DORA přináší nové povinnosti a vyšší bezpečnost

V předchozím článku jsme si představili balíček právních předpisů v oblasti digitálních financí, jehož součástí je mimo jiné také návrh nařízení o digitální provozní odolnosti, též známý jako DORA. Jaké změny s sebou tento návrh přináší? Na to se podíváme nyní.

Primárním cílem směrnice je sjednocení pravidel pro řízení rizik v oblasti informačních a komunikačních technologií. „Tím, že harmonizuje pravidla pro řízení rizik v oblasti IKT a pro hlášení, testování a rizika v oblasti IKT spojená s třetími stranami, odstraňuje překážky a zlepšuje vytváření a fungování vnitřního trhu s finančními službami. Stávající nesrovnalosti v této oblasti jak na legislativní úrovni, tak na úrovni dohledu a rovněž nesrovnalosti na úrovni členských států a EU narušují fungování jednotného trhu finančních služeb, jelikož finanční subjekty působící ve více členských státech musí vyjma případů, kdy dochází k překrývání, plnit rozdílné regulatorní požadavky či očekávání orgánů dohledu, což může bránit výkonu jejich svobody usazování a poskytování služeb. Rozdílná pravidla narušují rovněž hospodářskou soutěž finančních subjektů stejného druhu v různých členských státech," uvádí se ve zprávě.

„Cílem nařízení DORA je sjednotit požadavky na řízení rizik v oblasti informačních a komunikačních technologií (IKT) a digitální provozní odolnosti u subjektů, které podléhají povolení a finančnímu dohledu. Ve všech regulovaných oblastech finančního trhu již nyní platí nějaká pravidla pro řízení rizik IKT. Tato pravidla jsou však rozdílná, v některých oblastech jsou jen rámcová či kusá, někde, jako např. v bankovnictví a platebních službách, jsou již nyní velmi robustní. Od účinnosti nařízení DORA budou všechny v něm vymezené subjekty podléhat jednotné regulaci řízení rizik v oblasti IKT. Nařízením to však nekončí, na ně budou navazovat regulatorně technické standardy (RTS) vypracované evropskými orgány pro finanční regulaci, a to po konzultaci s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA). Tyto RTS půjdou do velkého detailu a stanoví jasné mantinely správné praxe," uvedl k DORA Lumír Schejbal, advokát ve společnosti Schejbal & Partners.

Požadavků je několik

Digitální provozní odolnost vychází ze souboru klíčových zásad a požadavků na rámec řízení rizik v oblasti IKT, který je v souladu se společným odborným doporučením evropských orgánů dohledu. Tyto požadavky, inspirované příslušnými mezinárodními, vnitrostátními a odvětvovými normami, pokyny a doporučeními, se týkají specifických funkcí řízení rizik v oblasti IKT (identifikace, ochrana a prevence, detekce, reakce a obnova provozu, vzdělávání a rozvoj a komunikace). Aby finanční subjekty udržely krok s rychle se rozvíjející oblastí kybernetických hrozeb, musí jako nedílnou součást provozní strategie zachování provozu vytvořit a spravovat systémy a nástroje IKT, které minimalizují dopad rizik v oblasti IKT, nepřetržitě identifikovat všechny zdroje rizik v oblasti IKT, vytvořit ochranná a preventivní opatření, rychle zjišťovat anomální činnosti, uplatňovat specializované a komplexní strategie zachování provozu a plány pro případ havárie a plány obnovy provozu. Mezi základní požadavky patří:

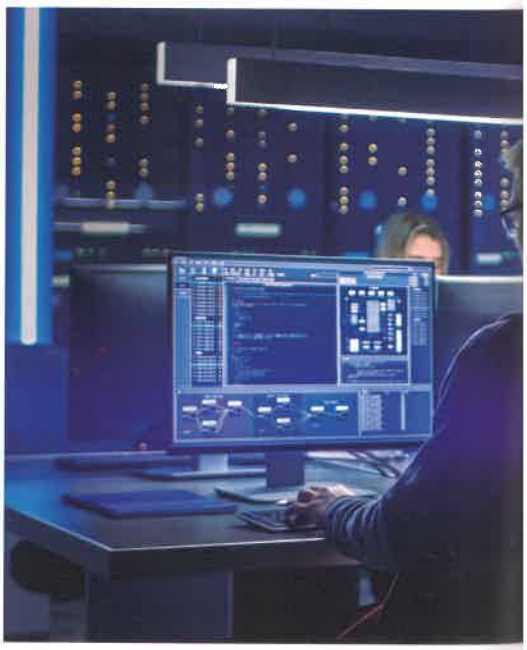
Aby finanční subjekty udržely krok s rychle se rozvíjející oblastí kybernetických hrozeb, musí jako nedílnou součást provozní strategie zachování provozu vytvořit a spravovat systémy a nástroje IKT, které minimalizují dopad rizik v oblasti IKT.

Požadavky na hlášení incidentů souvisejících s IKT – harmonizace a zjednodušení hlášení incidentů souvisejících s IKT je dosaženo zaprvé obecným požadavkem, aby finanční subjekty vytvořily a uplatňovaly proces řízení sledování a evidence incidentů souvisejících s IKT, a dále povinností jejich klasifikace podle vybraných kritérií. Příslušným orgánům musí být hlášeny pouze incidenty související s IKT, které jsou považovány za závažné. Hlášení je třeba zpracovávat podle společného vzoru a harmonizovaným postupem vypracovaným evropskými orgány dohledu. Finanční subjekty by měly předkládat prvotní, průběžné a závěrečné zprávy a informovat své uživatele a klienty v případech, kdy incident má nebo může mít dopad na jejich finanční zájmy.

Testování digitální provozní odolnosti – toto nařízení umožňuje proporcionální použití požadavků na testování digitální provozní odolnosti podle velikosti a profilů činnosti a rizik finančních subjektů: zatímco testování IKT nástrojů a systémů by měly provádět všechny subjekty, pokročilé testování prostřednictvím penetračních testů na základě hrozeb by se mělo týkat pouze subjektů určených příslušnými orgány. Nařízení rovněž stanoví požadavky na subjekty provádějící testování a uznávání výsledků penetračních testů.

Sledování rizik v oblasti IKT spojených s třetími stranami – zcela zásadní je dodržovat pravidla založená na zásadách, které platí pro sledování rizik, jež představují poskytovatelé služeb IKT z řad třetích stran. Nařízení harmonizuje hlavní prvky služeb a vztahů s poskytovateli služeb IKT z řad třetích stran. Tyto prvky se týkají minimálních aspektů považovaných za zásadní pro umožnění úplného sledování rizik v oblasti IKT. Změny se dotknou zejména smluv s těmito subjekty, které budou muset obsahovat daleko specifičtější informace. V neposlední řadě nařízení podporuje také sbližování dohledových přístupů nad riziky v oblasti IKT spojenými s třetími stranami ve finančním sektoru.

Sdílení informací – za účelem zvýšení povědomí o rizicích IKT, minimalizace jejich ší-



ření, podpory obranných prostředků finančních subjektů a technik zjišťování hrozeb toto nařízení umožňuje, aby finanční subjekty zajistily vzájemnou výměnu operativních a jiných informací o kybernetických hrozbách.

Dotkne se to všech, ale pokrok neomezí

Nařízení bude mít dopad na všechny regulované finanční instituce. „Některé subjekty, jako jsou např. banky či platební instituce, si s regulací poradí snadněji, protože již nyní musejí aplikovat sofistikované řízení rizik v oblasti IKT, jelikož jim to nařizuje směrnice PSD 2 a prováděcí akty jako např. Obecné pokyny EBA pro řízení rizik v oblasti IKT a bezpečnosti. Menší subjekty finančního trhu, jako jsou např. nebankovní obchodníci s cennými papíry, investiční společnosti či poskytovatelé služeb v oblasti kryptoaktiv, mohou mít s naplněním povinností problém. Požadavky regulace DORA totiž povedou k významnému zvýšení nákladů na bezpečnost a řízení rizik IKT, a to jak z důvodů technologických, tak i personálních," upřesnil Lumír Schejbal.

Nařízení počítá s aplikací zásady přiměřenosti, tedy finanční subjekty by měly mít možnost uplatňovat pravidla způsobem, který je přiměřený povaze, rozsahu a složitosti těchto subjektů a jejich činností. „Z licenční praxe však víme, že regulátor s uplatněním této zásady někdy aplikačně dost bojuje. Získání licence a vyhovění všem požadavkům nařízení tak bude pro menší hráče na finančním trhu velkou výzvou. I přesto se ale domnívám, že nařízení nepovede k pozastavení či zastavení vývoje fintechu. Vzhledem ke komplexnosti regulace řízení rizik IKT však bude vstup nových fintech společností do finančních odvětví zase o něco složitější. Společnosti budou muset vynaložit na získání licence v příslušném odvětví vyšší náklady, budou muset regulátorovi prokázat, že splňují vysoké nároky na regulaci IKT v daném odvětví. Opravdu inovativní fintechové služby si však cestu na trh najdou, buď ve spolupráci s investory, nebo již existujícími regulovanými subjekty v odvětví," dodal Lumír Schejbal.

S jeho slovy souhlasí také Maria Staszkiewicz, ředitelka České fintech asociace. „DORA zavede nové povinnosti ohledně reportování, vnitřních předpisů apod. – všechny firmy budou mít více práce, na malé to dopadne obzvlášť silně, protože budou muset např. zaměstnat další lidi. DORA by také měla zavést nové regulatorní technické standardy, otázka je, zda budou stejné pro všechny členské státy, nebo opět bude prostor pro národní variace."

Také samotné banky se staví k návrhu pozitivně. „Legislativní proces ještě sice není ukončen a návrh stále může doznat změn. Už nyní je ale možné říct, že se jedná o revoluční dokument. Především proto, že jde o první univerzální právní úpravu v této oblasti. Adresáty DORA jsou nejen finanční instituce a jiné regulované subjekty, ale za stanovených podmínek též poskytovatelé informačních a komunikačních technologií z řad třetích stran nebo vydavatelé kryptoaktiv. Pro ČSOB je informační bezpečnost (včetně provozní odolnosti) prioritou již dnes. Troufám si říci, že materiální dopad na naši činnost v této oblasti nebude nijak dramatický – banka již dnes pečlivě hodnotí rizika, a to na strategické i provozní úrovni, prověřuje své dodavatele a pravidelně testuje informační systémy. Přelomová je skutečnost, že nyní bude právním předpisem dán obecně závazný standard pro řízení ICT rizik. Pro banku, která náročně nastavený standard aplikuje již dnes, je DORA přínosem. Sjednocení požadavků na ošetření ICT rizik napříč trhem a jednotlivými EU jurisdikcemi je krok kupředu. Návrh nyní analyzujeme a je zřejmé, že aplikace DORA bude vyžadovat náklady. Budeme muset aktualizovat interní předpisy, procesy, revidovat smluvní dokumentaci. Bude potřeba nastavit nové role a odpovědnosti, řízení ICT rizik bude obsahovat nové instituty. Změny se budou muset promítnout v rámci celé finanční skupiny. Vyčíslení nákladů bude možné až po dokončení analýzy dopadů nového nařízení. Jsme přesvědčeni, že se bude jednat především o změny v oblasti organizační, administrativní a právní," uvedla k otázce DORA Lucie Vostatková, právnička v ČSOB.

Co se nákladů týče, vidí situaci podobně také Moneta. „Momentálně nedokážeme náklady odhadnout, nicméně zčásti počítáme s tím, že naše interní procesy již dnes naplňují požadavky tohoto návrhu nařízení, jelikož jsou v zásadě podobné s požadavky zákona o kybernetické bezpečnosti či Obecných pokynů EBA pro oblast řízení rizik v oblasti IKT a bezpečnosti či požadavky vyplývajícími z vyhlášky 163/2014 Sb. (rámec pro řízení IKT rizik, incident management, testování odolnosti IKT, řízení dodavatelů). Nicméně minimálně revizi procesů se nevyhneme," uvedla Zuzana Filipová, tisková mluvčí Monety.

Česká spořitelna pak počítá s cca desítkami milionů korun. „Za Finanční skupinu ČS můžeme uvést zatím opravdu jen hrubé odhady nákladů. Díky rozsahu služeb a požadavku na odborné činnosti, které budou vyžadovat rozšíření expertních týmů a zajištění testování odolnosti, se náklady související se zavedením mohou pohybovat v řádech desítek milionů korun," uzavřel Filip Hrubý, tiskový mluvčí České spořitelny.

B | Text Martina Sobková
www.bankovnictvionline.cz

Díky rozsahu služeb a požadavku na odborné činnosti, které budou vyžadovat rozšíření expertních týmů a zajištění testování odolnosti, se náklady související se zavedením mohou pohybovat v řádech desítek milionů korun.