5. 11. 2024

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

Připravované změny v právu kybernetické bezpečnosti podle směrnice NIS 2 v České republice

Digitalizace dnes hraje nezastupitelnou roli v mnoha oblastech života. Využití informačních a komunikačních technologií (ICT) se stalo nedílnou součástí každodenního fungování člověka ve společnosti. Na jednu stranu díky tomu dochází ke zvyšování efektivity, zjednodušení a automatizaci procesů a vznikají takřka neomezené možnosti komunikace a globálního propojení mezi jednotlivci i firmami. Na druhou stranu vzniká cela řada nových kybernetických hrozeb, jejichž dopady na společnost mohou být nezanedbatelné.

Kybernetická bezpečnost je proto jedním z nejdůležitějších aktuálních témat pro státy, organizace i jednotlivce a logicky se projevuje vývojem legislativy Evropské unie. O nejdůležitějších změnách v souvislosti se směrnicí NIS 2 bude pojednáno v tomto článku.

Směrnice NIS 2 a nový zákon o kybernetické bezpečnosti

- **Základní informace a hlavní rozdíly oproti původní směrnici NIS**

Evropská směrnice Network and Information Security 2 (NIS 2) navazuje na původní směrnici NIS z roku 2016, která byla první směrnicí Evropské unie zaměřenou ryze na oblast kybernetické bezpečnosti. Původní směrnicí NIS a její následnou implementací do vnitrostátního práva byly přijaty minimální požadavky napříč všemi členskými státy EU a představeny závazné harmonizované požadavky ke zvýšení bezpečnosti sítí a informačních systémů. Česká republika měla v době přijetí směrnice NIS už účinný zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB), který šel v řadě aspektů dál než směrnice. Pro Česko proto směrnice NIS nepřinášela žádné podstatné novinky (alespoň ne z pohledu dopadů na povinné subjekty). Česká republika dokonce jako první ze všech členských států přijala takto komplexní regulaci kybernetické bezpečnosti.[1]

Ani směrnice NIS 2 se výrazně neliší od regulace obsažené v současném českém ZKB a jeho prováděcích předpisech. Směrnice je reakcí na rostoucí hrozby v digitálním prostředí, potřebu zlepšit kybernetickou bezpečnost a zajišťovat fungování a kontinuitu poskytování základních služeb[2]. Kromě toho se směrnice pokouší odstranit rozdíly mezi jednotlivými členskými státy, které se objevují zejména na úrovni provádění povinností, hlášení incidentů a výkladu pojmu základní služba. Naplnění směřuje k zajištění větší právní jistoty a lepšího fungování vnitřního trhu.[3] Nová legislativa oproti původní směrnici NIS zejména:

- sjednocuje a rozšiřuje regulovaná odvětví a okruh povinných osob;
- zpřísňuje požadavky na zajištění důvěrnosti, dostupnosti a integrity informací pro vybrané organizace;
- zavádí přísnější sankce za nedodržení povinností;
- klade větší důraz na mezinárodní spolupráci a sdílení informací o kybernetických hrozbách; a
- požaduje koordinaci reakcí na kybernetické incidenty a zlepšení kapacit pro zvládání krizí.

Největší změnou, kterou směrnice NIS 2 skrze svoji transpozici do českého právního řádu přinese, je

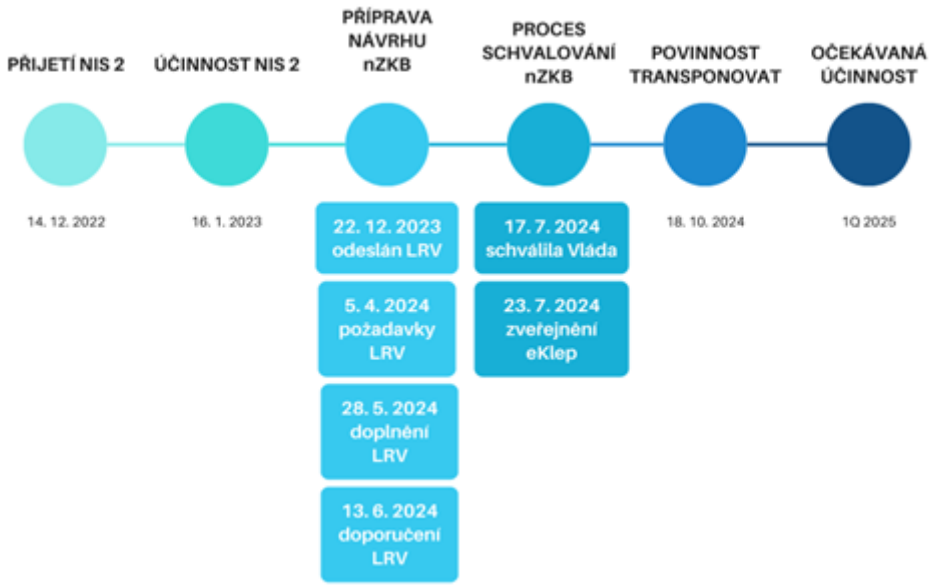
tedy hlavně rozšíření už (více či méně) existujících povinností na **mnohem více regulovaných subjektů**. Jednoduše — pro ty organizace, které doposud nemusely komplexně kybernetickou bezpečnost řešit budou některé povinnosti úplnou novinkou, i když jsou jiným osobám od účinnosti stávajícího zákona o kybernetické bezpečnosti důvěrně známé.

- **Transpozice do českého právního řádu**

Sama směrnice NIS 2 nemá horizontální přímý účinek,[4] přestože již byla přijata a 16. 1. 2023 nabyla účinnosti. To znamená, že v zásadě nezakládá práva ani povinnosti jednotlivcům mezi sebou, ale zavazuje státy. Ty byly povinny transponovat text směrnice do vnitrostátního práva ve stanovené lhůtě, tj. nejpozději do 17. 10. 2024 včetně.[5] Na základě již přijaté směrnice tak musí členský stát (Česká republika) připravit národní právní předpisy, zohledňující povinnosti podle směrnice NIS 2. **Směrnici NIS 2 budeme v České republice implementovat úplně novým zákonem o kybernetické bezpečnosti (nZKB).**

Návrh nZKB byl již vypracován a předložen příslušným orgánům v rámci legislativního procesu jeho tvůrcem, kterým je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Průběh legislativního procesu od přijetí směrnice NIS 2 až po schválení Vládou ČR a předložení nZKB Poslanecké sněmovně je znázorněn na časové ose níže. Účinnost se v současné době očekává hned na začátku roku 2025, tedy několik měsíců po uplynutí transpoziční lhůty stanovené NIS 2. Česká republika i přesto bude jeden z prvních států Evropské unie, který směrnici NIS 2 transponuje.



Faktické dopady na podnikatele a jiné organizace

- **Dopady na organizace podléhající původnímu ZKB**

Ačkoli s příchodem NIS 2 bude přijat zcela nový zákon, tento přístup NÚKIB zvolil zejména pro přehlednost a zachování stávající struktury pro adresáty normy. Pro povinné subjekty podle stávajícího ZKB, které budou i nadále muset plnit povinnosti dle nZKB, se nejedná o převratné

změny. Tyto budou muset „pouze" zrevidovat jejich soulad s nově příchozí legislativou, ale principy regulace a časově nebo finančně nejnáročnější povinnosti se výrazněji neliší oproti aktuálně účinné právní úpravě. Organizace tedy budou moci do značné míry využít aktuální postupy, zdroje a dokumentaci, které již mají zavedeny.

- **Pravidla pro určování povinných subjektů**

Největší změnou je rozšíření okruhu povinných osob, jelikož z původního počtu asi 500 povinných osob bude nová regulace dopadat až na 15násobek povinných subjektů.[6] V rámci konferencí a seminářů, které se průběžně konaly v roce 2024 na toto téma, se odhady odborníků různily a pohybovaly v rozmezí 12 000 – 15 000 povinných subjektů.[7] Regulace tedy bude relevantní pro značnou část organizací, které dosud neměly povinnost se kybernetickou bezpečností zabývat a úroveň kybernetické bezpečnosti byla ponechána čistě na jejich uvážení a principu dobrovolnosti (samozřejmě s přihlédnutím k jiným právním předpisům, např. GDPR na poli ochrany osobních údajů).

Nový zákon o kybernetické bezpečnosti počítá s tzv. regulovanými službami, rozdělenými do 22 odvětví, které stanoví prováděcí vyhláška k nZKB. V závislosti na významnosti či velikosti organizace pak bude muset každá organizace vyhodnotit, zda naplňuje podmínky pro regulovanou službu v jednom nebo více odvětvích a případně v jakém režimu (vyšších či nižších povinností). Celkem se jedná o následujících 22 odvětví:

1. Výkon svěřených pravomocí;
2. Energetika – Elektřina;
3. Energetika – Ropa a ropné produkty;
4. Energetika – Plynárenství;
5. Energetika – Teplárenství;
6. Energetika – Vodík;
7. Výrobní průmysl;
8. Potravinářský průmysl;
9. Chemický průmysl;
10. Vodní hospodářství;
11. Odpadové hospodářství;
12. Letecká doprava;
13. Drážní doprava;
14. Vodní doprava;
15. Silniční doprava;
16. Digitální infrastruktura a služby;
17. Finanční trh;
18. Zdravotnictví;
19. Věda výzkum vzdělávání;
20. Poštovní a kurýrní služby;
21. Obranný průmysl; a
22. Vesmírný průmysl.

Některé služby v těchto odvětvích budou předmětem regulace nZKB výlučně tehdy, dosahuje-li organizace podle doporučení Komise (metodiky obvykle používané v dotační agendě EU) alespoň určité velikosti (např. velký nebo střední podnik), nebo naplní-li jiné kritérium významnosti dané příslušnou vyhláškou k nZKB. Velikost se odvíjí od počtu zaměstnanců a obratu nebo bilanční sumy dané organizace. Naprostá většina regulovaných služeb se týká velkých nebo středních podniků, ale

nelze vyloučit, že minimálně do režimu nižších povinností mohou spadat i mikro či malé podniky.[8] Bez ohledu na velikost podniku proto doporučujeme každé organizaci, aby se s předmětnou vyhláškou seznámila a provedla základní posouzení (sebe-identifikaci), zda bude nebo nebude povinnou osobou, respektive poskytovatelem regulované služby podle nZKB.

Při určování velikosti podniku je nutné zohlednit také tzv. propojené subjekty, tedy mateřské, sesterské a dceřiné organizace podle předem stanovených kritérií. Tomuto tématu se věnuje řada jiných zdrojů, a proto jej nebudeme dále rozebírat.[9] Pokud je ale i relativně menší podnik členem skupiny podniků a poskytuje službu v nějakém z výše uvedených regulovaných odvětví, měl by zbystřit a provést sebe-identifikaci (viz níže).

- **Nejdůležitější povinnosti podle aktuálního návrhu nZKB**

Pokud organizace vyhodnotí, že na ni nZKB dopadá, aktuální návrh nZKB stanoví několik hlavních povinností, které musí každá taková organizace plnit. Nejprve je nutné ohlásit regulovanou službu přes tzv. Portál NÚKIB, a to do 60 dnů ode dne naplnění podmínek poskytování regulované služby dle prováděcí vyhlášky o regulovaných službách. Je tedy na každé organizaci, **aby sama včas zhodnotila, jestli na ni regulace dopadá či nikoliv, a pokud ano, aby se sama včas ohlásila NÚKIB**. Pokud bude nZKB skutečně účinný od ledna 2025, jak je nyní indikováno na webových stránkách NÚKIB, doporučujeme provést sebeidentifikaci nejlépe před koncem roku 2024. Úřad následně rozhodne o registraci a do 30 dní od doručení rozhodnutí o registraci je organizace povinná nahlásit kontaktní a další údaje.[10]

Dále musí organizace stanovit rozsah řízení kybernetické bezpečnosti, jinak bude do rozsahu spadat celá organizace bez ohledu na regulovanou službu a jinou činnost organizace. Ve stanoveném rozsahu je organizace povinna zavést a provádět bezpečnostní opatření v rozsahu a způsobem dle určeného režimu povinností (vyšší/nižší). Pokud dojde ke kybernetickému bezpečnostnímu incidentu, musí je organizace až na výjimky hlásit NÚKIB prostřednictvím Portálu NÚKIB a poskytnout na vyžádání NÚKIB dodatečné informace a součinnost k prošetření incidentu a přijetí vhodných opatření. Organizace v režimu nižších povinností musí hlásit kybernetické bezpečnostní incidenty pouze pokud mají významný dopad na poskytování regulované služby. NÚKIB má také možnost ad hoc vydat protiopatření (výstraha, varování, reaktivní protiopatření), které musí poskytovatelé regulovaných služeb zpravidla provést.

Klíčovým bodem je také zákonná povinnost zjišťovat a evidovat informace o dodavatelích bezpečnostně významných dodávek a zajištění dostupnosti strategicky významné služby z území České republiky. Mechanismus prověřování dodavatelů a zajištění dostupnosti se nicméně týká užšího okruhu regulovaných služeb, a to vybraných služeb elektronických telekomunikací, energetiky, dopravy, výkonu veřejné správy a digitální infrastruktury a služeb.

Odkud začít

- **Sebeidentifikace**

Nový zákon o kybernetické bezpečnosti bude přímo dopadat pouze na poskytovatele služeb ve vybraných odvětvích, které naplní kritérium významnosti nebo velikosti. Toto si ale musí každá organizace v zásadě vyhodnotit sama. Je proto stěžejní, aby každá organizace včas posoudila, zda poskytuje službu v regulovaném odvětví. Následně, zda naplňuje podmínku významnosti nebo velikosti. K tomu lze využít orientační kalkulačku dostupnou v Portálu NÚKIB[11].

Upozorňujeme, že organizace může z pohledu nZKB poskytovat i regulovanou službu, která nepředstavuje její hlavní podnikatelskou činnost, a proto je snadné ji v sebeidentifikaci omylem opomenout. Například pokud má společnost v důsledku využívání fotovoltaiky licenci od Energetického regulačního úřadu, může být poskytovatelem služby v odvětví energetika, i když se jinak jedná o „běžnou" výrobní společnost nebo společnost jiného typu.

Stejně tak často se stává, že společnost uvnitř holdingu poskytuje vedle jiných činností IT servis ostatním podnikům. Taková společnost pak velmi snadno naplní parametr poskytování tzv. řízené služby (*managed services)*, která podléhá regulaci nZKB, a z tohoto důvodu se může stát regulovaným subjektem, i když je jinak předmět její hlavní činnosti úplně odlišný.[12]

Obzvláště uvnitř koncernů nebo jiných typů propojených podniků může docházet k různému vzájemnému poskytování sekundárních služeb (zmiňoval jsem managed services, ale mohou to být i další, jako například doprava), které mohou vést k naplnění regulované služby. Je proto potřeba sebeidentifikaci provést odborně a zodpovědně.

- **Zmapování aktuálního stavu organizace**

Pokud výsledkem sebeidentifikace bude zjištění, že na organizaci regulace nZKB dopadá, organizace by se měla začít postupně připravovat na zavedení systému řízení bezpečnosti informací plněním povinností stanovených nZKB a prováděcími předpisy. Po sebeidentifikaci by dalším krokem mělo být zjištění, v jakém stavu z pohledu kybernetické bezpečnosti se organizace nachází.

- **Stanovení rozsahu řízení kybernetické bezpečnosti**

Dále je nutné určit, na které systémy, části infrastruktury a procesy se kybernetická bezpečnost vztahuje. Tento krok zahrnuje definování aktiv, která potřebují ochranu.

- **Analýza rizik**

Analýza rizik představuje proces identifikace potenciálních hrozeb, zranitelností a dopadů na klíčové systémy a data. Na základě této analýzy organizace zhodnotí pravděpodobnost výskytu jednotlivých rizik a jejich závažnost, což jí umožní rozhodnout, na jaká rizika se zaměřit při přijímání opatření.

- **Zavádění a provádění bezpečnostních opatření**

V posledním kroku se zavádějí konkrétní bezpečnostní opatření na základě zjištěných rizik. Tato opatření mohou zahrnovat technické, organizační a procedurální kroky, které minimalizují identifikovaná rizika a zajišťují ochranu kritických aktiv. Následně je důležité pravidelně kontrolovat a aktualizovat tato opatření, aby odpovídala aktuálním hrozbám.

Zavedení všech bezpečnostních opatření nebude pravděpodobně možné začít plnit v zákonné lhůtě. Je ale nutné předložit racionální a objektivní zdůvodnění, proč organizace nezavedla všechna bezpečnostní opatření a doložit, jaký systém řízení kybernetické bezpečnosti organizace má. V případě vyššího režimu se taková skutečnost projeví konkrétně v tzv. plánu zvládání rizik, v případě nižšího režimu v tzv. přehledu bezpečnostních opatření.[13]

Závěr

Přestože nový zákon o kybernetické bezpečnosti zatím nenabyl účinnosti a ani nebyl schválen, odborníci se shodují na tom, že všechny dotčené organizace se mají co nejdříve na přicházející

změny začít připravovat. Organizace, která nebude věnovat regulaci kybernetické bezpečnosti dostatečnou pozornost, nemusí po schválení nové národní úpravy stihnout splnit všechny stanovené povinnosti i přes poměrně štědré lhůty, a současně může v budoucnu narazit na vysokou poptávku po odbornících zejména z řad bezpečnostních expertů v oblasti IT, kterých je na trhu nedostatek. Přípravy přitom nyní nemusí znamenat významné náklady.

V prvé řadě je potřeba seznámit se s vyhláškou o regulovaných službách a ať už s pomocí odborníka, nebo na vlastní pěst zjistit, zdali na organizaci zákon o kybernetické bezpečnosti dopadá. Pokud ne, organizace by se ve vlastním zájmu měla tomuto tématu věnovat a zavést alespoň minimální bezpečnostní standard pro svá klíčová aktiva.

Poskytovatelé regulované služby, kterých se zákon nově bude týkat, ale i stávající „povinné osoby" by se měly poradit s odborníkem na kybernetickou bezpečnost a dle svých individuálních potřeb začít pracovat na compliance s novou legislativou. Čím dříve se organizace začne tomuto tématu věnovat, tím jednodušší a levnější pro ni proces pravděpodobně bude.

Nedoporučujeme spoléhat na jakákoli nabízená řešení na klíč jako tomu bylo v minulosti například v souvislosti s nařízením GDPR, jelikož každá organizace má jedinečné informační a komunikační systémy, vlastní zavedené procesy, lidské zdroje a jiný výchozí i cílový stav v organizaci. Každá organizace má jinou kyberbezpečnostní maturitu. Taková řešení stejně zpravidla nebudou odpovídat požadavkům nové legislativy a budou často zbytečnými, kontraproduktivními náklady.

Mgr. Jiří Císek
Partner

Mgr. Jan Přívora
Advokátní koncipient

Cisek.

Cisek, advokátní kancelář s.r.o.

Jana Babáka 2733/11
612 00 Brno

Tel.: +420 735 147 001
E- mail: office@akcisek.cz

---

[1] POLČÁK, Radim a SVANTESSON, Dan Jerker B. Information sovereignty: data privacy, sovereign powers and the rule of law. Cheltenham: Edward Elgar Publishing, 2017. ISBN 978-1-78643-921-5, s. 183.

[2] Bod 1 preambule směrnice NIS 2.

[3] Bod 4–7 preambule směrnice NIS 2.

[4] Směrnice v zásadě může mít tzv. vertikální přímý účinek. Jde zejména o případy, kdy jsou naplněny podmínky stanovené judikaturou Soudního dvora Evropské unie. Konkrétní podmínky zahrnují uplynutí implementační lhůty, vadnou implementaci nebo absenci implementace, přesnost a bezpodmínečnost směrnice, aktivní legitimaci osoby, která se přímého účinku dovolává, a zohlednění zásady, že přímým účiníkem směrnice nedojde k uložení povinnosti jednotlivci. Existují ale i problematické případy jistého „skrytého“ horizontálního přímého účinku u tzv. trojúhelníkových vztahů nebo v důsledku incidenčního efektu. Podrobněji se o účincích směrnice můžete dočíst například v CÍSEK, Jiří. Nepřímý účinek směrnice v judikatuře českých soudů. Diplomová práce. Brno: Masarykova univerzita, Právnická fakulta. 2016. Dostupné z: MUNI depozitáře závěrečných prací. K dispozici >>> zde.

[5] Česká republika, stejně jako mnoho dalších států EU tuto lhůtu nestihla dodržet.

[6] Sněmovní tisk 759/0. Vládní návrh zákona včetně důvodové zprávy a závěrečné zpráva z hodnocení dopadů regulace (RIA). Poslanecká sněmovna ČR. K dispozici >>> zde s. 86 a 87 a >>> zde, s. 5.

[7] Počítaje také tzv. sekundárně regulované subjekty, které sice nebudou povinnou osobou přímo podle nZKB, ale budou dodavatelem povinné osoby, a proto budou muset většinu povinností plnit taktéž, skrze závazky ve smlouvě s regulovaným subjektem.

[8] Nejčastěji by mohlo jít o poskytovatele veřejně dostupné služby elektronických komunikací.

[9] Při zadání výrazu „výpočet velikosti podniku“ i do prostého vyhledávání na internetu vyjede větší množství výsledků, od oficiálních pomůcek Evropské komise, přes články Agentury pro Podnikání a Inovace až po odborné nebo populární články advokátů, daňových poradců nebo dalších odborníků. Důležité ale bude při výpočtu velikosti zohledňovat i specifika přímo nZKB. V návrhu jsou určité (vítané) výjimky oproti obecným pravidlům. Tak například by se nemusely za propojené podniky počítat podniky, které mají zcela oddělená technická aktiva.

[10] Vizte ustanovení § 6 a 11 návrhu nového zákona o kybernetické bezpečnosti.

[11] Kalkulačku naleznete v Portálu NÚKIB k dispozici >>> zde.

[12] Na problém upozornily například HŮTOVÁ, Kateřina a KUBÍKOVÁ, Kateřina. Nejčastější chyby při samoidentifikaci dle nové kyberlegislativy. 2024. Dostupné >>> zde.

[13] Portál NÚKIB sekce FAQ v záložce Kde začít se zabezpečováním. Dostupné >>> zde.

Další články:

- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- 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