14. 6. 2024

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

Nařízení DORA: klíč k odolnosti finančního sektoru vůči digitálním hrozbám

V dnešním světě vysoké míry digitalizace čelí kybernetickým útokům celá rada institucí, počínaje od vlád přes nemocnice až po různé podnikatelské subjekty. Kybernetická bezpečnost a odolnost vůči kybernetickým útokům se tak stala ve vyspělých státech poměrně velkým tématem. Útokům se přitom nevyhnou ani finanční subjekty. Jelikož používaní informační a komunikační technologie (dále jen „IKT“) získalo v posledních dekádách při poskytování finančních služeb klíčovou úlohu, a to až do takové míry, že má zásadní význam při provádění obvyklých běžných funkcí všech finančních subjektů, předcházení kybernetickým útokům představuje pro finanční subjekty složitou výzvu.

Uvedené platí o to víc, že vysoká míra digitalizace ve spojení s vysokou mírou vzájemného propojení finančních subjektů a vzájemné závislosti systémů IKT mohou představovat systémovou zranitelnost, a to především s ohledem na možnost geograficky neomezeného rozšíření kybernetického incidentu vzniklého v kterémkoliv z přibližně 22 000 finančních subjektů Evropské unie na celý finanční systém.[1] I dílčí, na první pohled malé kybernetické útoky, tudíž mohou ohrozit stabilitu celého finančního sektoru. Tato stabilita je přitom úzce spjatá s důvěrou společnosti v daný sektor, a tato důvěra se dále zrcadlí na celkové výkonnosti ekonomiky.

Nutnost chránit finanční sektor od kybernetických útoků je proto nepřehlédnutelná. Evropská unie reaguje na tuto potřebu nařízením Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011, známým také jako DORA (Digital Operational Resilience Act) (dále jen „**Nařízení**“ nebo „**DORA**“), které s cílem zabezpečení kontinuity služeb finančních subjektů přináší pro tyto subjekty řadu nových požadavků. Následující řádky Vám proto v krátkosti představí hlavní prvky Nařízení a regulované subjekty. Aby ovšem nebyly jenom o povinnostech, dotknou se i výhod, které s sebou implementace nových opatření přináší.

Hlavní prvky Nařízení

Svého cíle má DORA dosáhnout prostřednictvím 4 základních pilířů, kterými jsou (i) řízení IKT rizik, (ii) řízení kybernetických incidentů, (iii) penetrační testy a (iv) kontrola nejen dodavatelů IKT, ale také subdodavatelů a ostatních článků dodavatelského řetězce.

První pilíř, tedy řízení rizik IKT, je založen především na zavedení bezpečnostních opatřeních. Bezpečnostními opatřeními se přitom rozumí opatření technická, organizační a procesní. Rozsah zavedení těchto opatření bude u jednotlivých subjektů založen na zásadě proporcionality, a tedy s přihlédnutím k jejich velikosti, celkovému rizikovému profilu, povaze a rozsahu a složitosti služeb, činností či operací.

V rámci druhého pilíře, a tedy v rámci řízení kybernetických bezpečnostních incidentů, se vyžaduje především implementace funkčního systému pro řízení kybernetických útoků. Zahrnuje nejen opatření pro identifikaci útoků, ale také postup pro zvládaní incidentu, obnovu dat a oznámení incidentu České národní bance jako dozorovému orgánu.

Jak je již uvedeno, třetí pilíř je založen na povinnosti finančních institucí pravidelně testovat svou digitální odolnost. Rozsah testování přitom zahrnuje nejen testování systémů a aplikací, ale také ověřování funkčnosti procesů řízení kybernetických incidentů. Nařízení přitom klade na vykonavatele penetračních testů poměrně přísné nároky v podobě nejen auditu vlastních penetračních testů, dobré reputace či certifikace, ale tak v podobě dostatečného profesního pojištění.

Čtvrtý pilíř je představován především řízením rizik spojených s třetími osobami, tedy osobami napříč dodavatelským řetězcem. Finanční subjekty budou povinně prověřovat důvěryhodnost poskytovatelů IKT služeb a využívat pouze dodavatele uplatňující aktuální a kvalitní normy bezpečnosti informací. Nároky na dodavatelský řetězec se, přirozeně, promítnou také ve smluvní dokumentaci s jednotlivými (sub)dodavateli.

Regulované subjekty

Jak již bylo výše uvedeno, Nařízení se vztahuje na finanční subjekty. Co všechno si ale pod tímto pojmem představit? Samozřejmě, nejedná se pouze o úvěrové instituce, tedy banky a další instituce přijímající vklady a poskytující úvěr. Finančními subjekty je podle DORA i řada dalších subjektů, a to např. platební instituce, instituce elektronických peněz, vymezení poskytovatelé služeb souvisejících s kryptoaktivy, centrální depozitáře cenných papírů, registry obchodních údajů, pojišťovny a zajišťovny, zprostředkovatelé pojištění a zajištění a zprostředkovatelé doplňkového pojištění, poskytovatelé služeb IKT z řad třetích stran.[2]

Výhody implementace nových opatření

Již nyní je zřejmé, že implementace Nařízení přinese finančním subjektům značné dodatečné náklady. Tyto náklady budou ovšem z dlouhodobého hlediska kompenzovány připraveností finančních institucí čelit kybernetickým útokům, což sníží rizika ztrát a narušení služeb. Nezanedbatelnou výhodou je také posílením důvěry zákazníků či regulační shoda, na jejímž základě budou finanční subjekty dodržující Nařízení v souladu v evropskými předpisy, čím se minimalizuje riziko pokut či sankcí.

Účinnost

Nařízení nabyde účinnosti 17. ledna 2025. V této souvislosti je nutno upozornit, že již od tohoto data budou všechny subjekty, na které Nařízení dopadá, povinny plnit povinnosti, které jim Nařízení přináší. Nařízení tedy bude na finanční subjekty dopadat přímo, bez nutnosti implementace ve vnitrostátních úpravách jednotlivých států Evropské unie.

Závěr

Stabilita finančního systému je ve velké míře ohrožena kybernetickým útoky. DORA proto představuje zásadní krok v posilňovaní kybernetické odolnosti finančních subjektů napříč celou Evropskou unii. Implementace Nařízení sice přinese od 17. ledna 2025 finančním subjektům řadu nových povinností, podepíše se ale také na zvýšení jejich ochrany proti kybernetickým útokům, na posilnění důvěry zákazníků a na zabezpečení regulační shody. Nařízení tak připraví celý finanční sektor na budoucí hrozby přicházející ruku v ruce s digitálním pokrokem.

Deborah Paláková

Weinhold Legal

Weinhold Legal, s.r.o. advokátní kancelář

Florentinum
Na Florenci 15
110 00 Praha 1

Tel.: +420 225 385 333
Fax: +420 225 385 444
e-mail: wl@weinholdlegal.com

---

[1] Odst. 6 Preambule Nařízení

[2] Pro taxativní výčet viď článek 2 Nařízení

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