Zdeněk Zajíček
prezident

V Praze dne 16. února 2026
Čj.: 798/8000/2026/HKCR

Věc: Rámcová pozice České republiky k návrhu revize Aktu o kybernetické bezpečnosti CSA2 a návrh směrnice obsahující cílené úpravy směrnice NIS2

Vážený pane Kalinowski,

obracíme se na Vás ve věci návrhu Nařízení "Cybersecurity Act 2" (CSA2), kterou pod číslem COM/2026/11 final zveřejnila Evropská komise 20. ledna tohoto roku, doprovázené návrhem revize směrnice NIS2. Návrhy po první analýze, kterou jsme provedli, představuje nejen zásadní potenciální zvýšení regulační zátěže pro poskytovatele služeb a sítí elektronických komunikací všech velikostí, ale hlavně významný zásah do svobody podnikání a možnosti svobodné volby obchodních partnerů.

Problematika dodavatelského řetězce

Zcela zásadní je v tomto případě celá část IV "Bezpečnost dodavatelských řetězců" (články 98 až 117). Jak jistě víte, už při schvalování nového českého Zákona o kybernetické bezpečnosti byla část týkající se takzvaného "Mechanismu prověřování bezpečnosti dodavatelského řetězce" poměrně významně připomínkována. Uvítali jsme konečné znění Zákona o kybernetické bezpečnosti, které ponechalo rozhodování o případném označování dodavatelů za rizikové, jejich omezování či zákazu na politické reprezentaci s demokratickým mandátem. Pouze Vláda České republiky je schopná vyhodnotit dopady případné regulace celistvě a posoudit dopady do všech ekonomických a bezpečnostních politik na našem území.

Stejně tak se vedly a povedou zásadní debaty o tom, na jaká aktiva se má toto posuzování zaměřit a jaký bude rozsah mechanismu. Jsme přesvědčeni, že znění zákona je vyvážené a ačkoli jde o další regulaci, která na nás dopadá, chápeme zájem státu nad větší kontrolou dodavatelů do kritických aktiv sítí u podniků, které jsou systémově významné.

Hospodářská komora České republiky
zajicek.zdenek@komora.cz | +420 266 721 311 | Florentinum (recepce A) | Na Florenci 2116/15 | 110 00 Praha 1
www.komora.cz

HOSPODÁŘSKÁ KOMORA ČESKÉ REPUBLIKY

Zdeněk Zajíček
prezident

Návrh CSA2 z pera Evropské komise je přitom násobně rozsáhlejší, než je kompromis, ke kterému jsme dospěli jako zástupci různých odvětví při vyjednávání s českou politickou reprezentací. Návrh zavádí závazný rámec pro vylučování tzv. vysoce rizikových dodavatelů napříč všemi regulovanými sektory dle NIS2 a významně rozšiřuje regulaci ICT dodavatelských řetězců. Dochází k bezprecedentní centralizaci pravomocí u Evropské komise – ta má získat naprosto klíčovou roli při určování rizikových zemí, seznamů dodavatelů, zákazů technologií i lhůt pro jejich vyřazení, převážně prostřednictvím prováděcích a delegovaných aktů, s omezenou možností zásahu členských států.

Regulace má dopadnout na všechny sektory, na které dopadá směrnice NIS2 - tedy veřejnou správu, energetiku, dopravu, zdravotnictví, digitální infrastrukturu a veškeré elektronické komunikace; u telekomunikací výrazně nad rámec 5G Toolboxu EU. Návrh předpokládá mechanismy, které přesouvají hodnocení kybernetických rizik z technické roviny do roviny politické, což může vést k selektivnímu či geopoliticky zaměřenému uplatňování opatření s řetězovými a celoevropskými dopady, včetně omezení dostupnosti technologií na vnitřním trhu EU.

Rozhodnutí, které znamená de facto sankce na konkrétní stát či dodavatele se děje na úřednické úrovni bez rozhodnutí či kontrasignace demokraticky zvolené politické reprezentace. Státem, který představuje kyberbezpečnostní riziko, může být kterákoliv třetí země včetně našich dosavadních aliančních partnerů.

Komise může nařídit delegovanými akty víceméně cokoli:

- označit třetí zemi jako „country posing cybersecurity concerns“ (čl. 100),
- sestavit a aktualizovat seznam vysoce rizikových dodavatelů (čl.104),
- identifikovat klíčová ICT aktiva (čl. 102),
- stanovit mitigační opatření (čl. 103),
- určit lhůty pro vyřazení technologií (čl. 110),
- rozhodovat o výjimkách a jejich podmínkách (čl. 105-107),
- stanovovat poplatky za výjimky (čl. 109),
- uznávat (či neuznávat) certifikace třetích zemí (čl. 87).

Hospodářská komora České republiky
zajicek.zdenek@komora.cz | +420 266 721 311 | Florentinum (recepce A) | Na Florenci 2116/15 | 110 00 Praha 1
www.komora.cz

HOSPODÁŘSKÁ KOMORA ČESKÉ REPUBLIKY

Zdeněk Zajíček
prezident

A to vše s velmi malou možností členských států a demokraticky zvolené politické reprezentace proces nějak ovlivnit. Komise by tak v podstatě ovládla dodavatelské řetězce do celé řady sektorů a v sektoru telekomunikací až na úroveň mikropodniků a drobných regionálních ISP (protože i ty jsou regulovanými entitami dle směrnice NIS2 a tedy i dle Zákona o kybernetické bezpečnosti).

Telekomunikační sektor má být dle návrhu z důvodů, které nejsou nijak vysvětleny, regulován daleko přísněji než ostatní sektory. U mobilních, pevných i satelitních sítí je výměna technologií od dodavatelů, které Komise označí za "vysoce rizikové", jediným možným řešením a nedodržení je sankcionované nejvyšší pokutou (až 7 % celosvětového ročního obratu). Aktiva jsou uvedena přímo v příloze k návrhu nařízení. V jiných sektorech jsou klíčová aktiva a povinná zmírňující opatření identifikována až po kompletním posouzení rizik (kde je alespoň nějaká účast členských států). Možná jsou i opatření snižující riziko, která nevedou k úplnému zákazu (např. blokování vzdáleného přístupu nebo oddělení systémů), přičemž sankce za jejich nedodržení jsou mírnější.

Nerealistické časové hledisko a podhodnocené náklady

Jak jsme psali výše, návrh počítá s tím, že se "vysoce rizikoví dodavatelé" vyřadí z mobilních sítí do tří let, a to nejen z jádra, ale i z RAN. Tento požadavek není v tak krátké lhůtě realizovatelný. Splnění tohoto termínu by znamenalo okamžité zastavení jakékoli modernizace sítí a dlouholeté zaměření výhradně na výměnu zařízení. Rozsah potřebných inženýrských prací k dosažení tohoto nerealistického cíle by významně překročil dostupné a nasmlouvané kapacity, narušil dodavatelské řetězce a vedl k prudkému růstu vstupních cen pro všechny podnikatele. Jednoznačně by došlo ke zhoršení kvality služeb. Pokrytí evropských států 5G by se daleko výrazněji vzdálilo úrovni USA a asijských zemí. Žádná země EU dosud neprovedla komplexní výměnu rádiové části sítě za méně než pět let. Zkušenost ze Spojeného království ukazuje, že jen pro zmírnění nejhorších provozních dopadů je nutné rozložit výměnu do období 7–10 let.

Požadavek na odstranění "vysoce rizikových dodavatelů" z pevných sítí je zcela nepřiměřený. Rozsah je obrovský (zahrnuje v podstatě celou infrastrukturu – přístupové, transportní a přenosové sítě). Není nijak odůvodněn mírou rizika ani kritičností jednotlivých komponent.

Hospodářská komora České republiky
zajicek.zdenek@komora.cz | +420 266 721 311 | Florentinum (recepce A) | Na Florenci 2116/15 | 110 00 Praha 1
www.komora.cz

HOSPODÁŘSKÁ KOMORA ČESKÉ REPUBLIKY

Zdeněk Zajíček
prezident

Náklady na takový projekt by byly enormní a opět zcela na úkor rozšiřování optických sítí do domácností a skutečné posilování jejich odolnosti.

Odhad nákladů na výměnu HRV (High Risk Vendors) v mobilních sítích ve výši 15–20 miliard eur je výrazně podhodnocen. Náklady na pevné sítě se rovněž vyšplhají do desítek miliard eur. Navrhované změny v přidělování spektra a další zjednodušující iniciativy uvedené v Digitálním síťovém aktu (DNA) zdaleka nevykompenzují povinnost odstranit zařízení označených jako vysoce rizikových z mobilních a pevných 5G sítí. Evropský telekomunikační sektor je již nyní pod silným finančním tlakem. Bez plné kompenzace bude pouze velmi omezený prostor pro investice do zlepšování sítí (včetně bezpečnosti) a povinnost odstraňovat neodepsané technologie může přispět k dalším inflačním tlakům v ekonomice.

Zvýšení byrokracie

Návrh nařízení CSA2 se také zaměřuje na možnost certifikace podniků na soulad se směrnicí NIS2. To vypadá na první pohled jako smysluplné řešení snižující administrativní zátěž, máme ale velkou obavu, že to ve finále povede k omezení možnosti národního státu vydávat vlastní prováděcí předpisy.

Pokud se bude certifikovat soulad se směrnicí NIS2, bude to zřejmě znamenat nutnost jednotné certifikační úpravy pro celou Unii. To povede nevyhnutelně k unifikaci požadavků na opatření podle článku 21 směrnice v podobném stylu, jako je Prováděcí nařízení Komise 2024/2690, kterým Komise stanovila pravidla pro provozovatele DNS, registry domén nejvyšší úrovně, provozovatele služeb cloud computingu, datových center a další digitální služby. V případě dalších podobných prováděcích nařízení pak podle návrhu změn směrnice NIS2, které doprovází návrh CSA2, nebude smět členský stát navíc uplatňovat jakékoli další požadavky.

Ve finále to tak může znamenat zvýšení administrativní zátěže pro podniky, které jsou nyní v režimu nižších povinností, protože už prováděcí nařízení komise k vybraným digitálním službám přináší větší byrokracii i pro podniky, které by jinak mířily do nižšího režimu. Zvláště u poskytovatelů služeb a sítí elektronických komunikací jde o velké riziko, protože regulované dle Zákona o kybernetické bezpečnosti jsou i mikro a malé podniky.

Hospodářská komora České republiky
zajicek.zdenek@komora.cz | +420 266 721 311 | Florentinum (recepce A) | Na Florenci 2116/15 | 110 00 Praha 1
www.komora.cz

HOSPODÁŘSKÁ KOMORA ČESKÉ REPUBLIKY

Zdeněk Zajíček
prezident

Příležitost ke snížení administrativy

Zároveň je ale změnová směrnice k NIS2 příležitostí, jak odstranit nesmyslné požadavky nyní platné právní normy a z ní vycházejícího Zákona o kybernetické bezpečnosti. Směrnice generuje množství administrativní zátěže pro všechny subjekty. Bezpochyby by se její rozsah měl zúžit ve všech odvětvích pouze na subjekty, které jsou v kategorii velkých firem (nebo ideálně „small mid-caps", což je nová definice velikosti podniku, se kterou návrh novelizace směrnice přichází). Je s podivem, že se směrnice vztahuje na podniky, které nejsou z hlediska bezpečnosti významné kvůli nízkým objemovým kritériím.

Například v sektoru telekomunikací dopadá na podniky všech velikostí – tedy i na živnostníky bez zaměstnanců. I tyto subjekty tak musí řešit byrokracii, hlášení a další administrativní povinnosti – i když reálný zájem státu na tom, aby kontroloval, zda a jakou úroveň kybernetické bezpečnosti dodržují, neexistuje.

Místo toho, aby novelizace a revize evropské legislativy přinášely snížení administrativní zátěže firem, vedou k jejímu dalšímu zvyšování. Jsme přesvědčeni, že po volbách do Evropského parlamentu zde existovala politická shoda napříč Evropskou unií na „resetu" regulace, především na tom, že se musí povinnosti a pravidla, která dopadají na evropské podniky, snižovat, aby se napříč sektory evropskému byznysu dýchalo lépe. Evropská komise svými návrhy toto zadání zcela zjevně neplní a je na místě, aby členské státy daly jasně najevo, že toto akceptovat nehodlají.

Vážený pane Kalinowski, doufáme, že NÚKIB bude jedním z nejdůležitějších úřadů, které se budou podílet na přípravě rámcové pozice k tomuto návrhu nařízení. Velmi bychom ocenili, kdybychom se dokázali shodnou na odmítavém postoji k tomuto excesivnímu návrhu, který zastává celé odvětví poskytovatelů služeb a podniků zastupovaných Hospodářskou komorou ČR.

Podobná nařízení, jako je CSA2, znamenají mimořádně vysokou míru centralizace na evropské úrovni, která nedostatečně zohledňuje národní podmínky. Zejména pro sektor elektronických komunikací by taková úprava představovala velmi významný zásah do podnikání se zásadními dopady na dostupnost služeb i investice do moderních technologií a podle našeho názoru nezohledňuje rozdílné výchozí pozice operátorů při realizaci investičních plánů v jednotlivých státech zejména z hlediska návratnosti provedených investic.

Hospodářská komora České republiky
zajicek.zdenek@komora.cz | +420 266 721 311 | Florentinum (recepce A) | Na Florenci 2116/15 | 110 00 Praha 1
www.komora.cz

Zdeněk Zajíček
prezident

Přijetí regulace v podobě návrhu CSA2 by tak mělo významný dopad na české podniky a mohlo by se projevit snížením konkurenceschopnosti našich firem na globálním trhu. A to, věříme, není zájmem ani nás jako reprezentantů českého byznysu a nemůže být ani zájmem českého státu.

S pozdravem

Vážený pan
Marek Kalinowski
Oddělení multilaterální spolupráce 1
Odbor mezinárodní spolupráce a Evropské unie
Národní úřad pro kybernetickou a informační bezpečnost
Olšanská 36/9
130 00 Praha - Žižkov

Na vědomí:
Ing. Lukáš Kintr
ředitel NUKIB
Národní úřad pro kybernetickou a informační bezpečnost
Olšanská 36/9
130 00 Praha - Žižkov