Nový zákon o kybernetické bezpečnosti - příležitost pro posílení odolnosti Česka

Proč potřebujeme nový zákon o kybernetické bezpečnosti

Digitální technologie dnes tvoří základ moderní společnosti – od řízení dopravy a energetiky po zdravotnictví a vzdělávání. S rostoucím využíváním těchto systémů se však zvyšují i **rizika spojená s kybernetickými útoky**. Bezpečnost infrastruktury, dat a digitálních služeb se tak pro ochranu státu a jeho občanů stává zcela klíčovou.

Česko v současnosti čelí bezprecedentnímu množství kybernetických hrozeb. Ty jsou navíc často spojené se **závislostí na dodávkách z nepřátelských zemí**, což představuje vážné bezpečnostní riziko, které může negativně ovlivnit fungování kritické infrastruktury, narušit dodávky strategických surovin a zvýšit pravděpodobnost kybernetických útoků.

Stát do velké míry spoléhá na infrastrukturu vlastněnou, dodávanou či spravovanou třetími osobami z jiných států, na kterých mu následně vzniká závislost. Možné dopady takových rizik ukázal např. **vývoj související s vojenskou invazí Ruské federace na Ukrajinu**, kdy mělo razantní zvýšení cen energií (zejména plynu), na jejíž dodávkách z Ruska bylo Česko závislé, za následek nezměrné ekonomické dopady.

Česko už sice má zákon o kybernetické bezpečnosti z roku 2014, ten ale pokrývá pouze část kritických oblastí. Zároveň je pro posílení kybernetické bezpečnosti potřeba vztáhnout působnost zákona také na některé dosud neregulované subjekty. Současnou právní úpravu je v neposlední řadě nutné aktualizovat tak, aby splňovala nové požadavky unijní legislativy (zejména **směrnice NIS 2**). **Implementační lhůtu směrnice přitom Česko už zmeškalo**, jelikož ji bylo nutné do českého práva transponovat do října roku 2024. S přijetím nového zákona by proto Poslanecká sněmovna neměla otálet a měla by jej v každém případě schválit v tomto volebním období.

S čím přichází nová legislativa

V polovině roku 2024 byl v Poslanecké sněmovně předložen **návrh nového zákona o kybernetické bezpečnosti a související změnový zákon** (sněmovní tisk č. 759 a sněmovní tisk č. 760), které připravil Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) jako nezbytný krok k posílení kybernetické odolnosti Česka. Co nový zákon přináší?

1. **Rozšíření působnosti na větší množství subjektů**: Zákon násobně zvyšuje počet subjektů, kteří budou muset dbát na kybernetickou bezpečnost. Zatímco se doteď regulace vztahovala na přibližně 400 subjektů, nově se dotkne až 10 000 společností. Zákon regulované osoby dělí do dvou skupin s větším a menším množstvím povinností podle rizikovosti v daném sektoru:
   - střední či velké podniky v regulovaných odvětvích, konkrétně firmy s více než 50 zaměstnanci nebo s ročním obratem nad 10 milionů eur (tzv. velikostní kritérium)
   - podniky působící v odvětví, jako je energetika, doprava, digitální infrastruktura, zdravotnictví, IT služby, poštovní služby a další (tzv. odvětvové kritérium).

   NÚKIB bude také moci určit některé společnosti poskytující strategicky významné služby (i přes nesplnění uvedených kritérií) jako regulované subjekty, případně stanovit, že se tyto společnosti musí řídit režimem vyšších povinností dle zákona namísto režimu nižších povinností.

2. **Rychlejší reakce na hrozby**: Poskytovatelé kritických služeb (např. energetika, zdravotnictví nebo doprava) budou muset do 24 hodin hlásit kybernetické incidenty, které mohou ovlivnit provoz nebo způsobit škody.

3. **Informovanost jednotlivců**: Poskytovatelé digitálních služeb budou mít povinnost upozorňovat uživatele na potenciální rizika (např. phishingové kampaně nebo podvodné weby). Zákon ukládá i povinnost poskytovat návod, jak chránit svá data.

4. **Zavedení mechanismu k prověřování dodavatelského řetězce** v oblasti informačních a komunikačních technologií. Tento nástroj umožní České republice po vzoru řady západních zemí (např. Francie, Litva, Nizozemí, Polsko, Norsko či Španělsko) provádět strategickou kontrolu dodavatelů u služeb a technologií, jejichž výpadek by mohl mít zásadní dopad na fungování státu. Tím se sníží riziko strategické závislosti na rizikových dodavatelích a posílí odolnost kritické infrastruktury.

5. **Zjednodušení legislativy a sjednocení s evropskými pravidly**: Zákon zapracovává evropské směrnice a nařízení (zejména směrnici NIS 2), čímž naplňuje povinnosti České republiky při zajišťování stejného standardu kybernetické bezpečnosti napříč Evropou.

Návrhy na převedení některých kompetencí z NÚKIB na vládu

V legislativním procesu byla předložena **řada pozměňovacích návrhů**, z nichž některé nový zákon oslabují a zároveň oslabují i roli NÚKIB. Bezpečnostní i

hospodářský výbor totiž schválily pozměňovací návrhy č. A4 a B4, které **posilují pravomoci vlády na úkor kybernetického úřadu**. Prováděcí předpis s kritérii pro určování strategicky významných služeb by nevydával vyhláškou NÚKIB, ale vláda nařízením. Na to navazují také pozměňovací návrhy č. A9 a B10, na základě kterých má vláda místo kybernetického úřadu stanovit také seznam nepominutelných funkcí strategicky významných služeb, tedy seznam takových činností, jejichž narušení by mělo na poskytování služby vliv. Podobně mají být omezeny pravomoci úřadu ve stanovení nezbytného rozsahu strategické služby, jehož dostupnost je poskytovatel služby povinen zajišťovat (pozměňovací návrhy č. A11 a B12).

Další **omezení pravomocí kybernetického úřadu** představuje změna § 29, který upravuje možnost úřadu zakázat nebo stanovit podmínky využívání plnění od dodavatele, který pro stát představuje kybernetickou hrozbu. Zatímco podle vládního návrhu zákona může úřad k takto výjimečnému kroku přistoupit za podmínky, že zjistí významné ohrožení bezpečnosti České republiky nebo vnitřního pořádku, podle pozměňovacích návrhů č. A10 a B11 tak učiní v případě, že se na tom usnese vláda. Přijetím tohoto návrhu by byla nastolena nežádoucí situace, kdy vláda vstupuje do správních řízení úřadu a přestože řízení vede nadále úřad, de facto se jedná o politické rozhodnutí vlády.

Návrhy na převedení některých kompetencí z NÚKIB na vládu

Nejvíce problematický pozměňovací návrh schválil rovněž Hospodářský výbor, a to pozměňovací návrh č. B9. Ten **oslabuje klíčový mechanismus prověřování bezpečnosti dodavatelského řetězce** tím, že zužuje jeho možný dopad pouze na nejkritičtější část infrastruktury. Mechanismus by se tak nevztahoval mj. na části dispečerských řídicích systémů, přes které se řídí i energetické sítě. Neexistuje přitom pádný důvod, proč by se klíčový mechanismus zákona neměl vztahovat na tyto vysoce důležité části systémů, jejichž narušení může zásadně ohrozit poskytování strategicky významných služeb v České republice. Došlo by tím k tomu, že by z dosahu mechanismu byly předem vyřazeny klíčové části infrastruktury a stát by se ani nedozvěděl, jací dodavatelé zde figurují, natož aby na ně mohl reagovat. S tímto omezením totiž padá také ohlašovací povinnost. **Proti takovému zúžení působnosti zákona se staví i kybernetický úřad**.

K zásadnímu oslabení cílů zákona vedou i pozměňovací návrhy č. B18-B21, v důsledku jejichž přijetí by **nebyla zajištěna kontinuita strategicky významných služeb v případě mimořádných událostí** (např. přírodních katastrof). Rozšířením požadavku na území EU hrozí, že strategickou službu nebude v takových situacích fyzicky možné na území ČR zajistit. Dopad změny původní koncepce lze ilustrovat na případu elektrárny, která napájí nemocnici. V případě, že by se nacházela mimo

území Česka, **stát by neměl možnost zajistit v krizové situaci její fungován**í. Obdobné riziko by nastalo v případě softwaru, serverů a cloudových služeb mimo naše území. Navrhovaný institut nebojuje proti cloudovým službám a nezavádí lokalizaci dat, pouze stanovuje, že má existovat postup, jak službu zajistit v případě ztráty spojení se zahraničím. Předmětné PN tento institut prakticky likvidují a navrhovaná úprava tak pozbude smyslu. Česko by se tím stalo výrazně zranitelnější a vydíratelnou zemí - v případě geopolitické nestability by příslušné orgány nemohly efektivně čelit masivním kybernetickým útokům. Rozsáhlé výpadky elektřiny a telefonických sítí by měly **nedozírné následky**.

Výše uvedené návrhy vyvolávají obavu z oslabení funkčnosti zákona. Hrozí, že zásadní nástroj pro vykonávání agendy NÚKIB a dohledu nad bezpečnými dodavatelskými řetězci nebude dostatečně účinný. Přenést klíčovou kompetenci z nezávislého a odborného Úřadu na politické rozhodnutí vlády, jejíž příklon k demokratickým zemím nelze do budoucna zaručit, může být **rizikové**. Ještě problematičtější jsou však návrhy, které budou de facto znamenat vyprázdnění samotného institutu **prověřování bezpečnosti dodavatelského řetězce.**

Podezřelé jsou okolnosti, za kterých jsou některé pozměňovací návrhy projednávány. Podle informací Českého rozhlasu zpravodaj tisku na hospodářském výboru Marek Novák (ANO) jednal v Číně se společností Huawei. Ta má přitom vysoký zájem na tom, aby pravidla kybernetickou bezpečnost zůstala co nejvolnější – NÚKIB již před 6 lety varoval, že právě technologie čínských společností Huawei a ZTE představují bezpečnostní riziko. Jak uvedl web Page Not Found ve svých článcích (zde a zde), pozměňovací návrhy hospodářského výboru směřují přesně k požadavkům Hospodářské komory ČR (HK ČR), která argumentuje mimo jiné čísly z Frontier Economics, kde si analýzu k dopadu směrnice NIS 2 platila přímo čínská Huawei. Podle zmíněného webu přitom Huawei posílá dary např. Výzkumnému ústavu pro podnikání a inovace, který je pod HK ČR začleněn. Huawei Technologies (Czech) s.r.o. je jinak také jedním z členů HK ČR.

Doporučení

1. Co nejdříve schválit kvalitní a funkční podobu zákona o kybernetické bezpečnosti ve třetím čtení.

2. Pozměňovací návrh č. B9, kterým dojde k podstatnému oslabení mechanismu prověřování bezpečnosti dodavatelského řetězce, zásadně nedoporučujeme.

3. Pozměňovací návrhy č. B18-21, kterými dochází k oslabení bezpečnostních mechanismů pro zajištění služeb v případě mimořádných událostí, zásadně nedoporučujeme.

4. V případě následujících pozměňovacích návrhů, které přenášejí pravomoci z expertního NÚKIBu na politický orgán, vládu:

a) č. A4: určování strategicky významných služeb vládou místo NÚKIB
b) č. A9: stanovení seznamu nepominutelných funkcí strategicky významných služeb vládou místo NÚKIB
c) č. A10: podmínění omezení rizik spojených s dodavatelem usnesením vlády
d) č. A11: stanovení nezbytného rozsahu strategické služby vládou místo NÚKIB
e) č. B4: určování strategicky významných služeb vládou místo NÚKIB
f) č. B10: stanovení seznamu nepominutelných funkcí strategicky významných služeb vládou místo NÚKIB
g) č. B11: podmínění omezení rizik spojených s dodavatelem usnesením vlády
h) č. B12: stanovení nezbytného rozsahu strategické služby vládou místo NÚKIB,

považujeme za sporné, zda je optimální měnit koncepci původního záměru zákona. Doporučujeme vhodnost uvedených návrhů ponechat na odbornou diskusi mezi vládou, NÚKIB a dalšími relevantními institucemi. V tomto směru je uklidňující zprávou podpora ze strany NÚKIB.

Vyjádření oslovených expertů

„Problém, který je dle mého názoru kruciální, je nelogické zúžení rozsahu mechanismu pouze na aktiva kritická (viz PN B9). Takováto „redukce“ povede k reálné slepotě orgánu, který má rozhodovat (tj. Vlády ČR). Neboť dojde ke zúžení možnosti ovlivnit dodavatele systémů v úrovni „vysoká“, přičemž tyto systémy jsou zcela nezbytné a je minimálně vhodné, aby Vláda byla schopna identifikovat to, o jaké dodavatele se jedná. Díky uvedenému pozměňovacímu návrhu odpadne ohlašovací povinnost dodavatelům infrastruktury v režimu vysoká. Problematické jsou rovněž PN B18-21. Je otázkou, zda po navržených úpravách má uvedený institut význam. Cílem ZoKB stejně jako novely krizového zákona je mimo jiné posílit odolnost ČR jak v digitální, tak fyzické rovině. Pokud bude strategicky významná služba (pro ČR) řízena ze zahraničí bez „backup plánu“ v podobě klidně i ne digitálního řešení v ČR, pak se domnívám, že naše resilience je naopak významně oslabena. Osobně se domnívám, že problematické je i datum navržené účinnosti zákona. Pokud je předpokládána účinnost od 1.7.2025 (u takto významné právní normy, která do značné míry mění postavení zcela nového okruhu povinných osob – viz dosud neregulované subjekty) pak ve vztahu k rychlosti legislativního procesu nového ZoKB a zatím „neběžícího legislativního procesu“ prováděcích vyhlášek, které jsou neméně významné, reálně vzniká velmi malý prostor se s novou regulací seznámit a začít plnit z ní vyplývající požadavky. Logické by bylo posunout legisvakanční lhůtu. Domnívám se, že by bylo vhodné, aby byl zákon účinný např. od 1. 1. 2026.“ — **doc. JUDr. Jan Kolouch, Ph.D., metodik kybernetické bezpečnosti, CESNET**

„Jakákoliv snaha o omezení regulace v oblasti kybernetické a informační bezpečnosti je znakem neschopnosti vnímat okolní svět, jeho nástrahy a jeho současné velmi dynamické

změny. A v podstatě také vypnutí pudu sebezáchovy. Instituce, která si nevyhodnotí rizika, která vyplývají z její závislosti na dodavatelském řetězci, se radostně řítí do záhuby. Není mým cílem tady jmenovat konkrétní firmy, jejichž produkty a jejich použití s sebou nesou bezpečnostní rizika. Každá firma, organizace, instituce by měla mít analýzu rizik, která rizika z využití technologií jakékoliv firmy plynou. A je navýsost žádoucí zahrnout i tzv. netechnická bezpečnostní rizika. Například pod jakou jurisdikci výrobce technologií v dané zemi spadá, jaký má na něj vliv stát jako takový apod.
Je nutno vzít v potaz všechny klíčové informace a je možné, že instituce zjistí, že lákavě nízká cena za řešení přinese následně více problémů než užitku. Veškerá opatření kybernetické a informační bezpečnosti musí vycházet z analýzy rizik a to právě i těch netechnických. Zvláště pak, pokud se jedná o zabezpečení významných služeb, které mají vliv na chod státu. Musí být provedena analýza rizik na dodavatele, respektive na závislost na nich. Analýza rizik poskytuje odpovědi na otázky typu, co se stane když moje významné služby závisí na funkčnosti dodavatele, který má sídlo v zemi, jejíž vedení má nepředvídatelné chování. A to v jakékoliv významné oblasti. Například se chystá zvýšit cla na technologie i služby. Bezbřehá důvěra ve „spojence" už není na místě.
Kybernetické útoky jsou charakteristické svojí rychlostí a také nutností okamžité reakce a prodlužování této reakce vsazováním dalších článků do rozhodovacího procesu je cestou do pekla. A vůbec nejhorší je do tohoto procesu vsazovat orgán veskrze politický. Tady je na místě, ať už se to líbí nebo ne, pragmatická a rychlá reakce bez politických půtek. Zmíněná analýza rizik i tyto faktory musí hodnotit. Jestliže jsme byli zvyklí na absolutní spolehlivost spojenců, tak ta doba už je pryč. Už delší dobu používané technologie postavené na „zero trust" tuto zásadu přesouvají i do netechnologického prostoru. V kyberprostoru se bezbřehá důvěra prostě nevyplácí. Stejně tak jako snaha o vnesení jakéhokoliv zpomalujícího a nepragmatického (politického) prvku do rozhodovacího procesu." — **Ing. Aleš Špidla, ředitel Centra rozvoje informačních kompetencí CEVRO Univerzity**

„Česká republika schválila v roce 2014 zákon o kybernetické bezpečnosti, který vedl nejen ke smysluplnému nastavení základních institutů kybernetické bezpečnosti v Česku, ale byl i vzorem pro evropskou směrnici schválenou v roce 2016. Ta prošla revizí a návrh nového zákona o kybernetické bezpečnosti má reagovat nejen na tuto revidovanou evropskou normu, ale i na měnící se prostředí v kybernetickém prostoru. Nárůst počtu kybernetických incidentů, proměna jejich složení i nepokryté využívání hackerských kapacit státními aktéry jen potvrzují nutnost brát nastavení kybernetické bezpečnosti vážně. Komplexita dodavatelského řetězce a jeho nedávná zneužití nejen ve válečném konfliktu nám ukazují, že ani tuto oblast nesmíme podceňovat a věřím, že kompromis, který byl přijat na půdě gesčního Výboru pro bezpečnost obsahuje rozumné nastavení pravidel. Byť je nutné mít stále na paměti, že doba „neškodných" hackerů z Alabamy skončila a naše digitální infrastruktura a služby a jejich bezpečnost budou neustále testovány." — **Jaromír Novák, partner pro styk s veřejnou správou sdružení CZ.NIC**

Pro další informace kontaktujte

Lukáš Kraus

Email: lukas.kraus@odolnecesko.cz

Te.:: 773 794 347

www.odolnecesko.cz