Nová směrnice EU o kybernetické bezpečnosti „NIS2“

17.05.2023 / 06:36

Kybernetická bezpečnost je v dnešní digitální době klíčovou oblastí, která má výrazný vliv na hospodářský a společenský život. Z tohoto důvodu byla v roce 2016 Evropskou Unií přijata směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii („NIS“), která zavedla minimální bezpečnostní požadavky pro poskytovatele kritických a digitálních služeb.

Karolína Liptáková
Weinhold Legal, s.r.o. advokátní kancelář

Dne 27. prosince 2022 byla přijata nová směrnice Evropského parlamentu a Rady (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii („**NIS2**“, případně „**Směrnice**“), která navazuje na NIS a má ambiciózní cíl zlepšit kybernetickou bezpečnost v celé Evropské Unii.

V následujícím článku se podíváme na pár důležitých vybraných změn, které s sebou nová Směrnice přináší, a to zejména tedy na její **tři hlavní cíle**:

- posílení kybernetické odolnosti poskytovatelů základních služeb
- zlepšení připravenosti EU na kybernetické útoky
- zvýšení účinnosti kybernetické odolnosti prostřednictvím přísnějších bezpečnostních požadavků a sankcí za jejich porušení

V neposlední řadě nás bude zajímat způsob implementace do českého právního systému, tedy jak bude na vnitrostátní úrovni zajištěno dodržování zásad, cílů a požadavků stanovených ve Směrnici.

Posílení kybernetické odolnosti poskytovatelů základních služeb

Prvním cílem směrnice NIS2 je zvýšit kybernetickou odolnost všech poskytovatelů základních služeb v EU. Rozsah působnosti směrnice NIS2 je na základě toho rozšířený oproti původní směrnici NIS a zahrnuje více poskytovatelů služeb. Všechny veřejné i soukromé organizace v rámci uvedených kategorií musí dodržovat stanovené opatření kybernetické bezpečnosti, což zajišťuje méně zranitelných oblastí mezi poskytovateli kritických služeb v EU.

Dle článku 2 Směrnice se **počet povinných osob rozšíří**, a to jednak rozšířením regulovaných odvětví (např. odvětví odpadového hospodářství), dále rozšířením stávajících regulovaných odvětví o nové regulované služby (např. stávající odvětví digitální infrastruktury o nové regulované služby cloud computingu nebo poskytovatele služeb a sítí elektronických komunikací) nebo změnou způsobu identifikace povinných osob.[1]

NIS2 také nyní zavádí obecné ustanovení pro určení regulovaných subjektů na základě **velikostního omezení**. Všechny střední a velké subjekty v odvětvích, jako jsou energetika, doprava, zdravotnictví a digitální infrastruktura, budou spadat do oblasti působnosti nových pravidel. Aktualizuje se také seznam odvětví a činností, na které se vztahují povinnosti v oblasti kybernetické bezpečnosti. V rámci jednotlivých členských států bude také existovat variabilita a příslušné instituce budou moci v legislativě přidat další subjekty, na které se budou pravidla vztahovat.[2]

Nově bude tato regulace aplikována na jakýkoliv subjekt, který splní dvě podmínky současně, a to podmínku poskytování alespoň jedné ze služeb uvedených ve Směrnici a zároveň kvalifikaci jako střední nebo velký podnik dle doporučení 2003/361/ES.

Směrnice se však nebude vztahovat na všechny subjekty. Některé subjekty, které vykonávají činnost v oblastech jako jsou obrana nebo národní bezpečnost, veřejná bezpečnost či prosazování práva, budou z působnosti Směrnice vyloučeny.[3]

Dále jsou kategorie subjektů, které spadají pod NIS2, rozděleny do dvou skupin, a to do skupiny „**základní**" a skupiny „**důležité**". Pro určení toho, jaká oblast spadá do jaké kategorie subjektů, je klíčové posouzení pravidel z článku 3 Směrnice.

Za **základní subjekty** se podle tohoto článku považují subjekty uvedené v příloze I Směrnice, které překračují stropy pro střední podniky, a to zejména v oblasti energetiky, dopravy, bankovnictví, pitné a odpadní vody, digitální a finanční infrastruktury či veřejné správy nebo vesmíru.

V rámci subjektů v kategorii **důležité** můžeme naopak zařadit oblasti jako poštovní a kurýrní služby, nakládání s odpady, chemický průmysl, potraviny či výroba a distribuce výrobků od zdravotních prostředků, počítačů až po elektroniku atd.

Oba typy subjektů musí dodržovat stanovené bezpečnostní opatření. Avšak hlavním rozlišujícím faktorem je to, že narušení služeb v kategorii "**základní**" by mělo závažné dopady na ekonomiku země nebo na celou společnost. Na základě toho subjekty v kategorii "**základní**" budou pod pravidelným dohledem a vyžaduje se proto určitá proaktivita v rámci monitorování. Subjekty v kategorii "**důležité**" budou sledovány až po nahlášení porušení předpisů.[4]

V rámci určení toho, do jaké kategorie budou jednotlivé subjekty spadat, musí být členskými státy vytvořen seznam základních a důležitých subjektů, stejně jako subjektů poskytujících služby registrace jmen domén. Tento seznam musí být pravidelně, alespoň každé dva roky, přezkoumáván a případně aktualizován členskými státy.[5]

Připravenost EU na kybernetické útoky

Druhým stěžejním cílem NIS2 je zlepšit celkovou připravenost EU na kybernetické hrozby a schopnost rychle na ně reagovat. Toho bude dosaženo zlepšením komunikace a sdílením informací mezi orgány EU a členskými státy. NIS2 proto stanovuje postupy, které musí být dodržovány v případě výskytu rozsáhlého kybernetického incidentu, aby byla zajištěna účinná reakce.

Každý členský stát musí stanovit nebo vytvořit jeden nebo více týmů **CSIRT**. Tyto týmy musí splňovat požadavky uvedené v článku 11 odst. 1 NIS2 a musí pokrývat alespoň odvětví, pododvětví a druhy subjektů uvedené v přílohách I a II. Tyto týmy budou zodpovědné za řešení incidentů podle stanoveného postupu. Týmy CSIRT musí spolupracovat a v příslušných případech si vyměňovat informace s odvětvovými nebo meziodvětvovými komunitami základních a důležitých subjektů podle článku 29 NIS2.[6]

Dále je povinností týmů CSIRT zajistit vysokou dostupnost svých komunikačních kanálů kdykoliv je to nezbytné, jasně tyto své komunikační kanály definovat a sdělit je spolupracujícím partnerům a subjektům, které spadají do jejich působnosti. [7]

Následně je důležitá právě **oznamovací povinnost**, kterou musí členské státy zajistit a to, že základní či důležitý subjekt oznámí svému týmu CSIRT nebo příslušnému orgánu každý incident, který má významný dopad na poskytování jeho služeb, a to bez zbytečného odkladu. V případě, že incident může negativně ovlivnit poskytování služeb příjemcům, musí dotčené subjekty oznámit incident bez zbytečného odkladu i jim. V případě bezpečnostního incidentu budou dotčené subjekty povinny poskytnout prvotní oznámení do 24 hodin a podrobnější informace do 72 hodin.[8]

Přísnější bezpečnostní požadavky a zvýšení sankcí za nedodržení povinností

Třetím cílem NIS2 je zlepšit koordinaci kybernetické odolnosti všech relevantních organizací prostřednictvím **přísnějších bezpečnostních požadavků** a sankcí za jejich porušení. Původní směrnice NIS umožňovala organizacím přizpůsobit si požadavky na kybernetickou bezpečnost, což sice umožňovalo flexibilitu, ale vedlo to k nejednotné úrovni bezpečnosti v celé EU.[9] Nové požadavky jsou lépe koordinované a jejich cílem je minimalizovat rozpory, které vytvořila původní směrnice NIS.

Nově jsou v souladu se směrnicí NIS2 stanoveny také **finanční sankce**, které mají být uděleny organizacím, které nedodržují požadavky NIS2. Ačkoliv je konkrétní výše sankcí ponechána na jednotlivých členských státech, NIS2 stanoví, že v závislosti na typu a velikosti organizace bude horní hranice pokuty ve výši alespoň 10 milionů EUR nebo 2 % hrubých ročních celosvětových příjmů organizace u základních subjektů a 7 milionů EUR nebo nebo 1,4 % hrubých ročních celosvětových příjmů u důležitých subjektů.

Způsob implementace do českého právního systému

Členské státy mají 21 měsíců na to, aby promítnuly směrnici NIS2 do svého národního práva. Tato lhůta začíná běžet ode dne, kdy směrnice NIS2 vstoupila v platnost. To znamená, že Česká republika by měla mít nový rámec povinností zavedený v národní legislativě do 16. října 2024.

Do českého právního systému by tato směrnice měla být implementována ve **formě zákona**, vzhledem k povaze rozsáhlých změn. Předpokládaná doba účinnosti je stanovena na druhou polovinu roku 2024.[10]

Weinhold Legal

---

[1] https://osveta.nukib.cz/mod/page/view.php?id=2582

[2] viz čl. 2 NIS2 a přílohy I, II

[3] viz čl. 2 ods. 7 NIS2

[4] viz čl. 3 NIS2

[5] viz čl. 3 ods. 3 NIS2

[6] viz čl. 10 NIS2

[7] viz čl. 11 ods. 1 NIS2

[8] viz čl. 23 NIS2

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

[10] https://osveta.nukib.cz/mod/page/view.php?id=2582