Executive summary: Návrh úprav k návrhu nového zákona o kybernetické bezpečnosti (ZKB)

(k mechanismu prověřování bezpečnosti dodavatelského řetězce a zajištění dostupnosti strategicky významné služby)

Připomínky k mechanismu prověřování bezpečnosti dodavatelského řetězce lze rozdělit do 3 hlavních bodů:

1) Omezení rozsahu regulace na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni

Jak uvedl NÚKIB, Mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. NÚKIB však ve svém návrhu vymezil rozsah Mechanismu formou vyhlášky o nepominutelných funkcí, která pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě, jako je jádro sítě, tak i v obecné rovině méně kritické části sítě, jako je rádiová přístupová síť nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb, jako je fakturační systém. V návrhu zákona také zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce.

V našem návrhu jsme kritické části strategické infrastruktury transparentně rozdělili **dle hrozeb a míry dopadu jejich realizace.** Nejvýznamnější hrozbou je výpadek regulované služby. Rozsah Mechanismu jsme tak omezili na aktiva, **jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro oblast telekomunikací se bude jednat zejména o jádro sítě, případně části přenosové sítě.**

Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, **aby byla dána možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifkuje významnou hrozbu.**

Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval NÚKIB. NÚKIB by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel strategicky významné služby měl povinnost každoročně aktualizovat.

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

Tento systém jsme nazvali **kaskádou bezpečnostních povinností**, kdy pro tu nejkritičtější část strategické infrastruktury bude povinnost řídit se případným zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.

2) Zapojení vlády a sektorového regulátora do Mechanismu

a) Zapojení vlády

Zákazem či omezením plnění dodavatele dochází k významnému zásahu do svobody podnikání mnoha subjektů na trhu. Zákaz i omezení plnění dodavatele může mít významné ekonomické, ale i geopolitické dopady. Obdobné dopady již stát v minulosti hodnotil v rámci právní úpravy **prověřování zahraničních investic**. V rámci procesu prověřování zahraničních investic dochází obdobně jako v případě Mechanismu k prověřování osoby investora na základě strategických kritérií. Stejně jako v případě Mechanismu může také dojít k zákazu investice. V případě prověřování zahraničních investic je zákaz investice **podmíněn usnesením vlády**. Stejně by tomu tak mělo být i v případě Mechanismu, zejména s ohledem na skutečnost, že plošný zákaz či omezení plnění dodavatele může mít **mnohem větší dopad na trh než zákaz doposud neuskutečněné investice.**

b) Zapojení sektorového regulátora

Respektujeme, že v rámci posouzení rizikovosti dodavatele bude mít hlavní roli NÚKIB společně s vládou. V rámci určení lhůty pro implementaci případného zákazu je však role sektorového regulátora klíčová. Případný zákaz totiž může mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů. V případě telekomunikací jsou to například výstavbové povinnosti vyplývající ze zákona o elektronických komunikací. Je tedy naprosto zásadní, aby daný sektorový regulátor, v tomto případě ČTÚ, měl možnost se k implementaci zákazu vyjádřit a NÚKIB musel k jeho stanovisku přihlédnout.

3) Kompenzace

Navrhuje se zakotvení možnosti náhrady škody, a to obdobně, jak je tomu např. v zákoně č. 289/2005 Sb., o vojenském zpravodajství („*zákon o vojenském zpravodajství*“), v němž je přiznána náhrada škody každému, komu škoda nebo nemajetková újma vznikla v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu. Náhrada škody je upravena ve vloženém ustanovení § 30a předkládaného návrhu, podle nějž má

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

poskytovatel strategicky významné služby vůči státu nárok na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z opatření obecné povahy.

Náhrada škody dle předmětného ustanovení je koncipována jako náhrada za nemožnost používání technologie po plnou dobu jejího životního cyklu a konkrétní výše je určována znalcem, a to na základě účetních odpisů, s tím, že by byla určena na základě rozdílu mezi délkou životního cyklu plnění dodavatele a lhůty stanovené Úřadem pro omezení či odstranění plnění dodavatele. Metoda určení výše náhrady škody dle odpisů se použije právě a jen pro případy náhrady za nemožnost používání dlouhodobého majetku v plném rozsahu. Pokud by tedy např. Úřad stanovil lhůtu pro odstranění plnění dodavatele v délce 3 roky a životní cyklus plnění dodavatele (technologie) by byl dle účetních odpisů 5 let, mohl by poskytovatel strategicky významné služby požadovat náhradu škody odpovídající 2 zbývajícím rokům odpisů. **Pro náhradu dalších účelně vynaložených nákladů vzniklých v důsledku plnění povinností uvedených v opatření obecné povahy se metoda odpisů z povahy věci nevyužije.**

Pro zajištění větší právní jistoty státu je maximální doba odpisů omezena na 7 let, aby nedocházelo k umělému protahování odpisů.

Pokud bude rozsah regulace nastaven tak, jak je uvedeno v tomto návrhu, lze říci, že kompenzace např. v oblasti telekomunikací nebudou reálně žádné. Ustanovení je však nastaveno tak, že pokud by škoda způsobena byla (například v jiných dotčených sektorech), nebo by došlo k novelizaci zákona a rozšíření rozsahu regulace, existovala by zde zákonná možnost nárokovat náhradu škody.

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

Detailní rozbor jednotlivých ustanovení

K § 28 návrhu nového ZKB:

- je navržena úprava kritické části stanoveného rozsahu aktiv tak, aby se jednalo pouze o aktiva ohodnocená povinnými subjekty na **úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby**
    - rozsah mechanismu jsme definovali na základě hrozeb a důsledku jejich případné realizace. Jako nejvýznamnější hrozbu jsme označili **nedostupnost strategicky významné služby**. -> zákaz dodavatele pro aktiva, jejichž výpadek může způsobit nedostupnost strategicky významné služby je tedy s ohledem na princip proporcionality **přiměřený**
    - pro oblast telekomunikací jde v zásadě o vztažení mechanismu pouze na části sítě zvané: „jádro sítě“ a části „přenosové sítě“. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace

K § 30 návrhu nového ZKB:

- Nad rámec výše uvedeného jsme zavedli **tzv. kaskádu bezpečnostních opatření**, kdy v případě vydání opatření obecné povahy (OOP) je pro poskytovatele strategicky významné služby zakotvena **nově povinnost provést analýzu rizik** pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu (tj. pro zbývající aktiva, která nejsou na úrovni kritická) – § 30 odst. 9-10
    - v rámci analýzy rizik musí povinná osoba zohlednit rizika, která NÚKIB uvedl v OOP
    - na základě analýzy rizik poskytovatel vypracuje plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v OOP
    - tento plán musí pravidelně aktualizovat
    - NÚKIB tedy může zakázat dodavatele v kritické části stanoveného rozsahu (**kde hrozí nedostupnost strategicky významné služby na kritické úrovni**). Pro zbytek aktiv vznikne povinným osobám automaticky povinnost provést analýzu rizik uvedených v OOP a vypracovat strategií zvládání rizik včetně implementace odpovídajících bezpečnostních opatření
- do procesu posuzování dodavatele je nově zapojen(a):
    - vláda (obdobně je tomu v zákoně o prověřování zahraničních investic) – § 30 odst. 1-4

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

- sektorový regulátor – § 30 odst. 5-6
  - poskytuje konzultaci a stanovisko k tématice lhůty omezení či zákazu plnění dodavatele a možnosti ohrožení plnění povinností dle zvláštního právního předpisu –> NÚKIB musí stanovisko zohlednit

K § 30a návrhu nového ZKB:

- v § 30a je nově zakotvena možnost náhrady škody
  - poskytovatel strategicky významné služby má vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z OOP
  - náhrada škody je určována znalcem, a to na základě účetních odpisů
  - maximální doba odpisů je omezena na 7 let, aby nedocházelo k umělému protahování odpisů
  - v případě zachování znění § 28 nevznikne operátorům škoda, kterou by nárokovali po státu

K § 31 návrhu nového ZKB:

- navrhuje se doplnění odstavce č. 5, v němž je zakotveno, že všechny informace týkající řízení o udělení výjimky a obsahu vydaného rozhodnutí Úřadu o povolení výjimky jsou považovány za informace, jejichž zpřístupnění může ohrozit zajišťování kybernetické bezpečnosti
- na doplněné ustanovení navazuje ustanovení § 37 návrhu nového ZKB ve znění předloženém NÚKIB, v němž jsou upraveny výjimky z práva na informace, a na jehož základě se podle právních předpisů upravujících svobodný přístup k informacím neposkytují informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost protiopatření vydaného podle ZKB

K § 34 návrhu nového ZKB:

- nově vloženo ustanovení (nový odstavec 2) deklarující speciální úpravu zajištění dostupnosti strategicky významné služby ve vymezených oblastech elektronických komunikací
  - cílem je zamezení možných dezinterpretací a výkladových nejasností problematiky zajištění dostupnosti strategicky významných služeb pro oblast telekomunikací

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

Komplexní návrh úprav:

Prověřování rizik spojených s dodavatelem
§ 28

1. Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele.
2. Činnosti podle odstavce 1 prioritizuje Úřad podle přístupu založeného na rizicích a dostupných kapacitách.
3. Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí
   a. kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní kritická, a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby,
   b. bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu
      1. technického prostředku nebo vybavení s výpočetní kapacitou,
      2. programového prostředku nebo vybavení, nebo
      3. informační či komunikační služby,
   c. dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.

§ 30

Omezení rizik spojených s dodavatelem

1. Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání Vládě České republiky (dále jen “Vláda”). Před předložením věci Vládě je Úřad povinen vyhotovit odhad nákladů povinných osob spojených se zavedením omezení či zákazu plnění dodavatele, který je nedílnou součástí dokumentace předkládané Vládě. Poskytovatel strategicky významné služby je povinen na výzvu poskytnout Úřadu potřebnou součinnost.

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

2. Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední soulad případného plnění dodavatele s principy demokratického právního státu, dopad na ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku.
3. V návaznosti na usnesení Vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu.
4. Usnesení Vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení Vlády podmíněno.
5. Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné povahy přiměřenou lhůtu zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele.
6. Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit.
7. Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pominutí takové hrozby.
8. Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí.

9. V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a).
10. Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládání rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládání rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok.
11. Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší.

§30a

Náhrada účelně vynaložených nákladů

1. V případě, že lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle §30 odstavce 3 je kratší, než životní cyklus bezpečnostně významné dodávky, nejdéle však 7 let, má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností podle § 30 odstavce 3, a to včetně nákladů na náhradu dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle § 30 odstavce 3 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost.
2. Životní cyklus bezpečnostně relevantní dodávky bude znalcem určen na základě účetních odpisů zařízení.
3. Zrušením opatření obecné povahy podle § 30 odstavce 11 nezaniká právo na náhradu nákladů podle tohoto ustanovení. Ve věci náhrady nákladů podle tohoto ustanovení jménem státu jedná Úřad.

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

§ 31

Výjimky z omezení rizik spojených s dodavatelem

1. Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § 30, jestliže by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby.
2. Řízení o povolení výjimky podle odstavce 1 lze zahájit na žádost poskytovatele strategicky významné služby nebo z moci úřední. Žadatel je povinen v rámci žádosti připojit důkazy prokazující skutečnosti, kterých se dovolává.
3. Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší.
4. Úřad výjimku nepovolí, pokud by to zcela zmařilo účel opatření obecné povahy podle § 30.
5. Veškeré informace týkající se rozhodnutí o povolení výjimky a řízení o povolení výjimky jsou považovány za informace, jejichž zpřístupnění může ohrozit zajišťování kybernetické bezpečnosti.

§ 34

Zajištění dostupnosti strategicky významné služby

1. Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky.
2. Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupní služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy k vyhlášce o regulovaných službách je povinen v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky zajistit dostupnost strategicky významné služby spočívající v
   a) poskytování veřejně dostupné mobilní služby elektronických komunikací,
   b) zajišťování veřejné mobilní komunikační sítě elektronických komunikací,
   c) poskytování veřejně dostupné služby elektronických komunikací v pevném místě.

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz

3. Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby v rozsahu kritické části stanoveného rozsahu z území České republiky nejméně jednou za dva roky.
4. Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2.
5. Stanovený čas a kvalitu služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu.
6. Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a).

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,

ISDS: nn7uc3f, www.apms.cz