SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

V PRAZE DNE 16. ÚNORA 2026

Stanovisko SP ČR k návrhu revize Aktu o kybernetické bezpečnosti (CSA2) a návrhu směrnice obsahující cílené úpravy směrnice NIS2

Svaz průmyslu a dopravy České republiky (SP ČR) dlouhodobě podporuje posilování kybernetické bezpečnosti v Evropské unii a zvyšování odolnosti digitální infrastruktury proti současným i budoucím hrozbám. Zároveň však považuje za nezbytné, aby přijímaná evropská legislativa byla předvídatelná, nepřekrývala se, byla technologicky neutrální, ekonomicky přiměřená a plně respektovala rozdělení pravomocí mezi Evropskou unií a členskými státy. Navrhovaná podoba zejména mechanismu k bezpečnosti dodavatelského řetězce včetně jeho implikací do směrnice NIS2 je z našeho pohledu v této chvíli nevyhovující.

Zásah do suverenity členských států v oblasti národní bezpečnosti

Národní bezpečnost je a musí zůstat výhradní pravomocí členských států, jak jasně stanoví **článek 4 odst. 2 Smlouvy o Evropské unii (SEU)**. Návrh CSA2 tuto zásadu obchází tím, že pod záminkou harmonizace vnitřního trhu (čl. 114 Smlouvy o fungování EU) zavádí nástroj, který je ve své podstatě bezpečnostně-politický a spadá do vnější obchodní politiky.

Návrh vytváří **nesrovnalosti mezi pravomocemi EU a členských států**. Zatímco členské státy si ponechávají pravomoc rozhodovat o tom, která odvětví zahrnout, Komise získává značné pravomoci ohledně kritérií technických a netechnických rizik. To vyvolává následné obavy:

- Potenciální **konflikty s jinými iniciativami EU**, jako je například Industry Accelerator Act, který podporuje nákladově efektivní zadávání veřejných zakázek na zařízení.
- Navzdory snahám o zjednodušení návrh zavádí **nové inspekční a hodnotící pravomoci**, které spíše zvyšují, než snižují administrativní požadavky.

Nehledě na to, že si Česká republika po dlouhé a náročné diskuzi vytvořila vlastní **mechanismus posuzování dodavatelů v novém zákoně o kybernetické bezpečnosti,** ke kterému máme i nadále přetrvávající výtky a je nezbytné vydat prováděcí právní předpisy, které stanovují detailní rozsah. I přes tyto výtky ale tento model svěřuje finální rozhodnutí o takto závažných otázkách do rukou **vlády ČR**, tedy demokraticky legitimovaného orgánu. Návrh Komise tento princip zcela popírá a přesouvá rozhodování na evropskou úroveň (Komise a její výbory).

Bezpečnost dodavatelského řetězce

Největší hrozbu spatřujeme v **Hlavě IV návrhu CSA2 (články 98–117)**, která zavádí **celoevropský mechanismus pro posuzování bezpečnosti dodavatelských řetězců.** Tento mechanismus dává Evropské komisi pravomoc, aby na základě vágně definovaných „netechnických rizik“ označovala celé třetí země za „rizikové“ a konkrétní dodavatele za „vysoce rizikové“, což by vedlo k jejich plošnému vyloučení z trhu EU.

TELEFON (+420) 731 829 128 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

Kritéria pro posouzení „netechnických rizik" jsou primárně politická, nikoli technická. Návrh umožňuje Komisi reagovat na „nezodpovědné chování státu v kyberprostoru" či jiné geopolitické faktory. To vytváří naprosto **nepředvídatelné prostředí** pro jakékoli dlouhodobé investice do technologií, protože jakákoli třetí země (včetně strategických partnerů jako USA či Izrael) se může stát terčem takového rozhodnutí na základě aktuální politické situace.

Plošný zákaz zavedených a prověřených dodavatelů by mohl **zásadně ovlivnit bezpečnost a kontinuitu** poskytování základních služeb veřejnosti a pro provozovatele kritické infrastruktury by znamenal **nutnost masivních, neplánovaných a extrémně nákladných investic do výměny technologií („rip and replace").** Tyto náklady by se pohybovaly v řádech desítek miliard korun jen v ČR a nevyhnutelně by se promítly do ceny služeb pro koncové zákazníky – občany i firmy. Zároveň by takový zásah **ohrozil stabilitu a kvalitu** poskytovaných služeb a dramaticky by zpomalil další inovace, včetně rozvoje sítí 5G, neboť tyto kritické infrastruktury jsou zpravidla založeny na vysoce specializovaných technologiích s dlouhým životním cyklem. Nejistota spojená s možností budoucího zařazení dodavatelů na evropské restriktivní seznamy může **negativně ovlivnit investiční plánování, financování infrastrukturních projektů a interoperabilitu technologií.**

Z pohledu právní jistoty a již existujícího režimu prověřování bezpečnosti dodavatelského řetězce v ČR, **navrhujeme, aby možnosti zásahů EK/ENISA do dodavatelského řetězce byly omezeny na formu pokynů (guidelines)**, které by nebyly přímo vykonatelné a byly s ohledem na národní podmínky prováděny ze strany jednotlivých národních regulačních orgánů v oblasti kybernetické bezpečnosti. Pokud se stanou povinnými, musí být vyváženy podporou zavádění technologií a podporou konkurenceschopnosti EU a zároveň respektovat bezpečnostní priority a dodavatelský řetězec příslušných zemí.

Postupné zpřísňování podmínek výběru dodavatelů přináší také řadu rizik jak z perspektivy povinného subjektu v režimu vyšších povinností (operator of essential services), tak i z pohledu veřejného zadavatele (povinný subjekt) zadávajícího sektorové veřejné zakázky, případně jiné osoby při zadávání sektorových veřejných zakázek, a to primárně z důvodu **omezení konkurenceschopnosti na trzích s omezeným počtem potenciálních dodavatelů.** S ohledem na pravomoc EK vytvářet tzv. blacklisty dodavatelů, **navrhujeme, aby o výjimku ze zařazení konkrétního dodavatele na tzv. blacklist EK mohli kromě samotného dodavatele požádat i zadavatelé**. Toto opatření má vést k vyloučení případů, kdy z důvodu omezené konkurence na relevantním trhu nebude možné vybrat dodavatele zejména v oblasti kritické infrastruktury, popř. omezená nabídka dodavatelů povede k výraznému navýšení výsledné ceny (např. v rozmezí více jak 30 % oproti předpokládané hodnotě zakázky) a může ohrozit realizaci investic do modernizace a rozvoje, včetně integrace obnovitelných zdrojů. Rozhodnutí o zařazení dodavatele na tzv. blacklist by rovněž mělo být podmíněno transparentní bezpečnostní a ekonomickou dopadovou analýzou.

Nadále vnímáme jako rizikové:

- Jakákoli země by mohla být klasifikována jako vysoce riziková na základě faktorů, jako je přístup orgánů činných v trestním řízení k datům, právní stát a stabilita právního systému a dalších stanovených kritérií, což by potencionálně mohlo **ovlivnit i důvěryhodné obchodní a bezpečnostní partnery EU a vést k diskriminačním výsledkům**.
- Návrh stanovuje, že koordinovaná posouzení bezpečnostních rizik na úrovni Unie musí být dokončena do šesti měsíců, ale **nevyžaduje komplexní technický přezkum dopadů** před označením podle článku 100. CSA2 nenařizuje, aby posouzení dopadů doprovázelo dané prováděcí akty.
- Článek 103 odst. 6 a 7 by měl postupovat dle stejných kritériích jako ve článku 100 návrhu.

- Návrh neobjasňuje, jak budou zařízení, služby nebo/a zboží IKT odděleny od dodavatelského řetězce EU a **co to bude znamenat pro konkrétního dodavatele**, pokud budou jeho zařízení, služby a/nebo zboží distribuovány v kritické infrastruktuře v několika zemích EU.
- Návrh umožňuje Komisi nebo skupině nejméně tří členských států požádat Skupinu pro spolupráci k NIS o provedení koordinovaného posouzení bezpečnostních rizik na úrovni Unie. Článek 99 stanoví, že pokud má Komise dostatečný důvod se domnívat, že existuje významná kybernetická hrozba, konzultuje s členskými státy zmírňující opatření. Nicméně tři členské státy spolu s Komisí by však mohly spustit označení podle článku 100, což by mohlo způsobit potenciálně významné problémy pro ostatní členské státy. To by nadále mohlo **podkopávat zásadu, že všechny země EU by měly mít dostatečný vliv na rozhodnutí** ovlivňující jejich národní bezpečnost, obranu, zadávání veřejných zakázek a kritickou infrastrukturu.
- Bude mít označení státu nebo dodavatele za „rizikové“ či „vysoce rizikové“ (které se provádí prostřednictvím prováděcích aktů, tedy mimo běžný legislativní proces) **účinek ex ante nebo ex post**, nebo obojí? Jaká je přesná souhra mezi označením země, vysoce rizikového dodavatele a zařízení/služby?

Jsme přesvědčeni, že navrhovaný mechanismus v CSA2 je v současné podobě nepřijatelný. Podkopává právní jistotu, ohrožuje ekonomickou stabilitu a neoprávněně zasahuje do suverenity České republiky v klíčové oblasti národní bezpečnosti.

Mandát ENISA

Vítáme objasnění poradní role ENISA. Návrh však **výrazně rozšiřuje mandát ENISA** o přeshraniční dohled, společné kontrolní týmy a komplexní analýzu rizik pro subjekty působící ve více členských státech. Také staví ENISA do pozice de facto evropského normalizačního orgánu, paralelně k CEN, CENELEC a ETSI, zejména pokud jde o vývoj certifikačních schémat v rámci evropského rámce pro certifikaci kybernetické bezpečnosti (ECCF). Obáváme se, že tento rozšířený mandát bude **v rozporu s klíčovou rolí evropských normalizačních organizací** při vývoji globálních norem.

Požadujeme, aby návrh CSA2:

- **objasnil poradní roli ENISA**,
- zajistil, aby evropská certifikační schémata kybernetické bezpečnosti byla **založena na evropských normách** nebo specifikacích vyvinutých evropskými normalizačními organizacemi (ESO),
- umožnil ENISA vyvíjet dočasné technické specifikace, pokud existuje zdokumentovaná naléhavost a posouzení potvrdí, že **neexistuje žádná stávající specifikace** se stejným nebo podobným rozsahem, přičemž specifikace ENISA musí být do 2 let nahrazena normou nebo specifikací ESO,
- zajistil, aby tyto technické specifikace ENISA **nebyly v rozporu s existujícími globálními nebo národními specifikacemi** členských států EU.

EU certifikační rámec

Ve vztahu k budoucímu EU certifikačnímu rámci doporučujeme již nyní v návrhu nařízení CSA2 stanovit, že **za splnění podmínek budoucího certifikačního schématu bude možné považovat i řádně implementované mezinárodní standardy** (např. ISO 27000). Důvodem je skutečnost, že řada povinných subjektů v oblasti kybernetické bezpečnosti investovala nemalé prostředky pro zajištění certifikace svých systému i vnitřních

procesů podle dosud nejlepších dostupných praktik a případná nutnost podrobit tyto systémy i procesy novému certifikačnímu schématu by pro ně představovala **nepřiměřenou finanční zátěž.**

Zkušenosti s Evropským systémem pro certifikaci kybernetické bezpečnosti (EUCS) ukazují, jak politické a netechnické požadavky mohou podkopávat cíle jednotného trhu. Mezi klíčové obavy patří:

- **Nedostatečná doba vývoje a nedostatek transparentnosti:** Standardizační orgány (CEN-CENELEC, ETSI) potřebují dostatek času na poskytnutí odborné technické zpětné vazby (jak bylo zdůrazněno výše). Návrh stanoví, že ENISA připraví kandidátní schéma do 12 měsíců od obdržení žádosti Komise, ale standardizace vyžaduje dostatek času na to, aby odborníci poskytli technickou zpětnou vazbu. Certifikační systémy musí zůstat čistě technické a poskytovat dostatek času na transparentní a průmyslově inkluzivní vývoj, aby se zajistilo přijetí poskytovatelem, proveditelnost implementace a důvěra zákazníků.
- **Vztah k certifikaci specifické pro daný sektor:** Návrh uvádí, že certifikace vyvinuté v rámci CSA2 by byly použitelné napříč sektory a zajišťovaly by soulad s odvětvovými schématy, jako je CRA nebo CORA. CSA2 dále uvádí, že pokud tak stanoví konkrétní právní akt Unie, certifikát vydaný v rámci evropského systému certifikace kybernetické bezpečnosti prokazuje soulad a poskytuje presumpci shody s odpovídajícími požadavky stanovenými v daném právním aktu. To vyžaduje další objasnění procesu, postupného ukončování odvětvových schémat, platnosti v různých zemích a podobných záležitostí.
- **Rozšíření profilů:** Upozorňujeme na riziko využívání tzv. „rozšiřujících profilů“ jako prostředku k zavádění dodatečných, fragmentovaných požadavků na národní úrovni, které by mohly narušit jednotný trh, zvýšit regulatorní nejistotu a dále zatížit společnosti.

Normy a specifikace jsou úspěšné a dosahují svých cílů pouze tehdy, když je poskytovatelé a zákazníci považují za cenné. Totéž platí pro certifikační systémy EU v rámci CSA2. Dobrým příkladem, který tohle pravidlo podporuje je harmonizace, která nahrazuje roztříštěná národní schémata nebo nahrazení jednotlivých prováděcích aktů technickými požadavky. Komise v úvodním textu CSA2 a v hodnocení ENISA a ECCF uznala, že zkušenosti s EUCS ukazují, jak politické a netechnické požadavky podkopávají cíle jednotného trhu.

<u>Vyjasnění vztahu k sektorovým předpisům a zabránění regulatorním překryvům</u>

SP ČR považuje za nezbytné jednoznačně vyjasnit **vztah navrhovaného nařízení CSA2 k již existujícím sektorovým předpisům**. Návrh v současné podobě vytváří riziko překryvu povinností, duplicitních požadavků a paralelních hodnoticích a standardizačních mechanismů, což by vedlo k **nepřiměřené administrativní a finanční zátěži** povinných subjektů bez odpovídajícího přínosu pro reálné zvýšení bezpečnosti.

<u>Zapojení průmyslu musí zůstat prioritou</u>

CSA2 ruší tzv. SCCG (Stakeholders Cybersecurity Certification Group) a nahrazuje ji „výročním shromážděním“. EK však připouští, že proces EUCS se částečně potýkal s problémy kvůli nedostatku transparentnosti vůči externím zúčastněným stranám. Jak bylo zdůrazněno výše, certifikační rámec bude mít významný dopad na konkurenceschopnost a bezpečnost EU, což vyžaduje, aby **certifikační systémy byly doprovázeny řádným posouzením dopadů, které mohou poskytnout příslušné zúčastněné strany průmyslu.** Konkurenceschopnost EU se musí zlepšovat společně s podniky, nikoli bez nich.

Novela směrnice NIS2

Novela směrnice NIS2 mimo jiné navrhuje, aby se opatření přijatá na základě mechanismu bezpečnosti dodavatelského řetězce v CSA2 stala **právně závaznými pro všechny povinné osoby podle NIS2**.

Tímto krokem by se z doporučení (jako byl např. 5G Toolbox) stal přímo vymahatelný právní závazek. Jakékoli rozhodnutí Komise o vyloučení dodavatele by tak bylo okamžitě a plně závazné pro tisíce českých firem, a to pod hrozbou sankcí podle směrnice NIS2. **Jde o bezprecedentní zpřísnění,** které zcela mění povahu dosavadní spolupráce v EU v oblasti kybernetické bezpečnosti.

Změny směrnice NIS2, které návrh předkládá, zavádějí nové požadavky na dodržování předpisů pro provozovatele kritické infrastruktury, veškerá opatření však musí být provedena **s realistickými časovými lhůtami a odpovídajícími konzultacemi s odvětvím**, aby se zabránilo narušení základních služeb.

Považujeme také za zásadní jednoznačně vyjasnit koncept „**Main Establishment**" mimo jiné i v kontextu navrhovaných změn v CSA2 a NIS2 a zajistit jeho jednotnou a konzistentní definici napříč relevantní legislativou.

Dále upozorňujeme na nové povinnosti hlášení incidentů typu ransomware, včetně sdílení potenciálně citlivých údajů. Tyto požadavky představují **významné zvýšení administrativní a finanční zátěže** pro společnosti, přinášejí právní nejistotu v oblasti ochrany důvěrných informací a **nejsou v souladu s deklarovaným cílem zjednodušování regulace** a posilování konkurenceschopnosti.