Cybrela

Kyber Alert

Květen 2023

Weinhold Legal

Kyberbezpečnost podle NIS2

Směrnice NIS2 a její účinnost

Dne 16. ledna 2023 nabyla účinnosti směrnice Evropského parlamentu a Rady (EU) 2022/2555, 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, tzv. **směrnice NIS2**. Tímto datem začala České republice a dalším členským státům Evropské Unie běžet **lhůta pro transpozici** minimálního standardu pravidel stanovených směrnicí NIS2, která **uplyne dne 17. října 2024**.

Národní kyberbezpečnost

Transpozice směrnice NIS2 se na národní úrovni začala řešit velmi záhy, a to přímo Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), jakožto příslušným ústředním správním orgánem pro oblast kyberbezpečnosti. První **návrh nového zákona o kybernetické bezpečnosti** byl zpracován a zveřejněn na internetových stránkách NÚKIB již necelý měsíc po zveřejnění směrnice NIS2, tedy koncem ledna 2023. V důsledku zveřejnění návrhu zákona byla v rámci veřejných konzultací vyzvána odborná veřejnost, aby k návrhu sdělila své podněty. V tuto chvíli se tak návrh zákona o kybernetické bezpečnosti nachází ve fázi relativního bezvětří, nicméně se dle plánu legislativních prací vlády na rok 2023 očekává, že **bude návrh zákona vládě předložen v prosinci 2023 k projednání**.

Ačkoli zatím nejsou přesně známé všechny povinnosti, které závazně stanoví až nový zákon o kybernetické bezpečnosti, lze již nyní **určit subjekty, které s jistotou budou (nově) podléhat povinnostem kyberbezpečnostního minima směrnice NIS2**. Vedle zřejmých povinných subjektů určených přímo směrnicí NIS2 nicméně tento právní předpis stanoví **členským státům možnost určit některé z povinných subjektů dle vlastního uvážení** s ohledem na důležitost či zvláštní povahu dané entity.

Povinné subjekty

Stěžejními kritérii pro určení subjektu, který „spadne“ pod režim nové kyberbezpečnostní legislativy a v jakém rozsahu, jsou primárně (i) **odvětví a pododvětví**, ve kterém subjekt provozuje svoji činnost a (ii) **velikost subjektu** ve smyslu doporučení Evropské komise 2003/361/ES o definici mikropodniků, malých a středních podniků. Určením dle těchto parametrů se **povinné subjekty rozdělí do dvou skupin**, skupiny **(1) základních subjektů** spadajících do režimu **vyšších povinností** a skupiny **(2) důležitých** subjektů spadajících do režimu **nižších povinností**. Zpozornět by měly zejména entity, které budou kromě naplnění kritéria velikosti **provozovat svoji činnost v následujících odvětvích**:

- **energetika,**
- **doprava,**
- **bankovnictví a infrastruktura finančních trhů,**
- **zdravotnictví,**
- **pitná a odpadní voda,**
- **digitální infrastruktura,**
- **veřejná správa,**
- **vesmír a výzkum,**
- **poštovní a kurýrní služby,**
- **nakládání s odpady,**
- **výroba, produkce a distribuce chemických látek,**
- **výroba, zpracování a distribuce potravin,** a
- **výroba zdravotnických prostředků, počítačů, elektronických a optických přístrojů a elektrických zařízení a strojů, motorových vozidel, přívěsů a návěsů a dalších dopravních zařízení**.

Cybrela

Kyber Alert

Květen 2023

Weinhold Legal

Určení povinných subjektů

Vzhledem k absenci příslušné povinnosti členských států, kterou by stanovila přímo směrnice NIS2, jakož i vzhledem k penzu informací, které je třeba mít pro dané posouzení k dispozici, budou subjekty povinny **provést hodnocení svépomocí**. Následně bude mít povinný subjekt povinnost **registrovat se** v rámci jedné ze zmiňovaných skupin **na portálu NÚKIB**. Povinnost registrace je návrhem zákona předvídána **do 30 dnů** ode dne, kdy subjekt zjistil, že naplňuje kritéria stanovená pro jednu ze skupin, **ale nejpozději do 90 dnů** od jejich faktického naplnění.

Kromě procesu sebeurčení povinných subjektů dle výše uvedených kritérií se však předpokládá, že **některé z nich určí přímo stát**, pravděpodobně prostřednictvím NÚKIB. V takové případě NÚKIB informuje povinný subjekt o jeho povinnosti přímo.

Už jen z rozsahu výše uvedených kritérií je zřejmé, že zvládnout **přípravnou fázi** ve výše uvedených lhůtách bude pro povinné subjekty **časově, personálně i jinak náročné**.

Povinnosti

Ač zatím neoficiální, dává návrh zákona o kybernetické bezpečnosti v reflexi na obecné minimum nastavené směrnicí NIS2 vcelku jasnou představu o povinnostech, které budou povinné subjekty muset dodržovat. Povinnosti se pak budou drobně lišit podle toho, do jakého z režimů povinný subjekt spadá. V návaznosti na **úvodní analýzu rizik**, resp. určení technických aktiv a provedení business impact analýzy v režimu nižších povinností, se tak jedná například o **zavedení**:

- aktivní **participace vrcholného managementu** na řízení kyberbezpečnosti;
- **nových manažerských / odpovědných rolí** k zajištění souladu povinného subjektu s povinnostmi dle návrhu zákona;
- **politiky** bezpečnosti informací;
- **smluvních doložek** pro zajištění bezpečnosti v rámci dodavatelského řetězce;
- **vzdělávání** v oblasti kyberbezpečnosti;
- **bezpečnostních opatření** a postupů pro hodnocení jejich účinnosti;
- **kryptografie** a případně šifrování informací;
- pravidel pro **řízení přístupových oprávnění;**
- vícefaktorového **ověření identity**, bezpečných **komunikačních nástrojů** a nástrojů pro nouzovou komunikaci;
- pravidel pro **zvládání** bezpečnostních **incidentů** a jejich **hlášení NÚKIB,** resp. provozovateli Národního CERT;
- pravidel **krizového řízení**;
- pravidel pro **kontinuitu činnosti, zálohování a zotavení** v souvislosti s bezpečnostním incidentem.

Sankce

Po uplynutí přechodného období, které se zatím předpokládá v délce jednoho roku od zápisu do evidence NÚKIB na základě předešlé registrace subjektu, tedy pravděpodobně **od listopadu 2025**, bude NÚKIB oprávněn ukládat sankce za nesplnění povinností stanovených návrhem zákona. Kromě **nápravných opatření** a **sankce pozastavení platnosti evropského certifikátu kybernetické bezpečnosti** uděleného dle nařízení Evropského Parlamentu a Rady (EU) 2019/881 (akt o kybernetické bezpečnosti) bude NÚKIB oprávněn uložit i **pokuty za správní přestupky** předběžně specifikované návrhem zákona, a to **až do výše 250 000 000 Kč** nebo **2 % čistého celosvětového ročního obratu subjektu či jeho konsolidačního celku**. Jen pro doplnění, oprávnění k udělení sankce v období **před listopadem 2025** bude mít NÚKIB v případě **nesplnění povinnosti včasné registrace povinného subjektu** udělením **pokuty až do nejvyšší**

Cybrela

Kyber Alert

Květen 2023

Weinhold Legal

možné výše.

Posledním druhem sankce, o kterém však už nebude rozhodovat NÚKIB, bude **soudy vydávané rozhodnutí o pozastavení výkonu řídící funkce** osob v postavení např. člena statutárního orgánu, vedoucího odštěpného závodu či prokuristy. Důsledkem této sankce bude **zákaz vykonávat danou funkci** vykonávanou v managementu základního subjektu, tedy **v rámci režimu vyšších povinností, až do odstranění zjištěných nedostatků, ale vždy alespoň po dobu 6 měsíců**.

Další kroky

Aktuálním úkolem každého subjektu je provést vyhodnocení, zda a případně v jakém rozsahu na něj povinnosti podle nové právní úpravy dopadnou. Za tímto účelem je naše advokátní kancelář připravena poskytnout Vám potřebné právní služby, a to v úzké spolupráci s konzultační společností Cybrela s.r.o.

Cybrela s.r.o. je konzultační společnosti na kyberneticko-informační bezpečnost, zejména s ohledem na organizační a procesní opatření. Její hlavní činnosti se zaměřují na ISO 27001, ISO 27005, risk management, TISAX, zákon a vyhlášku o kybernetické bezpečnosti, NIS2, nové návrhy zákona a vyhlášek o kybernetické bezpečnosti, outsourcing rolí manažera kybernetické bezpečnosti a auditora kybernetické bezpečnosti. S Weinhold Legal propojuje síly pro poskytnutí komplexních služeb pro klientelu v oblasti kyberneticko-informační bezpečnosti.

Mgr. Kateřina Hůtová, LLM., CISA
Cybrela s.r.o.
Manažer kybernetické bezpečnosti

Cyber Security tým Weinhold Legal

Martin Lukáš
Partner
martin.lukas@weinholdlegal.com

Tereza Hošková
Vedoucí advokát
tereza.hoskova@weinholdlegal.com

Michal Švec
Advokát
michal.svec@weinholdlegal.com

Klára Mladá
Advokát
klara.mlada@weinholdlegal.com

Jiří Kvaček
Advokát
jiri.kvacek@weinholdlegal.com

Deborah Paláková
Advokátní koncipientka
deborah.palakova @weinholdlegal.com