1. 11. 2023

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Proč by implementaci směrnice NIS2 neměli řešit ve firmách pouze IT specialisté?

V polovině roku 2024 by měla být dokončena transpozice evropské směrnice NIS2 do české legislativy. Směrnice se promítne do nového zákona o kybernetické bezpečnosti (ZKB) a souvisejících vyhlášek a ovlivní zhruba 6 000 subjektů, které doposud nemusely zákonné nároky na kyberbezpečnost prakticky řešit. Aby tyto subjekty splnily povinnosti vyplývající z nového zákona, budou muset implementovat řadu opatření. Zcela esenciální pak bude zapojit do celého procesu nejen IT specialisty, ale i další odborníky.

Na koho NIS2 a ZKB dopadne

Mezi zmíněných zhruba 6 000 subjektů patří střední a velké podniky a některé podniky bez ohledu na jejich velikost celkem v 60 službách rozdělených do 18 odvětví. Mezi službami lze nalézt poskytovatele online tržišť, internetové vyhledávače, poskytovatele ICT služeb, poskytovatele cloud computingu, ale i služby z „tradičních oblastí“, jako je energetika, doprava, zdravotnictví, zajišťování vody či potravinářství.

Opatření, která budou muset subjekty dodržovat

Subjekty, na které regulace spadá, budou muset dodržovat dvě skupiny opatření. První skupinou jsou opatření bezpečnostní, mezi které patří zajišťování minimální úrovně kybernetické bezpečnosti, rozdělení bezpečnostních rolí, zavedení procesů zvládání kybernetických bezpečnostních událostí, vedení dokumentace či řízení dodavatelů a přístupu. Druhou skupinou jsou technická opatření, která zahrnují používání kryptografických algoritmů či zajišťování dostupnosti služby. Jsou stanovena i nová pravidla týkající se lokalizace dat. Rozsah nových povinností se odvíjí od toho, zda bude daný subjekt spadat do režimu nižších či vyšších povinností.

Sankce při nedodržování opatření

Pokud subjekt nesplní dané povinnosti, hrozí mu vysoká pokuta – až 250 mil. Kč nebo 2 % čistého celosvětového ročního obratu.

Nová a konkrétní odpovědnost statutárních orgánů

Statutární orgány (např. jednatel společnosti s ručením omezeným, správní rada či představenstvo v akciové společnosti) by měly implementaci požadavků zakotvených v nové regulaci věnovat zvláštní pozornost, protože na ně navrhované znění zákona o kybernetické bezpečnosti vrhá novou odpovědnost.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) může dle návrhu nového zákona provádět ve společnosti, na kterou se regulace vztahuje, kontroly v oblasti kybernetické bezpečnosti. Pokud NÚKIB zjistí v rámci této kontroly nedostatky, může dané společnosti nařídit nápravná opatření, která je společnost povinna zavést a dodržovat.

Pokud ale společnost

- je subjektem v režimu vyšších povinností a
- nápravné opatření nedodrží či nesplní a
- toto nesplnění je způsobeno závažným či opakovaným neplněním povinnosti při výkonu řídící funkce, a to např. členem statutárního orgánu,

může soud na návrh NÚKIB zakázat této osobě po dobu nejméně 6 měsíců vykonávat řídící funkci, než dojde k naplnění nápravných opatření. Pokud tedy společnost nebude plnit povinnosti v souladu s regulací, ponesou osoby v řídících funkcích přímé následky. Rozhodnutí o pozastavení funkce bude navíc zveřejněno na internetových stránkách NÚKIB.

Dle směrnice NIS2 a návrhu vyhlášek k novému zákonu musí také vrcholové vedení společností, na které úprava dopadne, absolvovat pravidelná školení o kybernetické bezpečnosti. Do působnosti statutárního orgánu je také svěřeno další množství pravomocí, jako zajišťování bezpečnostních politik, informování zaměstnanců, podílení se na vypracovávání analýz a přijímání bezpečnostních opatření.

Požadavky směrnice NIS2 a ZKB není tedy možné přesunout pouze na IT oddělení. Regulace je rozsáhlá a vyžaduje nové technologické, procesní a právní prostředí.

Pro implementaci požadavků zákona je nejdříve nutné zjistit, zda se na vaši společnost nová úprava vztahuje. Protože platí pravidlo sebeaplikace, každý potenciálně regulovaný subjekt si musí svůj status vyhodnotit sám. Dále je nutné určit které konkrétní povinnosti na vás dopadají, jaká rizika z nich vyplývají a zavést potřebné kroky – zejména technologické, týkající se úpravy dokumentace, řízení procesů, nahlašování incidentů či školení.

Nejúčinnějším způsobem, jak zajistit řádnou implementaci, je zapojení právních, IT a compliance specialistů. Takový one-stop-shop vám zajistí efektivní implementaci všech aspektů. Dobře vybraný implementační tým vám pomůže s řízením dodavatelů, firemním governance či analýzou rizik. Zároveň vyhodnotí dopady do veškeré dokumentace, ať už smluvní, či do vnitřních předpisů, a upraví je. Posoudí i komplementaritu s dalšími předpisy, které se na vaši společnost vztahují, a vyhodnotí dosavadní rozhodovací praxi úřadů či soudů, abyste se vyhnuli případným problémům. Čistě IT specialisté zase připraví technologické řešení a posoudí dopady tohoto řešení do veškerých dotčených technologií.

Hana Gawlasová,
partnerka a advokátka

Marie Kejlová,
advokátní koncipientka

Deloitte Legal

Deloitte Legal s.r.o., advokátní kancelář

Churchill I
Italská 2581/67
120 00 Praha 2 – Vinohrady

Tel.: +420 246 042 100
e-mail: legalcz@deloittece.com

---

[1] Směrnice Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie.
[2] Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.
[3] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[4] Čímž není naplněna podmínka stanovená v čl. 17 odst. 1 písm. a) GDPR.
[5] Čl. 17 odst. 3 písm. b) GDPR.
[6] Čl. 17 odst. 3 písm. e) GDPR.

Další články:

- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus