Jak a zda vůbec ovlivní nový Zákon o kybernetické bezpečnosti podnikání malých a středních podniků?

Zákon o kybernetické bezpečnosti – návrh 1Q/2023

Jakub Rejzek

Výbor Nezávislého ICT průmyslu

Teze nového ZKB

- Současný, stále platný zákon dle NIS1 definuje základní infrastruktury-oborová kritéria

- Současná, stále platná vyhláška stanovuje objemová a dopadová kritéria
  = drtivou většinu MSP kritéria současné úpravy ZKB míjí, nejsou základní infrastrukturou.
- I současná regulace ale stanoví povinnost prověřovat důvěryhodnost dodavatelů a řídit rizika (§8 82/2018Sb.)

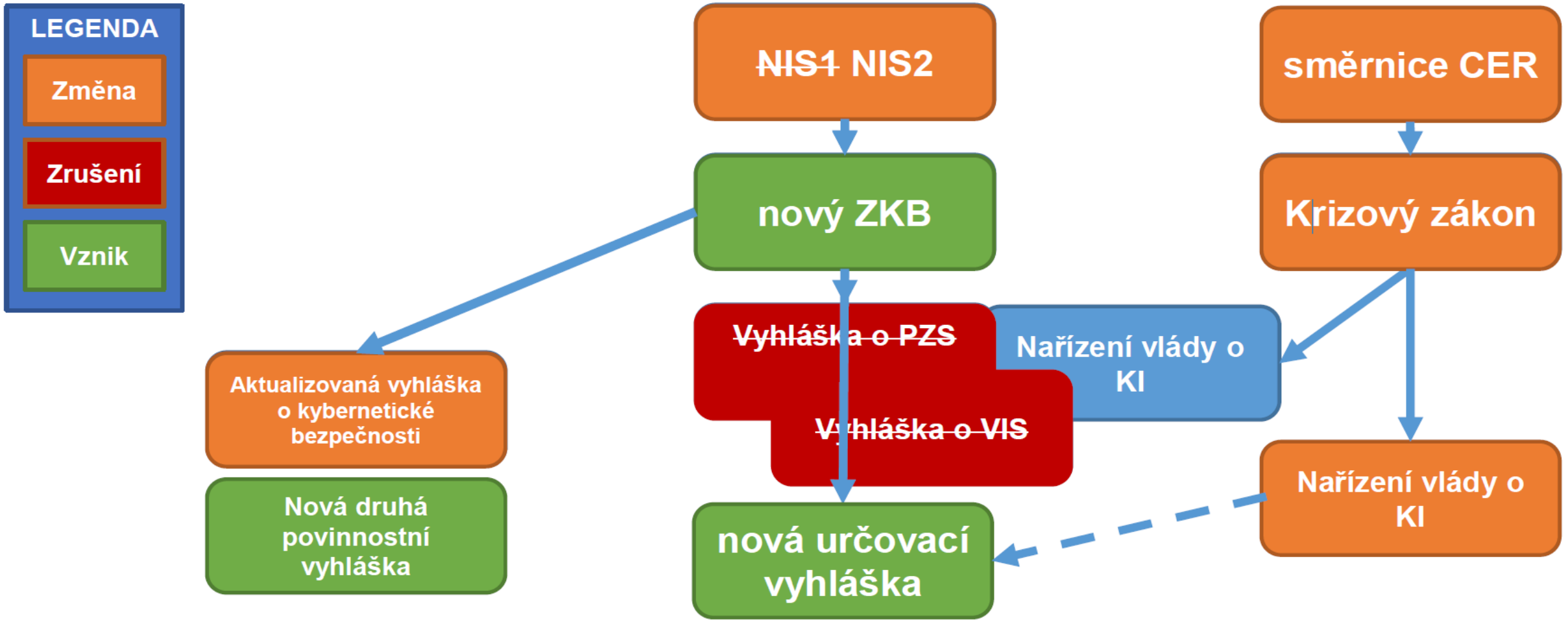
Nová Směrnice EU o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2, rozšiřuje oblast regulace. V ICT oborech jsou tak dotčení regulací všichni podnikatelé poskytující veřejně dostupné služby; odvětví „Digitální infrastruktury“.

- do odvětví digitální infrastruktury se nově řadí 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),

- nově se pod NIS2 řadí také subjekty v odvětví veřejné správy (ústřední subjekty veřejné správy, orgány samosprávy).

článek Jakub Rejzek - https://www.lupa.cz/clanky/provozovatelum-siti-a-it-sluzeb-se-nova-kyberbezpecnostni-regulace-nevyhne/

Teze nového ZKB



Výbor Nezávislého ICT průmyslu

NIS2 a Mechanismus

- Doporučení NUKIB pro hodnocení důvěryhodnosti dodavatelů a technologií do 5G sítí v ČR

Hlavní teze:

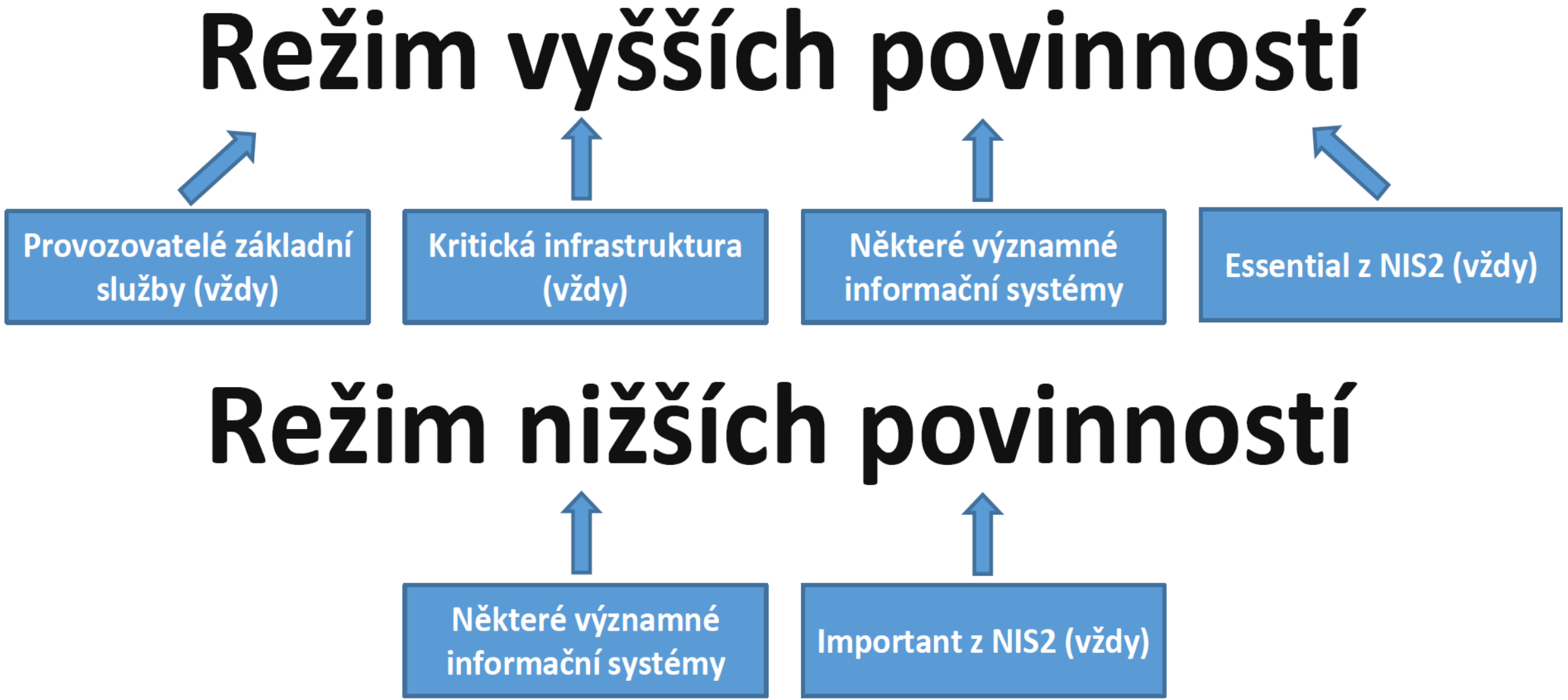
- Regulované subjekty budou rozdělené podle velikosti na dva režimy:
- Important and Essential (Režim nižších povinností a Režim Vyšších povinností)

Provozovatelé ~~Základní služby~~ (Strategické infrastruktury státu) - Speciální kategorie pro Mechanismus prověřování bezpečnosti dodavatelského řetězce.

- Dvě regulace v jednom návrhu zákona, týkající se stejné věci – BDŘ.
- NUKIB: Koordinované posouzení rizik dle čl. 22 NIS2, na které odkazovaný recitál 91 NIS2 míří, představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus prověřování bezpečnosti dodavatelských řetězců, obsažených v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces, hodnotící kritéria důležitá pro bezpečnost České republiky. Z tohoto důvodu se tyto dva systémy posuzování rizik, resp. hrozeb, procesně i co do kritérií posuzování liší.

- Aktuálně navrhované kritérium je 100 000 aktivních přípojek nebo 350 000 SIM karet pro BDŘ dle Mechanismu.

NIS2 a Mechanismus



Výbor Nezávislého ICT průmyslu

NIS2 a Mechanismus

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.

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

Základním kritériem pro posouzení velikosti podnikatele je počet zaměstnanců, velikost ročního obratu a bilanční suma roční rozvahy (velikost aktiv). Údaje, které se mají použít pro stanovení počtu zaměstnanců a finančních veličin, jsou údaje vztahující se k poslednímu uzavřenému zdaňovacímu období vypočtené za období jednoho kalendářního roku.

- Za **drobného, malého a středního podnikatele** se považuje podnikatel, který zaměstnává méně než 250 zaměstnanců a jeho roční obrat nepřesahuje 50 milionů EUR nebo jeho bilanční suma roční rozvahy nepřesahuje 43 milionů EUR.
- V rámci kategorie malých a středních podniků jsou **malé podniky** vymezeny jako podniky, které zaměstnávají méně než 50 osob a jejichž roční obrat nebo bilanční suma roční rozvahy nepřesahuje 10 milionů EUR.
- V rámci kategorie malých a středních podniků jsou **drobní podnikatelé** vymezeni jako podnikatelé, kteří zaměstnávají méně než 10 osob a jejichž roční obrat nebo bilanční suma roční rozvahy nepřesahuje 2 miliony EUR.

Výbor Nezávislého ICT průmyslu

Současná opatření pro posílení KB

- Doporučení NUKIB pro hodnocení důvěryhodnosti dodavatelů a technologií do 5G sítí v ČR

Hlavní teze:

- Vodítko pro dodávky informačních a komunikačních systémů KI v ČR.
  - vlastnická struktura
  - prokázat princip „Security by design“
  - účinná bezpečnostní pravidla a procesy

- Principy
  - strategická
  - obchodní
  - technicko-bezpečnostní

- Operátoři by podle doporučení měli například sledovat, zda je dohledatelná vlastnická struktura dodavatelské firmy, zda má sídlo ve státě s demokraticky volenou vládou a nezávislým soudním systémem, který dlouhodobě nebo systematicky neporušuje mezinárodní právo.

Hlavní body připomínky ZKB VNICPT

- Připomínky VNICTP k návrhu nového ZKB – odkaz

Hlavní teze:

- RIA je vysloveně nepochopení, kdo na trhu a jak vlastně podniká
- nejasně ohraničená část sítě pro Mechanismus
- příliš složité definice, sloučení kyberbezpečnosti s geopolitikou a z toho plynoucí zmatky pro MSP
- Mechanismus nastavený na hranici, kdy se vztahuje i na relativně velký počet subjektů a náklady na regulaci
- OOP jako nevhodný nástroj – viz. zkušenosti s přezkumem OOP u jiného regulátora
- OEM a generičtí výrobci
- problematika DNS
- problematika CDN a menší IPTV provideři
- dostatek nebo nedostatek dodavatelů… Co trápí menší viz Orange projekt Samsungu.
- mnoho dalších…

Náklady na regulaci

*„Náklady na dodržování regulace jsou nejen náklady vznikající podnikům i jiným stranám, na které je právní úprava zacílena, v souvislosti s přijímáním opatření nezbytných k dodržení požadavků právní úpravy, ale i administrativní zátěž a náklady veřejné správy související s vynucováním regulace.“**

*Zdroj: Metodika Vlády ČR pro měření celkových nákladů plnění povinností vyplývajících z regulace

Jaké povinnosti bude muset regulovaný subjekt plnit?

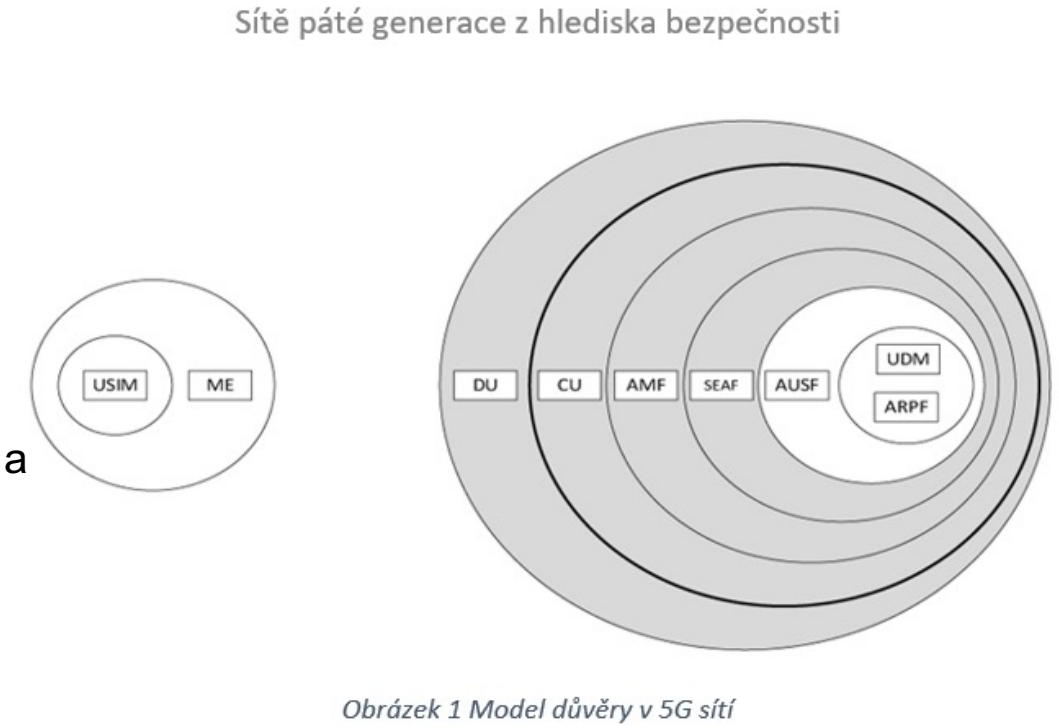
Povinný subjekt bude muset plnit dvě základní kategorie opatření; technické a netechnické. V první řadě je to povinnost přijmout vhodná a přiměřená odpovídající technická a organizační opatření k řízení bezpečnostních rizik. Opatření musí zahrnovat tyto základní aspekty:

- analýzu rizik a politiku bezpečnosti informačních systémů
- řešení incidentů včetně prevence a reakce na ně, opět technické i netechnické kategorie opatření
- řízení kontinuity provozu a krizové řízení; včetně například cvičení přechodu na nedigitální provoz v nouzovém režimu
- zabezpečení dodavatelského řetězce včetně bezpečnostních aspektů týkající se vztahů mezi subjekty, jeho dodavateli či poskytovateli služeb. Opět zde řešíme technické a netechnické aspekty
- zabezpečení pořizování, vývoje a údržby sítě a informačních systémů včetně zveřejňování informací o zranitelnostech a jejich řešení, myšleno především nadřízeným a odpovědným orgánům – v našem případě pravděpodobně NÚKIB nebo CSIRT
- vytvářet politiky a postupy, včetně auditů a penetračních testů s účelem posouzení účelnosti opatření řízení rizik KB
- subjekty budou povinny používat kryptografii a šifrování

Analýza bezpečnosti 5G sítí

[Článek LUPA.cz, Michal Poupa (ČVUT): 5G sítě mají daleko lepší zabezpečení nežli minulé generace. Analýza 5G sítí z pohledu bezpečnosti – odkaz.]

Pokud tak stát chce skutečně snížit jím vnímané riziko vyplývající z dodavatelského řetězce, ať to učiní proporčně problému a identifikuje kritické funkcionality v síti (které se v drtivé většině dotýkají citlivé části sítě, takzvaného jádra) a na nich poté provádí přísnější posuzování rizik včetně netechnických faktorů. Méně kritické části, jako je rádiová část, kde jsou rizika mizivá a snadno řiditelná, nechť nechá na operátorech a jejich volbě dodavatele. Tím zajistí “strategickou” bezpečnost, nevytvoří obludnou regulaci a ponechá většinu odpovědnosti na operátorech, kteří mají s bezpečností svých sítí desítky let zkušeností.



Obrázek 1 Model důvěry v 5G sítí

Výbor Nezávislého ICT průmyslu

Závěr

Obávat se jako investic do přístupové sítě nebo do rádiové části sítě, pokud jste MSP?

Není třeba, ale vždy zpracujte risk analýzy. Což tak jako tak odpovídá zdravému přístupu Zero Trust Policy.

Závěr

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
MPŘ + vypořádání	Q2 2023	Q3 2023
Legislativní proces	Q3 2023	Q3 2024
Účinnost a možné zahájení prověřování	Q4 2024	
První povinnosti hlášení dodavatelů	Q4 2025	

Děkuji Vám za pozornost.

Výbor nezávislého ICT průmyslu, z.s
jakub.rejzek@vnictp.cz