Povinné subjekty podle nové regulace kybernetické bezpečnosti

V nedávné době došlo v ČR k několika velmi závažným kybernetickým útokům (např. na nemocnici v Benešově, Fakultní nemocnici v Brně či Národní knihovnu). Tématu kybernetické bezpečnosti se proto věnuje zvýšená pozornost. Z legislativního hlediska však dosud platilo, že se zákonná regulace kybernetické bezpečnosti aplikovala pouze na ty nejvýznamnější či největší subjekty.[1] To se však velmi pravděpodobně změní.

Dne 27. 12. 2022 byla zveřejněna nová směrnice EU o kybernetické bezpečnosti označovaná zkratkou NIS2.[2] Jedním z požadavků této směrnice je, aby se právní regulace kybernetické bezpečnosti týkala všech subjektů ve vybraných regulovaných odvětvích, pokud splňují kritéria pro střední podnik nebo tato kritéria překračují.[3] Zároveň směrnice uvádí, že bez ohledu na velikost daného subjektu se má právní regulace kybernetické bezpečnosti uplatnit např. na ty subjekty, u nichž by narušení jejich činnosti mohlo mít významný dopad (např. na ochranu zdraví či veřejnou bezpečnost).[4] To ukazuje, že do budoucna se právní regulace kybernetické bezpečnosti může uplatňovat na výrazně širší okruh subjektů než dosud.

Navrhovaná česká právní úprava

Na druhou stranu z kritérií stanovených ve směrnici ještě nelze činit konkrétní závěry o tom, kterých subjektů v ČR se bude nová regulace kybernetické bezpečnosti týkat. Obecně totiž platí, že směrnice je závazná pro členské státy EU. Pro povinné subjekty[5] bude rozhodující až národní právní úprava. Na její přípravu a schválení mají členské státy EU necelé 2 roky.[6] Dokud tedy nebude schválena nová česká právní úprava, lze ohledně okruhů povinných subjektů a jejich povinností činit jen předběžné závěry.

Národní úřad pro kybernetickou a informační bezpečnost („NÚKIB“) nicméně již zveřejnil návrh nového zákona o kybernetické bezpečnosti i návrhy souvisejících vyhlášek.[7] Díky tomu si lze udělat alespoň hrubou představu o budoucí právní úpravě v této oblasti. Zveřejněné návrhy předpokládají mimo jiné zavedení následujících změn:

- dojde k rozlišení povinných subjektů na (i) ty, pro které platí přísnější pravidla (tzv. režim vyšších povinností), a (ii) ty, pro které platí o něco mírnější pravidla (tzv. režim nižších povinností); a
- dojde k rozlišení povinných subjektů na (i) ty, které mají povinnost provést posouzení, zda na ně právní úprava dopadá, a pokud ano, registrovat se následně u NÚKIB,[8] a (ii) ty, na které se právní regulace kybernetické bezpečnosti uplatní pouze v případě, že je NÚKIB určí svým rozhodnutím jako povinný subjekt.[9]

Např. pro oblast zdravotnictví je tak navrhováno, že „sebeidentifikaci“ mají provést poskytovatelé zdravotní péče podle zákona o zdravotních službách,[10] přičemž:

- jedná-li se o (i) velký podnik nebo (ii) poskytovatele zdravotní péče, který disponuje nejméně 270 lůžky akutní péče, platí pro něj režim vyšších povinností; a

- jedná-li se o střední podnik, platí pro něj režim nižších povinností.[11]

Kromě toho může NÚKIB svým rozhodnutím určit jako povinný subjekt také ty poskytovatele zdravotní péče, kteří sice nesplňují výše uvedená kritéria pro sebeidentifikaci, ale splňují některé z tzv. „kritérií pro určení".[12] Takovým kritériem je mimo jiné to, že narušení určité služby/činnosti daného poskytovatele zdravotní péče by mohlo mít významný dopad na veřejné zdraví.

Obdobným způsobem jsou stanovena a strukturována kritéria pro sebeidentifikaci či určení ze strany NÚKIB i dalších subjektů z oblasti zdravotnictví (např. provozovatele zdravotnické záchranné služby, výrobce zdravotnických prostředků či výrobce léčivých přípravků a léčivých látek), ale i subjektů z celé řady dalších oblastí (např. energetiky, dopravy, vodárenství či chemického průmyslu).

Problematický aspekt sebeidentifikace

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.

Rozlišení na mikro, malé, střední a velké podniky se provádí pomocí posouzení počtu zaměstnanců, obratu či bilanční sumy roční rozvahy daného subjektu.[13] Komplikované se toto posouzení stává zejména u těch subjektů, které mají např. stážisty či přidělené zaměstnance nebo které jsou součástí skupiny vzájemně propojených osob či působí v rámci franšízy.[14] Posouzení, zda konkrétní subjekt naplňuje kritéria pro sebeidentifikaci dle nové právní úpravy kybernetické bezpečnosti, tak může být časově náročné a může vyžadovat součinnost externích právních a účetních poradců.

Zároveň je třeba zmínit, že za porušení povinnosti registrovat se u NÚKIB v případě splnění kritérií pro sebeidentifikaci, může takovému subjektu podle nové právní úpravy hrozit pokuta.[15] Není tedy vhodné tento aspekt sebeidentifikace podcenit.

Možnosti dalšího postupu

Jak již bylo zmíněno, dokud není nová právní úprava schválena, nelze s jistotou určit, jaký bude přesný okruh povinných subjektů a jaké konkrétní povinnosti budou muset splnit. V rámci projednání nového zákona o kybernetické bezpečnosti v obou komorách Parlamentu může totiž tento zákon ještě doznat mnohých změn. Vzhledem k tomu může být rizikové, pokud subjekty začnou realizovat významné investice do oblasti kybernetické bezpečnosti před tím, než budou vědět, jaká opatření budou povinny zavést.

Na druhou stranu, čas na schválení a zavedení nové právní úpravy je (vzhledem k obvyklé délce legislativního procesu) poměrně krátký. Nelze tedy spoléhat na to, že zákonodárce následně stanoví adekvátně dlouhou lhůtu pro přípravu před tím, než nový zákon nabude účinnosti. Potenciální povinné subjekty by si proto měly alespoň průběžně vyhodnocovat, do jaké míry je pravděpodobné, že se na ně nová právní regulace kybernetické bezpečnosti uplatní. V oblasti kybernetické bezpečnosti totiž platí víc než jinde, že, kdo je připraven, není překvapen.

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

1) seznámit se 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 středního podniku;
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;
4) průběžně sledovat legislativní vývoj v této oblasti a tomu postupně uzpůsobovat svůj postup.

Závěrem je pak už jen třeba zmínit, že určením, zda se na daný subjekt bude aplikovat nová regulace kybernetické bezpečnosti, celý proces teprve začíná. Povinné subjekty musí 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.

Mgr. Jakub Adámek, advokát
act Řanda Havel Legal advokátní kancelář s.r.o.

act
Řanda Havel Legal

Poznámky:

1 Srov. § 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
2 Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).
3 Srov. čl. 2 odst. 1 směrnice NIS2.
4 Srov. čl. 2 odst. 2 písm. c) směrnice NIS2.
5 Návrh nové české právní úpravy kybernetické bezpečnosti označuje subjekty, na které se bude tato nová právní regulace aplikovat, jako „poskytovatele regulované služby".
6 Srov. čl. 41 směrnice NIS 2.
7 Návrhy jsou dostupné na adrese: nis2.nukib.cz.
8 K tomuto účelu slouží tzv. kritéria pro identifikaci – viz příloha s kritérii pro identifikaci k navrhované vyhlášce o regulovaných službách.
9 K tomuto účelu slouží tzv. kritéria pro určení – viz § 4 navrhované vyhlášky o regulovaných službách.
10 Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách).
11 Srov. čl. 18 přílohy s kritérii pro identifikaci k navrhované vyhlášce o regulovaných službách.
12 Srov. § 4 navrhované vyhlášky o regulovaných službách.
13 Srov. čl. 2 přílohy doporučení 2003/361/ES.
14 Srov. čl. 3 až 6 přílohy doporučení 2003/361/ES.
15 Srov. str. 42 návrhu nového zákona o kybernetické bezpečnosti.