Rada
Evropské unie

Brusel 24. září 2020
(OR. en)

Interinstitucionální spis:
2020/0268(COD)

11052/20
ADD 2

EF 229
ECOFIN 847
TELECOM 160
CYBER 169
IA 62
CODEC 872

PRŮVODNÍ POZNÁMKA

Odesílatel:	Jordi AYET PUIGARNAU, ředitel, za generální tajemnici Evropské komise
Datum přijetí:	24. září 2020
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	SWD(2020) 204 final
Předmět:	PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE SOUHRN ZPRÁVY O POSOUZENÍ DOPADŮ Průvodní dokument k Návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2006/43/ES, 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 a (EU) 2016/2341

Delegace naleznou v příloze dokument SWD(2020) 204 final.

Příloha: SWD(2020) 204 final

EVROPSKÁ
KOMISE

V Bruselu dne 24.9.2020
SWD(2020) 204 final

This document corrects document SWD(2020) 204 final of 24.09.2020
Two references in the title of the cover page have been corrected.
Concerns the EN version only.
The text shall read as follows:

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN ZPRÁVY O POSOUZENÍ DOPADŮ

Průvodní dokument k

Návrh směrnice Evropského parlamentu a Rady,

kterou se mění směrnice 2006/43/ES, 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 a (EU) 2016/2341

{COM(2020) 596 final} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

Souhrnný přehled

Posouzení dopadů návrhu nařízení o digitální provozní odolnosti ve finančním sektoru

A. Potřeba opatření

Proč? Jaký problém se řeší?

Finanční sektor ve velké míře využívá informační a komunikační technologie (IKT). Současná pandemie COVID-19 tento proces pravděpodobně ještě uspíší, vzhledem k výhodám plynoucím ze zajištění neustálého vzdáleného přístupu k finančním službám. Spoléhání na digitální technologie s sebou však nese určité obavy: podniky musí být schopny zvládnout potenciální narušení fungování IKT, aby digitální incidenty a hrozby byly řešeny a bylo zachováno poskytování služeb. Ve značně provázaném finančním sektoru, který poskytuje zásadně důležité přeshraniční služby, na nichž závisí reálná ekonomika, jsou slabá místa vyplývající ze závislosti na IKT (ačkoliv to se týká všech odvětví ekonomiky) obzvlášť zřetelná, a to vzhledem k 1) intenzivnímu a širokému využívání IKT a 2) možnému riziku šíření dopadů provozního incidentu, k němuž dojde v jednom finančním podniku nebo finančním subsektoru, do dalších podniků či subsektorů, a nakonec i do celé ekonomiky.

Ačkoli je finanční sektor z hlediska tržní a regulační integrace trhů značně pokročilý a prospívá mu díky jednotnému souboru harmonizovaných pravidel („evropský jednotný soubor pravidel“), reakce EU na potřebu zvýšené operační odolnosti na horizontální i sektorové úrovni byla buď:

- založena na minimální harmonizaci, což nechávalo prostor pro vnitrostátní interpretaci a fragmentaci jednotného trhu, nebo
- příliš obecná a s omezenou působností, přičemž řešila v různé míře celkové provozní riziko a částečně regulovala některé složky digitální provozní *odolnosti* (např. řízení rizik v oblasti IKT, hlášení incidentů a riziko vyplývající z poskytování IKT třetími stranami), zatímco jinými se nezabývala (testování).

Intervence EU dosud neřešily provozní riziko způsobem, který by odpovídal potřebám finančních podniků zvládat slabá místa IKT, reagovat na ně a zotavit se z nich, ani neposkytuje orgánům finančního dohledu nástroje, aby mohly plnit svůj úkol spočívající v omezování finanční nestability, která z těchto slabých míst IKT vyplývá.

Stávající nedostatky a nesrovnalosti vedly ke vzniku mnoha nekoordinovaných vnitrostátních iniciativ (např. ohledně testování) a přístupů v oblasti dohledu (např. pokud jde o závislost na poskytování IKT třetími stranami), které se projevují v podobě překrývání požadavků a vysokých nákladů na administrativu a dodržování předpisů pro přeshraniční finanční podniky, nebo způsobují, že rizika IKT zůstávají nezjištěna a neřeší se. Celkově není zajištěna stabilita a integrita finančního sektoru, jednotný trh finančních služeb je i nadále fragmentován a následkem je oslabení ochrany spotřebitelů a investorů.

Čeho by měla tato iniciativa dosáhnout?

Obecným cílem je posílit digitální provozní odolnost finančního sektoru EU prostřednictvím zjednodušení a aktualizace stávajících právních předpisů EU ve finanční oblasti a zavedení nových požadavků tam, kde dosud existují nedostatky, se zaměřením na:

- zlepšení řízení rizik z hlediska IKT ve finančních podnicích,
- prohloubení znalostí orgánů finančního dohledu ohledně hrozeb a incidentů,
- zlepšení testování systémů IKT ve finančních podnicích a dále
- zlepšení dohledu nad riziky, která vyplývají ze závislosti finančních podniků na poskytování IKT třetími stranami.

Konkrétně by měl návrh vytvořit soudržnější a důslednější mechanismy pro oznamování incidentů a tím snížit administrativní zátěž finančních institucí a posílit účinnost dohledu.

Jakou přidanou hodnotu budou mít opatření na úrovni EU?

Jednotný trh finančních služeb EU upravuje rozsáhlá soustava právních předpisů stanovených na úrovni EU, která díky pasu EU umožňuje finančním podnikům povoleným v jednom členském státě poskytovat služby na celém jednotném trhu. V důsledku toho by pravidla na vnitrostátní úrovni nepředstavovala účinný způsob, jak posílit provozní odolnost finančních podniků, které tohoto pasu využívají. Evropský jednotný soubor pravidel navíc obsahuje, jako důsledek finanční krize, velmi podrobná a závazná pravidla, která řeší „tradičnější“ rizika, jako jsou úvěrová a tržní rizika, rizika selhání protistrany a rizika likvidity. Stávající ustanovení týkající se provozního rizika jsou nadále jen všeobecná. Aby bylo možné posílit digitální provozní odolnost, je nutné změnit ustanovení o provozních rizicích, která jsou již na úrovni EU určena – a mohou tedy být dále aktualizována a doplňována pouze na úrovni EU.

B. Řešení

Jaké legislativní a nelegislativní možnosti byly zvažovány? Je některá možnost upřednostňována? Proč?

Posouzení dopadů zvážilo tři možnosti, kromě základního scénáře žádná opatření týkající se právních předpisů EU v oblasti finančních služeb nepřijímat. Konkrétně:

- **„Nedělat nic“**: pravidla pro provozní odolnost by byla i nadále stanovena stávajícími rozdílnými ustanoveními, která se týkají finančních služeb v EU, částečně směrnicí o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii a již existujícími nebo budoucími vnitrostátními režimy.
- **Možnost č. 1 – posílit kapitálové rezervy**: byly by zavedeny další kapitálové rezervy, aby se zvýšila schopnost finančních podniků absorbovat ztráty, které by mohly vzniknout v důsledku nedostatečné provozní odolnosti.
- **Možnost č. 2 – akt o digitální provozní odolnosti finančních služeb**: tím by se zavedl komplexní rámec na úrovni EU, který by stanovil pravidla týkající se digitální provozní odolnosti pro veškeré regulované finanční instituce, jenž by
    - uceleněji řešil rizika IKT,
    - umožnil orgánům finančního dohledu přístup k informacím o incidentech souvisejících s IKT,
    - zajistil, aby finanční podniky posuzovaly účinnost svých opatření týkajících se prevence a odolnosti a aby určily slabá místa IKT,
    - posílil pravidla pro externí zajištění služeb, která platí pro nepřímý dohled nad třetími stranami – poskytovateli IKT,
    - umožnil přímý dohled nad aktivitami třetích stran – poskytovatelů IKT, když poskytují své služby finančním podnikům a
    - rovněž podněcoval výměnu informací o rizicích ve finančním sektoru.
- **Možnost č. 3 – akt o digitální provozní odolnosti v kombinaci s centralizovaným dohledem nad klíčovými třetími stranami – poskytovateli IKT**: kromě aktu o digitální provozní odolnosti (možnost č. 2) by vznikl nový orgán dohledu nad třetími stranami – poskytovateli klíčových služeb IKT pro finanční podniky. Tento akt by rovněž přesněji vyčlenil finanční sektor z oblasti působnosti směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Upřednostňovanou možností je možnost č. 2. Ve srovnání s ostatními možnostmi tato varianta splňuje většinu z cílů této iniciativy a zároveň zohledňuje kritéria účinnosti a soudržnosti. Tato možnost má také největší podporu zúčastněných stran.

Kdo podporuje kterou možnost?

Většina zúčastněných stran (soukromých, veřejných) souhlasí s tím, že aby bylo možné lépe chránit provozní odolnost finančních podniků, jsou nutná opatření na úrovni EU. Mnozí se rovněž domnívají, že opatření na úrovni EU jsou nutná k řešení regulační zátěže vyplývající z toho, že finanční podniky podléhají nesoudržným a duplicitním pravidlům stanoveným ve směrnici o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, v právních předpisech EU o finančních službách a v rámci vnitrostátních režimů (například pokud jde o oznamování incidentů). Pouze malý počet zúčastněných stran proto podporuje variantu nedělat nic. Několik zúčastněných stran vidí přínos v ochraně provozní odolnosti pomocí zvýšení kapitálových rezerv (možnost č. 1). Jedná se o tradiční přístup k provoznímu riziku, zejména v bankovnictví, a jako takový ho zvažují například mezinárodní tvůrci norem. Kvalitativní opatření vyložená pod možností č. 2, která by zjednodušila a aktualizovala právní předpisy EU ve finanční oblasti a zavedla nové požadavky tam, kde existují nedostatky, a zároveň zachovala vazby na horizontální směrnici o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, se těší široké podpoře zúčastněných stran, které reagovaly na veřejnou konzultaci. Zatímco některé zúčastněné strany (zejména veřejné) vidí přínos v posíleném dohledu nad třetími stranami – poskytovateli IKT, jak je uvedeno v možnosti č. 3, vytvoření nového orgánu EU k tomuto účelu se setkává jen s omezenou podporou zúčastněných stran, stejně jako rozsáhlejší odklon od rámce směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

C. Dopady upřednostňované možnosti

Jaké jsou výhody upřednostňované možnosti (je-li nějaká doporučena, jinak uveďte výhody hlavních možností)?

Možnost č. 2 by řešila **rizika z hlediska IKT** v celém finančním sektoru posílením schopnosti finančních institucí zvládnout incidenty související s IKT. Tím by se snížilo riziko, že se kybernetický incident rychle rozšíří po finančních trzích. Ačkoliv je obtížné odhadnout náklady provozních incidentů ve finančním sektoru (všechny incidenty nejsou oznámeny, rozsah nákladů je nejistý), průmyslové analýzy naznačují, že náklady pro finanční sektor v EU by se mohly pohybovat v rozmezí 2–27 miliard EUR ročně. Upřednostňovaná možnost by snížila tyto přímé náklady i jakékoli širší dopady, které by závažné kybernetické incidenty mohly mít na finanční

stabilitu. Odstranění překrývajících se **povinností informování a oznamování** by snížilo administrativní zátěž. Pro některé z největších bank by úspory s tím spojené mohly dosahovat 40 až 100 milionů EUR ročně. Přímé oznamování by také zvýšilo znalosti orgánů finančního dohledu o incidentech IKT. **Harmonizované postupy testování** by zvýšily odhalování dosud neznámých slabých míst a rizik. Rovněž by se snížily náklady, zejména pro přeshraniční podniky. Očekávané celkové přínosy společného přístupu k testování by pro 44 největších přeshraničních bank mohly dosáhnout částky 11–88 milionů EUR. Zavedením soudržného souboru pravidel pro řízení rizik vyplývajících z **poskytování služeb IKT třetími stranami** by měly finanční podniky větší kontrolu nad tím, jak třetí strany – poskytovatelé IKT – dodržují regulační rámec, což by mohlo podpořit orgány finančního dohledu. Dalším přínosem by byla obezřetnost vyplývající z dohledu, který by příslušné orgány vykonávaly nad třetími stranami – poskytovateli IKT. Celkově znamená upřednostňovaná možnost větší přínosy pro společnost díky odolnějšímu provoznímu prostředí pro všechny účastníky finančního trhu a posílení ochrany spotřebitelů a investorů.

Jaké jsou náklady na upřednostňovanou možnost (je-li nějaká doporučena, jinak uveďte náklady na hlavní možnosti)?

Upřednostňovaná možnost přináší jednorázové i opakující se náklady. Ty první vznikají kvůli investicím do systémů IT a je obtížné je vyčíslit vzhledem k různému stavu stávajících systémů v podnicích. Některé finanční podniky již investovaly značné prostředky do systémů IKT i bez regulačního zásahu. Znamená to, že pro velké finanční podniky budou pravděpodobně náklady na zavedení opatření tohoto návrhu nízké. Pokud jde o menší podniky, rovněž se očekávají nižší náklady, protože pro ně budou platit méně přísná opatření úměrná jejich menšímu riziku. Pokud jde o testování, odhadly evropské orgány dohledu, že náklady související s penetračními testy na zjišťování hrozeb se pohybují mezi 0,1 % a 0,3 % celkového rozpočtu dotčených podniků na IKT. Výrazně by se snížily náklady na oznamování incidentů, protože by nedocházelo k žádnému překrývání s oznamováním podle směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Orgánům finančního dohledu by rovněž vznikly určité náklady, protože by musely vykonávat dodatečné úkoly. Pokud by například příslušný orgán vykonával přímý dohled nad třetími stranami – poskytovateli IKT, očekávaný nárůst zaměstnanců na plný úvazek by byl pro hlavní orgán finančního dohledu jeden až pět zaměstnanců a pro zúčastněný orgán dohledu přibližně 0,25 plného úvazku zaměstnance.

Jaký bude dopad na podniky, včetně malých a středních podniků a mikropodniků?

Upřednostňovaná možnost by se týkala všech finančních podniků, aby se zvýšila provozní odolnost celého odvětví. Takto široká oblast působnosti je důležitá vzhledem k tomu, že je finanční sektor natolik propojený a že existuje s tím spojená potřeba mít celkově rozumný stupeň provozní odolnosti. Při určování klíčových požadavků v hlavních oblastech zásahu se však bude ve všech subsektorech, stejně jako v rámci každého subsektoru uplatňovat zásada proporcionality. Bude zohledňovat mimo jiné rozdíly v obchodních modelech, ve velikosti podniků, rizikový profil, systémový význam atd. Například pravidla týkající se oznamování incidentů a testování budou méně přísná pro menší finanční podniky.

Očekávají se významné dopady na vnitrostátní rozpočty a správní orgány?

Ne. Dodatečný dohled si může, jak bylo výše ukázáno, vyžádat v omezené míře dodatečné zdroje, které mohou plně nebo částečně (v případě poplatků za dohled) nést veřejné rozpočty.

Očekávají se jiné významné dopady?

Sociálně-ekonomické důsledky pandemie COVID-19 ukazují, jak jsou digitální finanční trhy a jejich provozní odolnost klíčové. Upřednostňovaná možnost by vytvořila solidní základnu pro využití přínosů digitální transformace tím, že zajistí provozní odolnost jednotného trhu finančních služeb, včetně bankovnictví a unie kapitálových trhů, na základě společného souboru pravidel a požadavků, které budou usilovat o bezpečnost, výkonnost, stabilitu a rovné podmínky. Tím se rovněž posílí postavení Evropy jako světového lídra v oblasti financí a digitální ekonomiky, což je cíl, který Komise vytyčila ve svém sdělení „Formování digitální budoucnosti Evropy“.

D. Návazná opatření

Kdy bude tato politika přezkoumána?

První přezkum by byl proveden 3 roky po vstupu tohoto právního nástroje v platnost. Komise by o svém přezkumu podala zprávu Evropskému parlamentu a Radě. Přezkum by podle potřeby mohla podpořit veřejná konzultace a dále studie, diskuse odborníků, šetření a semináře.