NIS2 a česká cesta: Přísnější pravidla kybernetické bezpečnosti od listopadu 2025

Směrnice NIS2 — nový rámec kybernetické bezpečnosti v Evropě

Směrnice NIS2 je aktualizovaná legislativa Evropské unie v oblasti kybernetické bezpečnosti, která nahradila původní směrnici NIS z roku 2016. Byla schválena koncem roku 2022 a členské státy EU ji měly převzít do svého práva nejpozději do října 2024. NIS2 zavádí **jednotný rámec kybernetické bezpečnosti napříč 18 kritickými sektory** a výrazně tak rozšiřuje působnost oproti původní směrnici. Nově pokrývá odvětví jako elektronické komunikace, digitální služby (sociální sítě, cloud), vodní a odpadní hospodářství, kritická výroba, vesmír, doprava, energetika, zdravotnictví, finance a veřejná správa. Směrnice byla přijata, aby odstranila nedostatky prvního režimu NIS a reagovala na sílící kybernetické hrozby v Evropě.

Směrnice NIS2 výrazně **rozšiřuje okruh organizací** podléhajících kybernetické regulaci. Zavádí pravidlo podle velikosti podniku, takže všechny střední a velké podniky v určených odvětvích spadají do její působnosti. Prakticky to znamená, že každý subjekt s více než 50 zaměstnanci nebo s ročním obratem nad 10 milionů eur v těchto sektorech musí požadavky splňovat. Tím se pod regulaci dostává mnohem více poskytovatelů, nejen úzký okruh, jak tomu bylo doposud, což naplňuje princip **„stejná rizika, stejná pravidla“** napříč EU.

NIS2 vyžaduje, aby dotčené organizace zavedly základní opatření pro řízení kybernetických rizik. Patří sem povinnost mít bezpečnostní politiku a soubor opatření, jako jsou pravidelné analýzy rizik, zajištění bezpečnosti v dodavatelském řetězci, používání vícefaktorové autentizace pro přístupy, řádné zálohování dat, plány reakce na incidenty a periodické testování odolnosti systémů. Směrnice tak stanoví **minimální standardy kybernetické bezpečnosti**, které musí všechny dotčené subjekty splňovat. Cílem je zajistit společnou základní úroveň zabezpečení ve všech státech EU.

Směrnice **sjednocuje postupy a lhůty pro hlášení vážných kybernetických incidentů.** Organizace musí významný incident nahlásit příslušnému úřadu velmi

rychle. Musí totiž odeslat úvodní ohlášení do 24 hodin, průběžnou zprávu do 72 hodin a závěrečnou zprávu s podrobnostmi do 1 měsíce. Toto fázované hlášení zajišťuje, že národní týmy pro reakci na incidenty (CSIRT) a regulátoři obdrží včasné varování a mohou **koordinovat reakci a sdílet informace**. Standardizace hlášení napříč EU by měla zlepšit přehled o hrozbách a umožnit rychlejší společnou reakci na velké kybernetické útoky.

NIS2 klade důraz na to, aby kybernetická bezpečnost byla odpovědností vrcholového managementu. **Řídicí orgány** zásadních i významných subjektů (či jejich statutární zástupci) musí schválit a dohlížet na realizaci bezpečnostních opatření a mohou být voláni k odpovědnosti, pokud firma nesplní požadavky. Tím se kybernetická bezpečnost dostává na pořad jednání vedení firem, namísto aby zůstávala jen v gesci IT oddělení. V krajních případech umožňuje NIS2 členským státům dočasně zakázat vedoucím pracovníkům vykonávat manažerské funkce, pokud hrubě zanedbají své kybernetické povinnosti. **Přenesením odpovědnosti na management** chce EU motivovat firmy, aby kybernetická rizika braly strategicky vážně.

Směrnice NIS2 rovněž dává regulátorům **silnější nástroje pro vynucování pravidel**. Dozorové úřady v každé zemi získají větší pravomoci k prověřování a kontrole firem. Směrnice také stanoví vysoké sankce za nedodržení povinností, a to až 10 milionů EUR nebo 2 % celosvětového ročního obratu pro essential entities (subjekty s vyšším významem) a až 7 milionů EUR nebo 1,4 % obratu pro important entities (subjekty s nižším významem). Tyto horní hranice pokut (obdobné jako u GDPR) mají vytvořit silný odstrašující efekt v celé EU. NIS2 dále umožňuje vydávat závazné instrukce k nápravě a v krajním případě omezit činnost podniku do odstranění zjištěných nedostatků.

Směrnice NIS2 vyžaduje, aby každý stát přijal národní strategii kybernetické bezpečnosti a určil příslušné **orgány pro dohled nad plněním pravidel**. Posiluje také celoevropskou spolupráci. Například formálně zřizuje síť EU-CyCLONe pro koordinaci řízení rozsáhlých kybernetických krizí mezi členskými státy. NIS2 byla navržena v souladu s dalšími unijními předpisy, zejména s novým nařízením DORA (Digital Operational Resilience Act) pro finanční sektor a směrnicí CER o odolnosti kritických entit, aby se zabránilo překryvům a zmatkům v regulaci.

Stručně řečeno, směrnice NIS2 představuje zásadní **posílení kybernetických požadavků v Evropě**. Do regulace zahrnuje mnohem více organizací, stanovuje povinné minimální zabezpečení a dává úřadům ostřejší nástroje k vymáhání pravidel. Rozšířením záběru a sjednocením standardů má NIS2 eliminovat slabá místa v digitálním prostředí a dosáhnout vysoké společné úrovně **kybernetické odolnosti** v celé EU. Po přijetí NIS2 na úrovni EU se pozornost obrátila k implementaci v jednotlivých státech. Nyní se podíváme, jak tyto požadavky zavádí Česká republika prostřednictvím nového zákona o kybernetické bezpečnosti.

Česká implementace — nový zákon o kybernetické bezpečnosti

Pro transpozici NIS2 schválila Česká republika v roce 2025 **zcela nový zákon o kybernetické bezpečnosti** (publikován jako č. 264/2025 Sb.). Prezident zákon podepsal 26. června 2025 a účinnosti nabývá 1. listopadu 2025. Tento předpis nahrazuje dosavadní zákon z roku 2014 a do českého práva přenáší požadavky směrnice NIS2. Přijetí zákona se oproti unijnímu termínu zpozdilo, proto obsahuje přechodná období, aby se firmy mohly na nové povinnosti připravit.

Nový zákon výrazně rozšiřuje okruh regulovaných osob. Z původních několika stovek organizací na odhadovaných několik tisíc (až kolem 10 000) subjektů. Do jeho působnosti spadají **prakticky všechny střední a velké podniky v asi 18 odvětvích**, jež jsou považo-

vána za klíčová či významná. Patří mezi ně energetika, doprava, bankovnictví a finanční trhy, zdravotnictví, správa pitné vody a kanalizací, digitální infrastruktura a ICT služby, poštovní a kurýrní služby, veřejná správa (ústřední organy státu a kraje) či vysoké školy a další sektory. Mnohé podniky a instituce, které dosud kybernetické regulaci nepodléhaly (např. střední firmy v průmyslu, regionální nemocnice, komunální služby), nyní nově spadají pod dohled. Toto rozšíření z několika stovek až na deset tisíc dotčených entit sleduje zásadu NIS2, že při stejných rizicích mají platit stejná pravidla, a zajišťuje, aby **důležité služby napříč ekonomikou nepředstavovaly slabé místo bez zabezpečení**.

České znění zavádí obdobu rozdělení na essential a important entities tím, že rozlišuje subjekty v režimu **vyšších povinností a nižších povinností**. Vysoce významné organizace (např. velké podniky v kritické infrastruktuře) jsou zařazeny do vyššího režimu, zatímco méně významné subjekty spadají do nižšího režimu s mírnějšími požadavky. Toto „dvourychlostní" nastavení má zajistit přiměřenost skrze přísnější pravidla pro nejkritičtější subjekty a méně náročná pro subjekty s nižším rizikem. **NÚKIB jako dozorový orgán** může svým rozhodnutím zařadit konkrétní firmu do vyššího režimu, pokud poskytuje strategicky významnou službu, i když by jinak spadala jen do režimu nižšího.

Nový zákon ukládá regulovaným subjektům řadu povinností a stanovuje k nim termíny. Do 60 dnů od nabytí účinnosti zákona (případně do 60 dnů od chvíle, kdy se na organizaci začne zákon vztahovat) musí každý dotčený subjekt provést interní posouzení a nahlásit NÚKIB, že je regulovanou osobou, včetně informací o poskytovaných regulovaných službách. NÚKIB následně daný subjekt zaregistruje do evidence. Do 12 měsíců od registrace rovněž musí organizace zavést předepsaná bezpečnostní opatření a dosáhnout plného souladu s požadavky. Tato opatření vycházejí z **minima podle NIS2**. Například zavést systém řízení rizik, nastavit technická a organizační opatření (kontrola přístupů, vícefaktorové ověřování uživatelů, monitorování sítí, zálohování dat, plány reakce na incidenty, školení zaměstnanců apod.).

Subjekty ve vyšším režimu musí zavést pokročilejší prvky (např. detailní bezpečnostní politiky, řízení dodavatelských rizik, uchovávání auditních záznamů či havarijní plány) oproti těm v nižším režimu. Regulační zákon také vyžaduje **ohlašování kybernetických incidentů** s významným dopadem na služby. Česká úprava přejímá systém NIS2 pro rychlé vícestupňové hlášení (např. počáteční oznámení incidentu do 24 hodin atd.), jejíž podrobnosti stanovuje metodika NÚKIB. Firmy také musí průběžně **monitorovat hrozby a přijímat preventivní opatření**. Tyto lhůty jsou však poměrně ambiciózní. Odborníci upozorňují, že roční období na plné splnění požadavků je **velmi krátké**, a vyzývají firmy, aby s přípravami začaly včas. Pokud subjekt nedodrží stanovené termíny nebo opomene zavést předepsaná opatření, vystavuje se **riziku postihu za nesoulad**.

Česká implementace v některých ohledech **překračuje minimum směrnice NIS2**, aby posílila dohled nad kyberbezpečností. Regulované firmy musí vést evidenci ICT aktiv (používaný hardware, software, sítě) a zpracovat mapu datových toků ve svých systémech. Mají rovněž povinnost provádět nezávislý audit v souladu s kybernetickými požadavky alespoň jednou ročně. Zákon také posiluje **osobní odpovědnost manažerů**. Pokud by subjekt v režimu vyšších povinností opakovaně nebo závažně porušil své povinnosti, může NÚKIB navrhnout soudu uložit dočasný zákaz výkonu funkce člena statutárního orgánu až na 3 roky dané fyzické osobě. Taková diskvalifikace vedení firmy je novým sankčním prvkem (tzv. „gold-plating" směrnice) a přesahuje rámec základního textu NIS2. Jejím cílem je zajistit, že odpovědní vedoucí pracovníci budou kybernetickou bezpečnost skutečně brát vážně.

Dohled nad plněním zákona **vykonává NÚKIB**, který může provádět audity a kontroly u regulovaných subjektů. Nový zákon stanovuje sankční režim jinak věrný směrnici NIS2. Při závažném porušení hrozí pokuta až 250 milionů Kč nebo 2 % celkového obratu (podle toho, co je vyšší) pro subjekty ve vyšším režimu. U subjektů v nižším režimu může pokuta dosáhnout až 100 milionů Kč nebo 1,4 % obratu. Takto vysoké sankce (250 mil. Kč odpovídá zhruba 10 mil. €) před-

stavují oproti dřívějšímu zákonu **řádový nárůst a mají silně odrazující účinek**. NÚKIB může rovněž vydávat závazné pokyny k nápravě zjištěných nedostatků a v krajním případě omezit poskytování služby, pokud firma neodstraní zásadní zranitelnosti.

Nový český zákon byl vytvářen paralelně s unijními předpisy, přesto vznikají určité překryvy. Zejména **velké banky a finanční instituce**, na něž primárně dopadá evropské nařízení DORA, jsou zákonem o kybernetické bezpečnosti přesto označeny za „významné" nebo „kritické" subjekty. To může znamenat, že banky budou muset plnit povinnosti jak podle DORY, tak podle tohoto zákona. Odborníci poukazují na tuto dvojí regulaci a očekávají, že NÚKIB vyjasní, jak se povinnosti budou aplikovat, aby nedocházelo k duplicitám. Celkově však **český zákon doplňuje rámec NIS2** a další sektory (např. digitální finance či fyzická kritická infrastruktura) jsou řešeny samostatnými předpisy.

Nová legislativa zásadně **zvyšuje laťku kybernetické bezpečnosti v ČR**. Tisíce podniků a organizací musí urychleně posílit svou ochranu, což bude vyžadovat nemalé investice (podle některých odhadů mohou celkové náklady firem na implementaci jít do miliard korun). Ačkoli panuje shoda, že vzhledem k rostoucím útokům je posílení odolnosti nutné, **podnikatelská sféra se obává** krátkých termínů a vysokých výdajů s tím spojených. NÚKIB proto připravil metodickou podporu včetně online kalkulačky pro posouzení dopadu zákona na konkrétní organizaci. Hlavním cílem zákona je však naplnit vizi NIS2 o vysoké společné úrovni kybernetické bezpečnosti a ještě ji lokálně posílit, čímž se zvýší odolnost Česka vůči kybernetickým hrozbám. Nový předpis zavádí v českém prostředí přísnější pravidla, než dosud platila, a české firmy nyní mají poslední chvíle na to, aby se s povinnostmi sžily. Od listopadu 2025 už bude NÚKIB moci nekompromisně kontrolovat a postihovat jejich nedodržování.