Zákon o kybernetické bezpečnosti – návrh 1Q/2023

Jakub Rejzek

Výbor Nezávislého ICT průmyslu

Hlavní body připomínky ZKB VNICPT

- Připomínky VNICTP k návrhu nového ZKB – odkaz

Hlavní teze:

- 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…

Výbor Nezávislého ICT průmyslu

Analýza bezpečnosti 5G sítí

- Stát má samozřejmě plné právo prověřovat, kteří dodavatelé jsou v kritické informační infrastruktuře a samozřejmě má plné právo prověřovat je z hlediska “netechnických” rizik, tedy posuzovat je vzhledem ke svým geopolitickým a zahraničněpolitickým zájmům.

- Zároveň jde ale o bezprecedentní regulaci, protože do nynějška byly odpovědní za kybernetickou bezpečnost obecně provozovatelé systému, nyní by stát stanovoval, jaké dodavatele není možné používat, protože to není v souladu se “strategickým” postojem státu. A to bez ohledu na to, jaká je struktura trhu a jaké to bude mít dopady na poskytování služeb. Zdá se, že toto nikdo moc do úvahy nebere.

- Na povinné subjekty přitom má dopadat řada nových regulací, především směrnice NIS 2 (o opatřeních k dosažení vysoké společné úrovně kybernetické bezpečnosti v Unii), která bude množstvím svých nároků na povinné subjekty podobná nařízení GDPR. Povinné subjekty budou muset například mít konkrétní politiku v oblasti bezpečnosti, posílat příslušné zaměstnance na pravidelná školení a to vše dokládat, každý incident bude muset být zaznamenán a ohlášen a podobně, což není fundamentálně špatné, ale je to nová a nákladná byrokracie.

Analýza bezpečnosti 5G sítí

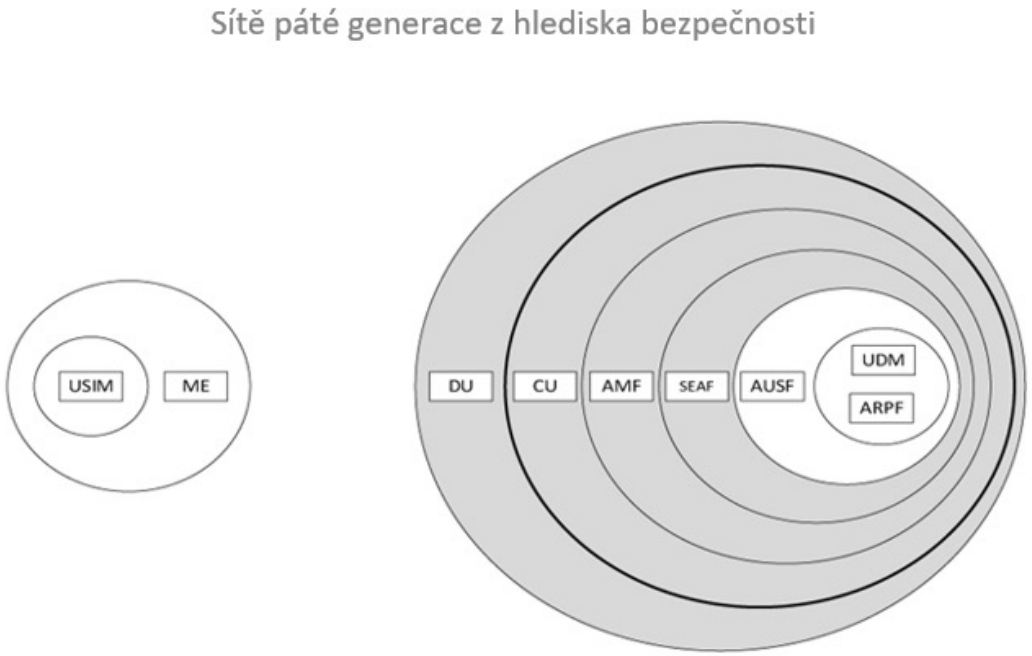
- Řešení těchto rizik (stejně jako ostatních rizik vyplývajících z dodavatelského řetězce) přitom spočívá především v přísném uplatňování standardů a pravidel kybernetické bezpečnosti.

- Pokud tak stát chce skutečně snížit jím vnímané riziko vyplývající z dodavatelského řetězce, ať to učiní propoprčně 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.

- Jde o kompromis, který uplatňují některé evropské země (např. Finsko) a který zajišťuje dosažení cíle a omezuje riziko zvýšení cen pro koncové spotřebitele vlivem zvýšených nákladů pro operátory způsobených snížením konkurenčního prostředí mezi dodavateli. Pokud už má být nějaká regulace, nechť je elegantní a nikoli finančně nákladná pro všechny strany.

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.]



Obrázek 1 Model důvěry v 5G sítí

Výbor Nezávislého ICT průmyslu

Děkuji Vám za pozornost.

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