (směrnice CER) a nařízení o digitální provozní odolnosti finančního sektoru (nařízení DORA).

# ZMĚNY PŘINÁŠENÉ NIS 2

- Významné rozšíření okruhu subjektů, na které se bude směrnice NIS 2 vztahovat

- Opuštění dělení subjektů na provozovatele základních služeb a poskytovatele digitálních služeb => **nově subjekty děleny na <u>základní a důležité</u>**, a to v návaznosti na kritickou důležitost daného odvětví/služby a úroveň závislosti jiných odvětví/služeb na daném odvětví

- Nově přidáno **kritérium velikosti subjektu** - do působnosti NIS 2 budou zahrnuty
  - **<u>všechny střední a velké podniky ve vybraných odvětvích dle NIS 2</u>**
  - **<u>malé podniky a mikropodniky spadající pod čl. 2 odst. 2 návrhu směrnice NIS 2</u>**
    - zejm. subjekty plnící klíčovou úlohu pro hospodářství či společnost, nebo pro konkrétní odvětví či druhy služeb (např. **veřejné sítě elektronických komunikací**, orgány veřejné správy apod.)

# KRITÉRIUM VELIKOSTI PODNIKU

- Velikost podniku pro  účely NIS 2 bude stanovena ve smyslu doporučení Komise 2003/361/ES, které stanovuje kritéria pro určení velikosti podniku:

  - **mikropodnik** – má méně než 10 zaměstnanců a roční obrat (finanční částka získaná za určité období) nebo rozvahu (výkaz aktiv a pasiv společnosti) do 2.000.000 EUR,
  - **malý podnik** – má méně než 50 zaměstnanců a roční obrat nebo rozvahu do 10.000.000 EUR,
  - **střední podnik** – má méně než 250 zaměstnanců a roční obrat do 50.000.000 milionů EUR nebo rozvahu do 43.000.000 EUR.

# ZÁKLADNÍ SUBJEKTY – ODVĚTVÍ JIŽ ZAHRNUTÁ V NIS

Základní subjekty a odvětví, která jsou již nyní řazena mezi provozovatele základních služeb dle NIS:

- energetika (elektřina, ropa, zemní plyn),
- doprava (letecká, železniční, vodní, silniční),
- bankovnictví (úvěrové instituce),
- infrastruktura finančních trhů,
- zdravotnictví (zdravotnická zařízení, včetně nemocnic a soukromých klinik),
- dodávky a rozvody pitné vody (dodavatelé a distributoři),
- digitální infrastruktura (výměnné uzly internetu (IXP), poskytovatelé služeb systému doménových jmen (DNS), registry internetových domén nejvyšší úrovně (TLD).

# ZÁKLADNÍ SUBJEKTY - NOVĚ POVINNÉ SUBJEKTY

- v odvětví digitální infrastruktury nově také poskytovatelé služeb **cloud computingu**, **služeb datových center**, **sítí pro doručování obsahu**, **služeb vytvářejících důvěru**, **veřejných sítí elektronických komunikací**, **služeb elektronických komunikací** (jsou-li jejich služby veřejně dostupné),
- v odvětví veřejné správy (ústřední subjekty veřejné správy, orgány samosprávy),

# DŮLEŽITÉ SUBJETKY - ODVĚTVÍ

- **výroba** (zdravotnických prostředků a diagnostických zdravotnických prostředků in vitro; **počítačů, elektronických a optických přístrojů a zařízení; elektrických zařízení**; strojů a zařízení j.n. (tj. strojů a zařízení, které mechanicky nebo tepelně působí na materiály nebo na materiálech provádějí výrobní procesy); motorových vozidel; přívěsů a návěsů a ostatních dopravních prostředků a zařízení),
- **digitální služby** (poskytovatelé online tržišť, internetových vyhledávačů a platforem služeb sociálních sítí).

# DALŠÍ ZMĚNY PŘINÁŠENÉ NIS 2

Nová **bezpečnostní opatření a hodnocení rizik**

- povinnost základních subjektů přijmout vhodná a přiměřená a odpovídající **technická a organizační opatření k řízení bezpečnostních rizik**
- součástí opatření i **posouzení a řízení bezpečnostních rizik vyplývajících z dodavatelských řetězců a dodavatelských vztahů**, a to s přihlédnutím jak k technickým, tak netechnickým faktorům
  - hodnocení rizik by měla reflektovat technické a příp. i netechnické faktory včetně faktorů vymezených v doporučení EU „Kybernetická bezpečnost 5G“, v koordinovaném posouzení rizik pro bezpečnost sítí 5G v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G (EU 5G Toolbox)
- Možnost provést koordinované posouzení rizik dodavatelských řetězců
  - provádí jej Skupina pro spolupráci v součinnosti s Komisí a agenturou ENISA u specifických kritických služeb, systémů nebo produktů ICT,
  - zohlednění technických, případně netechnických rizikových faktorů.

# OPATŘENÍ K ŘÍZENÍ RIZIK

- Opatření k řízení rizik v oblasti kybernetické bezpečnosti mají v souladu s čl. 18 NIS 2 zahrnovat alespoň následující aspekty:
  - ***analýzu rizik*** *a politiku bezpečnosti informačních systémů*
  - *řešení incidentů (prevence a odhalování incidentů a reakce na ně);*
  - *řízení kontinuity provozu a krizové řízení;*
  - ***zabezpečení dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho dodavateli nebo poskytovateli služeb, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo řízených bezpečnostních služeb****;*
  - *zabezpečení pořizování, vývoje a údržby sítě a informačních systémů, včetně zveřejňování informací o zranitelnostech a jejich řešení;*
  - *politiky a postupy (testování a audit) za účelem posouzení účelnosti opatření k řízení rizik v oblasti kybernetické bezpečnosti;*
  - *používání kryptografie a šifrování.*

# DALŠÍ ZMĚNY PŘINÁŠENÉ NIS 2

- Přesnější ustanovení o postupu **oznamování incidentů**
  - povinnost **neprodleně oznamovat každý incident**, **který má závažný dopad** na poskytování služeb dotčeného subjektu, i každou **významnou kybernetickou hrozbu, kterou tyto subjekty zjistí,** a která by mohla mít za následek významný incident, příslušným orgánům nebo týmu CSIRT (a ve vhodných případech i příjemcům svých služeb)
- Přísnější kontrolní opatření pro vnitrostátní orgány, přísnější požadavky na vymáhání povinností
- Zřízení Skupiny pro spolupráci
  - tvořena zástupci členských států, Komise a agentury ENISA
  - podpora a usnadnění strategické spolupráce a výměny informací mezi členskými státy

# ODPOVĚDNOST A SANKCE

- Bezpečnostní opatření nastavená dotčenými subjekty budou schvalovat jejich **vedoucí orgány**. Tyto také mají dohlížet na jejich uplatňování a **nést odpovědnost za neplnění povinností dotčeného subjektu vyplývajících z návrhu směrnice NIS 2.**

- **Za nedodržení některých pravidel stanovených směrnicí NIS 2** (zejm. přijetí opatření k řízení bezpečnostních rizik a plnění oznamovací povinnosti) má **hrozit pokuta ve výši minimálně 10.000.000 EUR (nebo 2% z celkového celosvětového ročního obratu podniku**, ke kterému patřil základní nebo důležitý subjekt v předchozím rozpočtovém roce – podle toho, co je vyšší).

# DĚKUJI ZA POZORNOST