



Kybernetická bezpečnost: rozšiřuje se okruh povinných subjektů

Dne 27. 12. 2022 byla zveřejněna nová směrnice EU o kybernetické bezpečnosti označovaná zkratkou NIS2. Tato směrnice rozšiřuje okruh povinných subjektů, na které bude dopadat právní regulace kybernetické bezpečnosti. Tuto směrnici má ČR povinnost do necelých 2 let promítnout do českého právního řádu.

Navrhovaná česká úprava

Národní úřad pro kybernetickou a informační bezpečnost („NÚKIB“) již zveřejnil návrh nového českého zákona o kybernetické bezpečnosti i návrhy souvisejících vyhlášek. Tyto návrhy nových právních předpisů navazují na směrnici NIS2 a upřesňují kritéria pro určení povinných subjektů v ČR. Připravovaná právní úprava se má týkat subjektů, které (i) splňují kritéria pro střední podnik nebo tato kritéria překračují a (ii) působí ve vybraných regulovaných odvětvích (např. v energetice, dopravě, zdravotnictví, vodárenství, veřejné správě či odpadovém hospodářství). Z toho vyplývá, že dojde k razantnímu nárůstu počtu povinných subjektů oproti současnému stavu. Novinkou má být také rozlišení povinných subjektů na ty, pro které budou platit přísnější požadavky na kybernetickou bezpečnost (tzv. režim vyšších povinností) a pro které budou platit o něco mírnější na kybernetickou bezpečnost (tzv. režim nižších povinností).

Sebeidentifikace

Dále NÚKIB navrhuje, aby pro podstatnou část povinných subjektů platila povinnost, že mají samostatně provést posouzení, zda se na ně nová právní úprava aplikuje či nikoliv (tzv. „sebeidentifikace“). Pokud z takového samostatného posouzení vyplýne, že jsou povinným subjektem, budou mít povinnost se následně registrovat u NÚKIB. Nesplnění této registrační povinnosti může být podle navrhované právní úpravy sankcionováno pokutou. Jedná se tedy o podobných mechanismus jako v případě registrace k DPH. Ačkoliv jsou jednotlivá kritéria pro sebeidentifikaci popsána v navrhované právní úpravě poměrně přesně a srozumitelně, při jejich aplikaci mohou povinné subjekty narazit na celou řadu účetně-právních problémů. Podstatným aspektem těchto kritérií je totiž posouzení, zda daný subjekt splňuje či překračuje kritéria pro střední podnik. To se posuzuje podle počtu zaměstnanců a obrátu či bilanční sumy roční rozvahy daného subjektu. Komplikované toto posouzení může být zejména u těch subjektů, které mají např. stážisty či přidělené zaměstnance nebo které jsou součástí skupiny vzájemně propojených osob či působí v rámci franšízy.

Možnosti dalšího postupu

Navzdory výše uvedenému, dokud není nová právní úprava schválena, nelze s jistotou určit, jaký bude přesný okruh povinných subjektů a jaké konkrétní povinnosti budou muset splnit. Navrhovaná právní úprava může v obou komorách Parlamentu doznat ještě značných změn. Zároveň však nelze spoléhat na to, že zákonodárce po schválení nové právní úpravy poskytne adekvátně dlouhou lhůtu na přípravu povinných subjektů před tím, než nový zákon nabude účinnosti. S přípravou je tedy potřeba začít dopředu.

Za těchto okolností lze potenciálním povinným subjektům doporučit alespoň následující postup:

- 1) seznámit se nyní s obsahem navrhované vyhlášky o regulovaných službách a zjistit, zda činnost daného subjektu spadá do některé z regulovaných oblastí;
- 2) předběžně posoudit, zda daný subjekt splňuje nebo překračuje kritéria pro střední podnik (což je však především účetní otázka);
- 3) zejména v případě, že se bude jevit pravděpodobné, že dojde k naplnění kritérií pro sebeidentifikaci jako povinného subjektu, zahájit školení vybraných klíčových zaměstnanců a vedoucích pracovníků (a to jak z právních, tak technických aspektů kybernetické bezpečnosti);
- 4) průběžně sledovat legislativní vývoj v této oblasti a tomu postupně uzpůsobovat svůj postup.

Závěrem je třeba ještě zmínit, že určením, zda se na daný subjekt bude aplikovat nová regulace kybernetické bezpečnosti, celý proces přizpůsobení se nové právní úpravě teprve začíná. Povinné subjekty budou muset plnit celou řadu povinností a provést řadu kroků, na které je potřeba se taktéž dopředu připravit. Proto je znalost toho, zda a v jakém režimu (vyšším či nižším) se nová právní úprava na daný subjekt uplatní, zcela klíčová.

Oblasti kybernetické bezpečnosti se intenzivně věnujeme a průběžně sledujeme legislativní vývoj v této oblasti. V případě Vašeho zájmu Vám rádi poskytneme asistenci (např. při posouzení naplnění kritérií pro sebeidentifikaci, zhodnocení rizik přijetí či nepřijetí příslušných opatření i bližší seznámení s novou právní úpravou).

Mgr. Ing. Jan Havel
jan.havel@actlegal-rhl.com

Mgr. Bc. Jakub Adámek
jakub.adamek@actlegal-rhl.com