STANOVISKO EVROPSKÉ CENTRÁLNÍ BANKY

ze dne 11. dubna 2022

k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Úvod a právní základ

Evropská komise přijala dne 16. prosince 2020 návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 ([1]) (dále jen „navrhovaná směrnice“). Dne 3. prosince 2021 se Rada Evropské unie dohodla na obecném přístupu k navrhované směrnici ([2]). Pravomoc Evropské centrální banky (ECB) zaujmout stanovisko je založena na čl. 127 odst. 4 druhém pododstavci Smlouvy o fungování Evropské unie, neboť navrhovaná směrnice obsahuje ustanovení, která spadají do oblasti působnosti ECB, zejména pokud jde o podporu plynulého fungování platebních systémů, příspěvek k řádnému provádění opatření, která příslušné orgány přijímají v oblasti stability systému finančního trhu, a úkoly ECB, které se týkají obezřetnostního dohledu nad úvěrovými institucemi podle čl. 127 odst. 2 čtvrté odrážky, čl. 127 odst. 5 a čl. 127 odst. 6 Smlouvy. V souladu s čl. 17.5 první větou jednacího řádu Evropské centrální banky přijala toto stanovisko Rada guvernérů.

Obecné připomínky

ECB důrazně podporuje cíle navrhované směrnice spočívající ve zvýšení úrovně kybernetické odolnosti ve všech příslušných odvětvích, snížení rozdílů v odolnosti na vnitřním trhu a zlepšení úrovně informovanosti o situaci a kolektivní schopnosti připravit se a reagovat zajištěním účinné spolupráce v Unii.

ECB uznává, že je důležité zachovat pevné vazby mezi navrhovanou směrnicí a finančním sektorem, který by měl zůstat součástí ekosystému sítí a informačních systémů s cílem podpořit jednotné posuzování rizik souvisejících s informačními a komunikačními technologiemi (IKT) v celé Unii a podpořit účinnou meziodvětvovou výměnu informací a spolupráci při řešení kybernetických hrozeb. Za tímto účelem by měly mít příslušné orgány podle navrhovaného nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru ([3]) (dále jen „DORA“) možnost účastnit se strategických politických diskusí a technické činnosti skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, jakož i vyměňovat si informace a dále spolupracovat s jednotnými kontaktními místy a vnitrostátními skupinami pro reakci na počítačové bezpečnostní incidenty (týmy CSIRT) uvedenými v navrhované směrnici ([4]).

1. Oblast působnosti navrhované směrnice

1.1 ECB vychází z toho, že pokud jde o subjekty finančního sektoru, bude nařízení DORA považováno za odvětvový právní předpis, který zavádí požadavky na řízení kybernetických bezpečnostních rizik a oznamování incidentů, které jsou přinejmenším rovnocenné požadavkům stanoveným v navrhované směrnici ([5]). Ustanovení navrhované směrnice, která se týkají řízení kybernetických bezpečnostních rizik, oznamovací povinnosti, sdílení informací, dohledu a vymáhání, se proto nebudou uplatňovat na finanční subjekty, na něž se vztahuje nařízení DORA ([6]). Jak je uvedeno v odůvodnění navrhované směrnice, namísto ustanovení navrhované směrnice by měla platit ustanovení

([1]) COM(2020) 823 final.
([2]) K dispozici na internetových stránkách Rady www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) Viz odstavec 1.5 stanoviska Evropské centrální banky CON/2021/20 ze dne 4. června 2021 k návrhu nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru(Úř. věst. C 343, 26.8.2021, s. 1). Všechna stanoviska ECB jsou zveřejněna na internetových stránkách EUR-Lex. Čl. 17 odst. 5 a článek 42 nařízení DORA; článek 11 navrhované směrnice.
([5]) Čl. 2 odst. 6 navrhované směrnice.
([6]) 13. bod odůvodnění a čl. 2 odst. 6 navrhované směrnice.

nařízení DORA, která se týkají opatření k řízení rizik v oblasti IKT, řešení incidentů souvisejících s IKT a hlášení incidentů, testování digitální provozní odolnosti, ujednání o sdílení informací a rizik v oblasti IKT spojených s třetími stranami ([7]).

1.2 ECB rovněž konstatuje, že Rada ve svém obecném přístupu k navrhované směrnici předkládá pozměňovací návrh s cílem vyloučit z uplatňování navrhované směrnice „subjekty, které vykonávají činnosti v oblasti justice, parlamenty nebo centrální banky“ ([8]). ECB vychází z toho, že navrhovaná změna by se vztahovala na všechny základní úkoly a pravomoci Evropského systému centrálních bank (ESCB), jak jsou stanoveny v čl. 127 odst. 2 Smlouvy a v článku 3.1 statutu Evropského systému centrálních bank a Evropské centrální banky (dále jen „statut ESCB“), jako je podpora plynulého fungování platebních systémů. V této souvislosti se infrastruktury finančního trhu, které vlastní a provozuje Eurosystém, jako jsou TARGET2 a TARGET2-Securities, považují za infrastruktury, na něž se vztahuje navrhované vynětí centrálních bank z uplatňování navrhované směrnice, jež navrhuje Rada.

2. **Pravomoci ESCB a Eurosystému v oblasti dozoru**

2.1 Vedle prvořadého cíle ESCB udržovat cenovou stabilitu je jedním ze základních úkolů ESCB v souladu s čl. 127 odst. 2 Smlouvy podpora plynulého fungování platebních systémů ([9]). Při plnění tohoto základního úkolu mohou ECB a národní centrální banky poskytovat facility a ECB může vydávat nařízení proto, aby byly zajištěny účinné a spolehlivé zúčtovací a platební mechanismy uvnitř Unie a ve styku se třetími zeměmi ([10]). Při výkonu své úlohy v oblasti dozoru přijala ECB nařízení Evropské centrální banky (EU) č. 795/2014 (ECB/2014/28) ([11]) (dále jen „nařízení o SIPS“), kterým se provádí zásady CPSS-IOSCO pro infrastruktury finančních trhů ([12]) do přímo použitelného právního předpisu. Nařízení o SIPS stanoví požadavky na systémově významné platební systémy pro velké i malé platby, ať už ve veřejném nebo soukromém vlastnictví. Požadavky podle nařízení o SIPS již zahrnují mimo jiné řízení provozních rizik a vytvoření rámce kybernetické odolnosti ([13]).

2.2 Kromě systémově významných platebních systémů se dozor Eurosystému vztahuje i na platební systémy, které nejsou systémově významné, elektronické platební prostředky, schémata a mechanismy a další infrastruktury a poskytovatele kritických služeb, jak je stanoveno v rámci politiky Eurosystému v oblasti dozoru ([14]). Platební systémy a jiné mechanismy podléhající dozoru Eurosystému nejsou výslovně zahrnuty do oblasti působnosti navrhované směrnice ([15]). Vzhledem k tomu, že navrhovaná směrnice je nástrojem minimální harmonizace ([16]), prováděcí právní předpisy přijaté členskými státy by se mohly případně překrývat s pravomocí Eurosystému v oblasti dozoru. Aby se tomu zabránilo, měly by být v odůvodnění navrhované směrnice výslovně uznány pravomoci ESCB podle Smlouvy a statutu ESCB, jakož i pravomoci Eurosystému podle nařízení o SIPS a obecně podle rámce politiky Eurosystému v oblasti dozoru.

([7]) 13. bod odůvodnění navrhované směrnice.
([8]) Čl. 2 odst. 3a první pododstavec písm. b) obecného přístupu Rady k navrhované směrnici.
([9]) Čl. 127 odst. 2 SFEU a shodně článek 3.1 statutu ESCB.
([10]) Článek 22 statutu ESCB.
([11]) Nařízení Evropské centrální banky (EU) č. 795/2014 ze dne 3. července 2014 o požadavcích v oblasti dozoru nad systémově významnými platebními systémy (ECB/2014/28) (Úř. věst. L 217, 23.7.2014, s. 16).
([12]) Viz dokument Výboru pro platební a vypořádací systémy (CPSS) a technického výboru Mezinárodní organizace komisí pro cenné papíry (IOSCO), „Principles for Financial Market Infrastructures“ (Zásady pro infrastruktury finančního trhu) z dubna 2012, k dispozici na internetových stránkách Banky pro mezinárodní platby na adrese www.bis.org. V části Odpovědnost D těchto zásad se uvádí, že od všech členů CPSS a IOSCO se očekává, že tyto zásady budou uplatňovat na příslušné infrastruktury finančního trhu ve svých jurisdikcích v co největším rozsahu, který umožňují právní předpisy v jejich jurisdikci“.
([13]) Článek 15 nařízení (EU) č. 795/2014 (ECB/2014/28).
([14]) Viz dokument „Eurosystem oversight policy framework, revised version (July 2016)“, který je k dispozici na internetových stránkách ECB na adrese www.ecb.europa.eu
([15]) Článek 2 navrhované směrnice a přílohy I a II navrhované směrnice.
([16]) Článek 3 navrhované směrnice.

3. **Rizika v oblasti IKT spojená s třetí stranou, řízení rozsáhlých incidentů a krizí, sdílení informací a národní strategie kybernetické bezpečnosti**

3.1 *Řízení rizik v oblasti IKT spojených s třetí stranou*

3.1.1 Navrhovaná směrnice zmocňuje příslušné orgány, aby při výkonu svých donucovacích pravomocí v souvislosti se základními subjekty vydávaly závazné pokyny nebo příkaz požadující, aby tyto subjekty napravily zjištěné nedostatky nebo porušení povinností stanovených v navrhované směrnici ([17]). „Hlavní orgán dohledu" určený podle nařízení DORA může zároveň vydávat kritickým poskytovatelům služeb IKT z řad třetích stran doporučení s cílem řídit potenciální systémová rizika spojená s postupy externího zajišťování služeb a koncentrací třetích stran v oblasti IKT ([18]).

3.1.2 Vzhledem k tomu, že základní subjekt podle navrhované směrnice může být rovněž označen za kritického poskytovatele služeb IKT z řad třetích stran podle nařízení DORA, ECB zdůrazňuje ([19]), že je třeba zabránit vydávání protichůdných doporučení a závazných pokynů. ECB v této souvislosti vítá obecný přístup Rady k navrhované směrnici. Podle tohoto přístupu mají příslušné orgány při výkonu svých pravomocí v oblasti dohledu a vymáhání ve vztahu k základnímu subjektu, který je označen za kritického poskytovatele služeb IKT z řad třetích stran podle nařízení DORA, informovat „fórum dohledu" zřízené podle nařízení DORA ([20]).

3.2 *Řízení rozsáhlých incidentů a krizí*

3.2.1 Podle navrhované směrnice ([21]) musí členské státy určit jeden nebo více příslušných orgánů odpovědných za řešení rozsáhlých incidentů a krizí. Jak je se uvádí v odůvodnění navrhované směrnice, rozsáhlý incident by měl označovat incident s významným dopadem na nejméně dva členské státy nebo takový incident, při kterém narušení přesahuje schopnost členského státu na něj reagovat. Rozsáhlé incidenty mohou přejít ve skutečné krize, které narušují řádné fungování vnitřního trhu ([22]).

3.2.2 I když příslušné orgány určené podle nařízení DORA zůstávají odpovědné za řízení kybernetických bezpečnostních incidentů týkajících se finančních subjektů, spolupráce se strukturami a orgány zřízenými podle navrhované směrnice bude mít zásadní význam pro zajištění koordinované reakce v celé Unii. ECB by proto uvítala účast příslušných orgánů určených podle nařízení DORA, včetně ECB, v Evropské síti styčných organizací pro řešení kybernetických krizí (EU-CyCLONe) ([23]), pokud rozsáhlé kybernetické bezpečnostní incidenty a krize mají dopad na finanční sektor.

3.3 *Sdílení informací*

3.3.1 Jak bylo uvedeno výše, ECB důrazně podporuje spolupráci mezi příslušnými orgány určenými podle nařízení DORA se strukturami a orgány zřízenými podle navrhované směrnice. Sdílení informací mezi orgány může zejména umožnit meziodvětvovou výměnu znalostí, přispět k prevenci a účinnému řízení kybernetických útoků a podpořit jednotné posuzování rizik souvisejících s IKT v celé Unii. ECB nicméně zdůrazňuje, že výměna informací by se měla uskutečňovat pouze v případě, že existují jasně stanovené mechanismy klasifikace a sdílení informací doplněné odpovídajícími zárukami pro zajištění důvěrnosti ([24]). ECB vítá obecný přístup Rady k navrhované směrnici, který

([17]) Čl. 29 odst. 4 písm. b) navrhované směrnice.
([18]) Článek 31 nařízení DORA.
([19]) Viz odstavec 1.2 stanoviska CON/2021/20.
([20]) Čl. 29 odst. 10 obecného přístupu Rady k navrhované směrnici.
([21]) Čl. 7 odst. 1 navrhované směrnice.
([22]) 27. bod odůvodnění navrhované směrnice.
([23]) Článek 14 navrhované směrnice.
([24]) Viz odstavec 1.5 stanoviska CON/2021/20.

navrhuje pravidelnou výměnu relevantních informací mezi orgány ([25]), uzavření ujednání o spolupráci, která upřesní mechanismus pro výměnu informací ([26]), a automatické a přímé předávání oznámení o incidentech ([27]). V tomto ohledu je třeba zajistit, aby informace, které jsou důvěrné podle ustanovení o služebním tajemství podle nařízení DORA ([28]) nebo příslušných odvětvových právních předpisů ([29]), mohly být vyměňovány s příslušnými orgány uvedenými v navrhované směrnici pouze tehdy, pokud je tato výměna nezbytná k tomu, aby příslušné orgány mohly uplatňovat ustanovení navrhované směrnice ([30]).

3.4 *Národní strategie kybernetické bezpečnosti*

3.4.1 Podle navrhované směrnice jsou členské státy povinny přijmout národní strategie kybernetické bezpečnosti, v nichž vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji ([31]). Jak je se uvádí v odůvodnění navrhované směrnice, členské státy by měly finanční sektor nadále zahrnovat do svých strategií kybernetické bezpečnosti ([32]). Členské státy by měly v rámci národní strategie kybernetické bezpečnosti přijmout politiky zabývající se kybernetickou bezpečností v dodavatelském řetězci pro produkty a služby IKT využívané subjekty k poskytování služeb. Pokud jde o finanční sektor, měly by být národní strategie kybernetické bezpečnosti v souladu s regulačním rámcem, který vychází z nařízení DORA. V této souvislosti se ECB domnívá, že je třeba navrhovanou úpravu dále vyjasnit, aby se zajistilo, že vnitrostátní strategie kybernetické bezpečnosti budou v souladu s odvětvovými právními předpisy.

Konkrétní pozměňovací návrhy k těm ustanovením navrhované směrnice, která ECB doporučuje změnit, jsou uvedeny v samostatném technickém pracovním dokumentu včetně příslušného odůvodnění. Technický pracovní dokument je k dispozici v anglickém jazyce na internetových stránkách EUR-Lex.

Ve Frankfurtu nad Mohanem dne 11. dubna 2022.

Prezidentka ECB
Christine LAGARDE

([25]) Čl. 11 odst. 5 obecného přístupu Rady k navrhované směrnici.
([26]) Bod odůvodnění 23a obecného přístupu Rady k navrhované směrnici.
([27]) 13. bod odůvodnění obecného přístupu Rady k navrhované směrnici.
([28]) Článek 49 nařízení DORA.
([29]) Články 53 až 62 směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).
([30]) Viz čl. 2 odst. 5 a čl. 11 odst. 4 navrhované směrnice.
([31]) Článek 5 navrhované směrnice.
([32]) 13. bod odůvodnění navrhované směrnice.