Důvodová zpráva z návrhu nového zákona o kybernetické bezpečnosti (ZKB)

Zvláštní část

§20, § 30, § 30a, § 31, § 34

K návrhu znění § 28 návrhu nového ZKB:

Navrhované ustanovení ponechává pravomoc Národního úřadu pro kybernetickou a informační bezpečnost („*Úřad*“) provádět prověřování rizik spojených s dodavatelem, tak jak přepokládá návrh nového zákona o kybernetické bezpečnosti („*návrh ZKB*“), odlišně však vymezuje některé pojmy spojené s touto pravomocí. Vzhledem k odlišné koncepci pojmu kritické části stanoveného rozsahu (viz níže), je obsolentní zakotvení vydání vyhlášky o nepominutelných funkcích stanoveného rozsahu, jak předpokládá návrh ZKB, proto byla ze znění tohoto návrhu vypuštěna.

Pravomoc Úřadu má být realizována, v souladu s návrhem ZKB, prostřednictvím shromažďování a vyhodnocování informací, jež mohou přispět k vyvození závěrů o existenci hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele stanovených prováděcím právním předpisem, a které jsou spojeny s plněním konkrétního dodavatele. Kritéria rizikovosti dodavatele stanoví prováděcí právní předpis – vyhláška, k jejímuž vydání je zmocněn Úřad v § 55 návrhu ZKB.

Jak uvádí Úřad v důvodové zprávě k návrhu ZKB, cílem mechanismu prověřování bezpečnosti dodavatelského řetězce („*mechanismus*“) je umožnit státu identifikovat a vyhodnocovat hrozby spojené jak s orgány nebo osobami, které již jsou dodavateli do infrastruktury poskytovatelů strategicky významné služby, tak s orgány nebo osobami, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly, a to s cílem odhalit hrozbu ještě dříve, než bude u strategicky významné služby moci způsobit narušení bezpečnosti informací. S ohledem na velké množství orgánů a osob, které mohou být předmětem prověřování, je stanovena možnost Úřadu prioritizovat činnosti spojené s prověřováním stávajících a potenciálních dodavatelů, tak jak to předpokládá i návrh ZKB, a to s ohledem na možná rizika a dostupné kapacity Úřadu.

Odstavec 3 předmětného ustanovení vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem. Pojem *„bezpečnostně významná dodávka“*, který vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů, a *„dodavatel bezpečnostně významné dodávky“,* který vymezuje okruh orgánů a osob, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených, je dle tohoto návrhu shodný se zněním uvedeným v návrhu ZKB, proto se mu text zde nebude věnovat.

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz

Změny však v tomto předkládaném návrhu doznal pojem *„kritická část stanoveného rozsahu“,* který vymezuje aktiva poskytovatele strategicky významné služby, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů.

Úřad opakovaně deklaroval, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB však Úřad vymezil rozsah mechanismu formou vyhlášky o nepominutelných funkcí, která je výrazně širší, než bylo deklarováno, a například pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě – „core“), tak i méně kritické části sítě (jako je např. rádiová přístupová síť) nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb (např. fakturační systém). V návrhu ZKB i důvodové zprávě k němu zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce.

Ve zde předkládaném návrhu je stanovena nová 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.**

Předkládaný návrh vychází z předpokladu, že kritická část stanoveného rozsahu se skládá z podmnožiny aktiv strategicky významných služeb, u kterých si poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu upravujícího bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností sám v rámci plnění povinností podle § 13 návrhu ZKB ohodnotil dopad narušení bezpečnosti informací úrovní kritická.

Kritické části strategické infrastruktury jsou transparentně rozděleny dle úrovně hrozby a dopadů její případné realizace. Nejvýznamnější hrozbou je výpadek regulované služby – rozsah mechanismu tak byl v návrhu omezen výlučně na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro příklad – pro oblast telekomunikací se jedná zejména o jádro sítě, případně části přenosové sítě. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace.

Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je přiměřené, aby byla dána možnost státu okamžitým zásahem omezit či 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 Úřad. Úřad by přitom jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově měla být upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel strategicky významné služby měl povinnost každoročně aktualizovat (blíže viz odůvodnění § 30 návrhu níže).

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz

K návrhu úpravy § 30 návrhu nového ZKB:

Navrhované ustanovení zakotvuje možnost omezit nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, a to zjistí-li Úřad postupem podle § 28 odst. 1 návrhu ZKB, že může být významně ohrožena bezpečnost České republiky nebo vnitřní či veřejný pořádek.

Oproti návrhu ZKB je do procesu prověřování rizik spojených s dodavatelem zapojena vláda. Zapojení vlády v procesu prověřování rizikovosti dodavatele je zásadně smysluplné a důležité, a to jak z hlediska transparentnosti a objektivity rozhodování, tak vzhledem k závažnosti opatření obecné povahy, které na základě uvedeného ustanovení zákona může být vydáno. Případný zákaz či omezení plnění dodavatele musí vždy být až nejzazším řešením – představuje totiž značný zásah do ústavně zaručených práv a povinností jednotlivých subjektů, i proto musí být podmíněn právě usnesením vlády.

Je třeba podotknout, že vláda do jisté míry v současnosti již do posuzování rizikovosti dodavatele (resp. investora) zapojena je, a to dle zákona č. 34/2021 Sb., o prověřování zahraničních investic („*zákon o prověřování zahraničních investic*“). Dle zákona o prověřování zahraničních investic jsou přijetím usnesení vlády podmíněna rozhodnutí omezující či zakazující zahraniční investici, a to právě s ohledem na míru zásahu do práv dotčených subjektů v důsledku tohoto omezení či zákazu. Začlenění vlády do procesu prověřování rizikovosti dodavatele má tedy pevné základy již v aktuálně účinné právní úpravě a rozhodnutí o omezení či zákazu plnění dodavatele by mělo být podmíněno usnesením vlády (obdobně jako u zahraničních investic), a to zejména s ohledem na to, že plošný zákaz či omezení plnění dodavatele může mít mnohem větší dopad na trh než zákaz doposud neuskutečněné investice.

Řešení otázky dodavatelského řetězce zasahuje do vícero oblastí, nejen do oblasti bezpečnostní. Pouze vláda může posoudit jak geopolitické a ekonomické dopady věci, tak i bezpečnostní aspekty – ostatně takto to činí již dle zákona o prověřování zahraničních investic, kdy vláda posuzuje, zda je případné omezení či zákaz zahraniční investice nutný z důvodu ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku, přičemž při posuzování jsou hodnocena i strategická kritéria, jako je hodnocení investorů z hlediska země jejich původu (např. zda je zahraniční investor ovládán přímo či nepřímo vládou třetí země, či zda již byl zapojen do činností ovlivňujících bezpečnost nebo veřejný pořádek v některém členském státě EU). Právě z důvodu komplexnosti celé problematiky a přesahu do rozličných oblastí není vhodné, aby věc byla konzultována pouze s Bezpečnostní radou státu („*BRS*“), jejímž předmětem činnosti je výhradně koordinace problematiky bezpečnosti České republiky, jak navrhuje návrh ZKB z dílny Úřadu. Nadto je třeba říci, že usnesení vlády jsou závazná zásadně šířeji, než usnesení BRS (usnesení vlády zavazují všechny členy vlády, ministerstva, jiné ústřední orgány státní správy, ostatní správní úřady a další subjekty, pokud tak stanoví zvláštní zákon, zatímco pokud jde o usnesení BRS, zde je

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz

závazná pouze jeho ukládací část (jen v oblasti zajišťování bezpečnosti České republiky), a to pouze pro určené členy vlády a vedoucí jiných správních úřadů).

Vedle zapojení vlády počítá předkládaný návrh rovněž s účastí sektorových regulátorů (příslušných ústředních orgánů státní správy), jejichž pozice je v návrhu ZKB značně opomíjena, je však v procesu prověřování zcela zásadní. Právě příslušní sektoroví regulátoři disponují potřebným penzem informací a odborných znalostí o fungování a činnosti daného regulovaného sektoru a jsou schopni posoudit reálné dopady případného omezení či zákazu plnění dodavatele, jakož i přesah do oblasti úpravy zajišťované zvláštními právními předpisy pro daný sektor (např. ohrožení plnění povinností subjektů stanovených těmito zvláštními právními předpisy).

V návaznosti na usnesení vlády a konzultaci se sektorovými regulátory, je dána Úřadu pravomoc vydat konkrétní omezení formou opatření obecné povahy, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb. Toto opatření obecné povahy však musí být přijato na základě usnesení vlády a zohledňovat stanovisko příslušného sektorového regulátora.

Proces prověřování rizikovosti dodavatele je dle tohoto návrhu nastaven následovně:

Pokud Úřad na základě vyhodnocení kritérií rizikovosti dojde k závěru, že plnění dodavatele může představovat významné ohrožení bezpečnosti anebo vnitřního či vnějšího pořádku České republiky, předloží věc k projednání vládě.

Vzhledem k tomu, že možné opatření omezující či zakazující plnění konkrétního dodavatele může mít rozsáhlé dopady nejen na dodavatele samého, ale i na povinné osoby (poskytovatele strategicky významných služeb), jichž se opatření obecné povahy dotýká, je Úřad ještě před předložením věci vládě povinen vypracovat odhad nákladů spojených s implementací povinností stanovených v opatření obecné povahy povinnými osobami. Tento podklad je zásadní pro samotnou vládu, aby mohla věc posoudit ve všech souvislostech (včetně případných ekonomických dopadů) a učinit informované rozhodnutí s vědomím veškerých hrozících dopadů. Za účelem vypracování odhadu nákladů jsou poskytovatelé strategicky významné služby povinni Úřadu poskytnout potřebnou součinnost.

Vláda má následně k dispozici lhůtu 45 dnů k projednání a vydání usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku (dále jen „*ohrožení*“), přičemž při posuzování věci vláda zohledňuje jak možný dopad plnění dodavatele na principy demokratického právního státu, 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. Usnesení vlády je pro Úřad vždy závazné a je jím podmíněno vydání zakazujícího či omezujícího opatření obecné povahy.

V návaznosti na usnesení vlády o tom, že plnění dodavatele představuje významné ohrožení, je Úřadu dána pravomoc vydat opatření obecné povahy, kterým stanoví podmínky nebo

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz

zakáže plnění dodavatele bezpečnostně významné dodávky. Z povahy opatření obecné povahy vyplývá, že jde o opatření, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb – směřuje však vždy vůči vymezeným plněním daného dodavatele (proti bezpečnostně významné dodávce). Stejně jako v návrhu ZKB, se vydání opatření obecné povahy řídí obecnou právní úpravou obsaženou ve správním řádu, a to s výjimkou ustanovení, která pojmově nejsou přiléhavá k problematice prověřování rizikovosti dodavatele (týkají se typicky nemovitostí a územního rozvoje). Z obecné právní úpravy také vyplývá možnost přezkoumat opatření obecné povahy v přezkumném řízení nebo v soudním řízení správním dle obecné úpravy správního řádu a správního řádu soudního, nelze však proti němu podat opravný prostředek.

V rámci omezujícího či zakazujícího opatření obecné povahy Úřad vždy stanoví i přiměřenou lhůtu pro zohlednění podmínek či zákazu. Nově předkládaný návrh stanovuje, že lhůta musí být vždy stanovena v návaznosti na projednání s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, neboť právě sektoroví regulátoři disponují objektivními informacemi, na jejichž základě lze přiměřenou lhůtu stanovit.

Je nutné trvat na tom, aby omezení či zákaz stanovený prostřednictvím opatření obecné povahy byl vždy proporcionální a přiměřené a nekolidoval s právní úpravou obsaženou ve zvláštních právních předpisech. Vzhledem k tomu, že případné omezení či zákaz plnění dodavatele může mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů, je za tímto účelem navrženo, aby Úřad projednal s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností uvedených ve zvláštních právních předpisech. Například pro oblast telekomunikací jde mj. o výstavbové povinnosti vyplývající ze zákona č. 127/2005 Sb. o elektronických komunikacích. Je tedy zásadní, aby daný sektorový regulátor, v tomto případě Český telekomunikační úřad, měl možnost se k implementaci omezení či zákazu vyjádřit a Úřad musel k jeho stanovisku přihlédnout.

V souladu s návrhem ZKB je i v tomto návrhu zachována povinnost Úřadu pravidelně (nejméně jednou za 3 roky) přezkoumávat trvání skutečností, na jejichž základě bylo vydáno omezení či zákaz, aby byla v případě jejich pominutí bezodkladně zrušena.

Navrhovatel si je vědom nutnosti zajištění kybernetické bezpečnosti a bezpečnosti informací, a to v celé síti, proto v rámci ustanovení § 30 navrhuje nově zavést taktéž povinnost pro poskytovatele strategicky významné služby **provést analýzu rizik spojených s dodavatelem dotčeným opatřením obecné povahy** u těch aktiv strategicky významné služby, které poskytovatel strategicky významné služby nezařadil do kritické části stanoveného rozsahu dle § 28 odst. 3 písm. a). Jde v podstatě o zavedení jakési kaskády bezpečnostních opatření, kdy pro tu nejkritičtější část strategické infrastruktury, kde hrozí

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz

přímý okamžitý dopad na nedostupnost strategicky významné služby, bude dána povinnost řídit se případným omezením či 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.

Na základě analýzy rizik poskytovatel strategicky významné služby vypracuje plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy, který musí pravidelně (alespoň jednou za kalendářní rok) aktualizovat.

Úřad tedy může omezit či zakázat plnění dodavatele v kritické části stanoveného rozsahu tam, kde hrozí nedostupnost strategicky významné služby. Pro zbytek aktiv pak vznikne poskytovatelům strategicky významné služby automaticky povinnost provést analýzu rizik uvedených v opatření obecné povahy i pro aktiva nezařazená do kritické části stanoveného rozsahu a vypracovat strategii zvládání rizik včetně implementace odpovídajících bezpečnostních opatření.

Návrh na doplnění § 30a do návrhu nového ZKB:

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.[1] Náhrada škody je upravena ve vloženém ustanovení § 30a předkládaného návrhu, podle nějž má 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

[1] Viz § 16n zákona o vojenském zpravodajství:
(1) *Každý, komu vznikla škoda nebo nemajetková újma v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu, má právo na jejich náhradu.*
(2) *Fyzické nebo právnické osobě se nahrazuje také škoda nebo nemajetková újma, která jí vznikla v důsledku realizace opatření přijatých Vojenským zpravodajstvím v zájmu provedení aktivního zásahu směřujícího k odstranění kybernetického útoku nebo hrozby v rámci zajišťování obrany státu v kybernetickém prostoru.*
(3) *Povinnost státu k náhradě škody nebo nemajetkové újmy podle odstavců 1 a 2 nevznikne, pokud se jedná o škodu nebo nemajetkovou újmu způsobenou fyzické nebo právnické osobě, která vyvolala útok nebo hrozbu.*
(4) *Za škodu nebo nemajetkovou újmu způsobenou Vojenským zpravodajstvím odpovídá stát. Náhradu škody nebo nemajetkové újmy poskytuje v zastoupení státu Ministerstvo obrany.*

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz

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.

K návrhu úpravy § 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.

Vzhledem k citlivosti informací, které jsou v rozhodnutí o povolení výjimky uvedeny, je potřebné, aby rozhodnutí nebylo veřejně dostupné. S ohledem na potřebu zajištění kybernetické bezpečnosti a ochrany informací, jakož i obchodního tajemství dotčených subjektů, není přípustné, aby bylo rozhodnutí o povolení výjimky veřejně dostupné. Zveřejnění informací o tom, komu a za jakých podmínek byla Úřadem povolena výjimka, je z hlediska cíle zajištění kybernetické bezpečnosti, jakož i z hlediska hospodářské soutěže a ochrany údajů zásadně nevhodné rozporné se smyslem zákona.

Tuto potřebu potvrzuje i znění ustanovení § 37 návrhu nového ZKB (ve znění předloženém Úřadem), na něž doplněné ustanovení § 31 odst. 5 návrhu nového ZKB pojmově navazuje, a 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 návrhu nového ZKB.

K návrhu úpravy § 34 návrhu nového ZKB

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz

Navrhuje se doplnění nového odstavce č. 2, v němž je zakotvena speciální úprava zajištění dostupnosti strategicky významné služby pro oblast elektronických komunikací.

Vzhledem k tomu, že oblast elektronických komunikací je velmi specifickým sektorem a již krátce po zveřejnění návrhu ZKB v eKLEP bylo zřejmé, že úprava navržená v návrhu ZKB (ve spojení s příslušnými prováděcími právními předpisy) způsobuje výkladové nejasnosti ohledně rozsahu a dopadu daného ustanovení, navrhuje se zakotvení speciální úpravy zajištění dostupnosti strategicky významné služby pro oblast elektronických komunikací, a to s cílem zamezit možným dezinterpretacím daného ustanovení pro oblast elektronických komunikací.

Asociace provozovatelů mobilních sítí, Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891,
ISDS: nn7uc3f, www.apms.cz