27. 4. 2023

ID: 116350

Nová evropská regulace přichází do Česka. V oblasti kybernetické bezpečnosti významně ovlivní až 6 tisíc tuzemských společností včetně finančního sektoru

Tuzemské firmy by se v brzké době měly začít připravovat na nové unijní regulace známé pod zkratkami NIS2 a DORA. Ty do českého podnikatelského prostředí přináší výrazný požadavek na zvýšení kybernetické bezpečnosti. Podle odhadů dopadnou až na šest tisíc českých firem a dalších organizací, které budou muset v následujících letech podstatně upravit svá bezpečnostní opatření, aby účinným způsobem snížily rizika možnosti kybernetických incidentů.

Směrnice **NIS2** (*Network and Information Security 2*) vstoupila v platnost na sklonku uplynulého roku a její transpozici do tuzemského právního řádu v současné době řeší Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Ten předložil na počátku roku návrh nového znění zákona o kybernetické bezpečnosti. *„Největší změnou oproti současné právní úpravě je několikanásobné rozšíření počtu regulovaných osob v ČR z původních několika set až na téměř šest tisíc. Zatímco současná právní úprava byla zaměřena především na kritickou infrastrukturu, veřejnou správu a telekomunikace, nově plánovaná legislativa se dotkne téměř všech středních a velkých podniků ve více než dvaceti odvětvích od výroby strojů a elektrických zařízení, přes potravinářský a chemický průmysl až po odpadové a vodní hospodářství,“* říká **Jan Tomíšek**, advokát a odborník na kybernetickou bezpečnost z ROWAN LEGAL.

„Rozšíření okruhu regulovaných institucí s ohledem na další regulace z balíčku kybernetické odolnosti EU může vyvolat ještě větší nedostatek odborníků kybernetické bezpečnosti na pracovním trhu. Zejména u menších subjektů nebude možné sestavit plnohodnotný tým odborníků na všechny oblasti kybernetické bezpečnosti, jednoduše nebudou k dispozici," uvedl **Jan Pich**, Cyber Security Manager, EY, a nastínil řešení: *„Stejně jako jsme se naučili využívat služeb sdílení automobilu nebo kol ve městech, tak i v oblasti kybernetické bezpečnosti lze očekávat zajišťování některých komponent formou outsourcingu*."

Současný návrh zákona rozděluje subjekty do dvou kategorií podle rozsahu vyžadovaných povinností. Do režimu vyšších povinností budou zahrnuty především velké podniky nad 250 zaměstnanců nebo nad 50 milionů EUR obratu. Na všechny ostatní subjekty – zejména středně velké podniky – nebudou kladeny tak vysoké nároky, nicméně ani ony se nevyhnou některým povinnostem. *„Společnosti budou muset především identifikovat, které informační systémy a jaká technika, dodavatelé či zaměstnanci jsou důležité pro jimi poskytovanou službu a následně tyto oblasti pokrýt bezpečnostními opatřeními. Například budou muset zabezpečit své sítě a systémy, nastavit systém řízení a určit odpovědné osoby nebo rychle reagovat na kybernetické útoky a další incidenty,“* doplnil **Jan Tomíšek**.

Návrh zákona rovněž stanovuje povinnosti i pro vrcholové vedení regulovaných firem, které se bude muset účastnit školení či se seznamovat s výstupy bezpečnostních kontrol. Při zjištění porušení povinnosti přitom bude moci NÚKIB navrhnout soudu pozastavení výkonu funkce člena vedení. Nové povinnosti budou organizace muset splnit do poloviny roku 2025, vzhledem ke komplexnosti

problematiky je vhodné začít aktivity plánovat již nyní.

Nařízení **DORA** (*Digital Operational Resilience Act*) v následujících měsících významným způsobem ovlivní celý finanční sektor EU, včetně toho v České republice. Vytvoří komplexní a jednotný soubor pravidel kybernetické bezpečnosti, kterému se budou muset přizpůsobit prakticky všechny finanční subjekty, ať už banky a stavební spořitelny, pojišťovny, investiční společnosti či obchodníci s cennými papíry. Hlavním cílem je ochrana finančních subjektů a jejich zákazníků před stále častějšími kybernetickými útoky. *„Finanční subjekty budou mít povinnost vypracovat komplexní strategii řízení ICT rizika a v jejím rámci zavést vhodná bezpečnostní opatření, detekovat incidenty, provádět pravidelná testování své digitální odolnosti, školit své pracovníky i upravit své smlouvy s dodavateli tak, aby vyhovovaly nařízení DORA,“* dodal **Josef Donát**, advokát a odborník na IT a bankovní regulaci z ROWAN LEGAL.

Další články:

- Advokátní kancelář Eversheds Sutherland posiluje svůj nemovitostní tým
- LEAGLE.ONE: Triangle Family Office #9: AI – nová infrastruktura světa, nebo přepálený příběh?
- Mgr. Helena Freyová, posiluje CEE Attorneys v oblasti M&A, Corporate Strategy & Technology
- Evropská unie rozšiřuje regulaci AI. Obsah generovaný nebo upravený umělou inteligencí musí být pro uživatele rozpoznatelný
- LEAGLE.ONE: Triangle Family Office #8: Umění jako investice: mezi vášní a rizikem
- ATREUM a K2 LEGAL se spojují: vzniká silná kancelář pro stavebnictví, technologie a byznys
- LEAGLE.ONE: Triangle Family Office #7: Tam, kde vznikají unicorny – Jak přemýšlí venture capital
- Ocenění Flamma získaly Ivana Janů, Jitka Chizzola, Ženy v právu a projekt Máš na to nadace Evy Pavlové
- ROWAN LEGAL povyšuje Jakuba Jirovského, Lindu Coufalovou, Evu Pavelkovou a Ondřeje Špičáka
- HAVEL & PARTNERS má tři nové counsely a na seniornější pozice postupuje dalších 16 lidí
- LEAGLE.ONE: Triangle Family Office #6: Startupy, AI a Izrael – Kde dnes vznikají miliardové výnosy