STANOVISKO EURÓPSKEJ CENTRÁLNEJ BANKY

z 11. apríla 2022

k návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Úvod a právny základ

Európska komisia prijala 16. decembra 2020 návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 ([1]) (ďalej len „navrhovaná smernica“) Rada Európskej únie sa 3. decembra 2021 dohodla na všeobecnom smerovaní k navrhovanej smernici ([2]). Právomoc Európskej centrálnej banky (ECB) vydať stanovisko je založená na článku 127 ods. 4 druhom pododseku Zmluvy o fungovaní Európskej únie, keďže navrhovaná smernica obsahuje ustanovenia, ktoré patria do pôsobnosti ECB, najmä pokiaľ ide o podporu plynulého fungovania platobných systémov, prispievanie k hladkému uskutočňovaniu politík prijatých príslušnými orgánmi, ktoré sa týkajú stability systému finančných trhov, a úlohy ECB týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami podľa článku 127 ods. 2 prvej a štvrtej zarážky, článku 127 ods. 2, 5 a 6 zmluvy. V súlade s článkom 17.5 prvou vetou rokovacieho poriadku Európskej centrálnej banky Rada guvernérov prijala toto stanovisko.

Všeobecné pripomienky

ECB jednoznačne podporuje ciele navrhovanej smernice zvýšiť úroveň kybernetickej odolnosti vo všetkých príslušných odvetviach, znížiť nezrovnalosti na vnútornom trhu a zlepšiť úroveň situačnej informovanosti a spoločnej schopnosti prípravy a reakcie zabezpečením efektívnej spolupráce v Únii.

ECB uznáva, že je dôležité zachovať silné väzby medzi navrhovanou smernicou a finančným sektorom, ktorý by mal zostať súčasťou ekosystému sietí a informačných systémov (NIS) s cieľom podporiť konzistentné posudzovanie rizík súvisiacich s informačnými a komunikačnými technológiami (IKT) v celej Únii a podporiť účinnú medziodvetvovú výmenu informácií a spoluprácu pri riešení kybernetických hrozieb. Na tento účel by príslušné orgány mali mať podľa navrhovaného nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora ([3]) (ďalej len „ nariadenie DORA“) možnosť zúčastňovať sa na diskusiách o strategickej politike a na technických činnostiach skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, ako aj vymieňať si informácie a ďalej spolupracovať s jednotnými kontaktnými miestami a vnútroštátnymi jednotkami pre riešenie počítačových bezpečnostných incidentov uvedenými v navrhovanej smernici ([4]).

1. Rozsah pôsobnosti navrhovanej smernice

1.1 ECB vychádza z toho, že pokiaľ ide o subjekty finančného sektora, nariadenie DORA sa bude považovať za právny predpis špecifický pre dané odvetvie, ktorým sa zavádzajú požiadavky na riadenie kybernetickobezpečnostných rizík a na oznamovanie incidentov, ktoré sú svojím účinkom minimálne rovnocenné s požiadavkami stanovenými v navrhovanej smernici ([5]). Ustanovenia navrhovanej smernice, ktoré sa týkajú riadenia kybernetickobezpečnostných rizík, oznamovacích povinností, výmeny informácií, dohľadu a presadzovania práva, sa preto nebudú vzťahovať na žiadne finančné subjekty, na ktoré sa vzťahuje nariadenie DORA ([6]). Ako je uvedené v odôvodneniach navrhovanej

([1]) COM(2020) 823 final.
([2]) Dostupné na webovom sídle Rady www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) Pozri odsek 1.5 stanoviska Európskej centrálnej banky CON/2021/20 z 4. júna 2021 k návrhu nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora (Ú. v. EÚ C 343, 26.8.2021, s. 1). Všetky stanoviská ECB sa uverejňujú na webových stránkach EUR-Lex. Článok 17 ods. 5 a článok 42 nariadenia DORA; článok 11 navrhovanej smernice.
([5]) Článok 2 ods. 6 navrhovanej smernice.
([6]) Pozri odôvodnenie 13 a článok 2 ods. 6 navrhovanej smernice.

smernice, namiesto ustanovení navrhovanej smernice by sa mali uplatňovať ustanovenia nariadenia DORA, ktoré sa týkajú opatrení na riadenie rizík v oblasti IKT, riadenia incidentov súvisiacich s IKT a oznamovania incidentov, testovania digitálnej prevádzkovej odolnosti, mechanizmov výmeny informácií a rizík týkajúcich sa IKT zabezpečovaných tretími stranami ([7]).

1.2 ECB tiež poznamenáva, že Rada vo svojom všeobecnom smerovaní k navrhovanej smernici predkladá pozmeňujúci návrh s cieľom vyňať z uplatňovania navrhovanej smernice „subjekty, ktoré vykonávajú činnosti v oblasti súdnictva, parlamenty alebo centrálne banky“ ([8]). ECB vychádza z toho, že navrhovaná zmena by sa vzťahovala na všetky základné úlohy a právomoci Európskeho systému centrálnych bánk (ESCB), ako sú stanovené v článku 127 ods. 2 zmluvy a v článku 3.1 Štatútu Európskeho systému centrálnych bánk a Európskej centrálnej banky (ďalej len „štatút ESCB“), ako napríklad podpora plynulého fungovania platobných systémov. V tejto súvislosti sa infraštruktúry finančného trhu, ktoré vlastní a prevádzkuje Eurosystém, ako napríklad TARGET2 a TARGET2-Securities, považujú za infraštruktúry, na ktoré sa vzťahuje navrhované vyňatie centrálnych bánk z uplatňovania navrhovanej smernice, ktoré navrhuje Rada.

2. **Právomoci ESCB a Eurosystému v oblasti dohľadu**

2.1 Popri hlavnom cieli ESCB, ktorým je udržiavať cenovú stabilitu, a v súlade s článkom 127 ods. 2 zmluvy, je jednou zo základných úloh, ktorá sa má uskutočňovať prostredníctvom ESCB podporovanie plynulého fungovania platobných systémov ([9]). Pri plnení tejto základnej úlohy ECB a národné centrálne banky môžu poskytnúť zariadenia a ECB môže vydávať nariadenia na zabezpečenie účinnosti a spoľahlivosti zúčtovacích a platobných systémov v rámci Únie a voči iným krajinám ([10]). ECB pri výkone svojej úlohy dohľadu prijala nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 (ECB/2014/28) ([11]) (ďalej len „nariadenie o SDPS“), ktorým sa zásady CPSS-IOSCO pre infraštruktúry finančného trhu ([12]) transformujú do priamo uplatniteľného právneho predpisu. V nariadení o SDPS sa stanovujú požiadavky pre systémy pre veľké platby aj pre systémovo dôležité retailové platobné systémy, či už vo verejnom alebo súkromnom vlastníctve. Požiadavky podľa nariadenia o SDPS už zahŕňajú okrem iného riadenie prevádzkového rizika a ustanovenie stratégie kybernetickej bezpečnosti ([13]).

2.2 Okrem systémovo dôležitých platobných systémov sa dohľad Eurosystému vzťahuje aj na nesystémovo dôležité platobné systémy, elektronické platobné nástroje, schémy a mechanizmy a iné infraštruktúry a poskytovateľov kritických služieb, ako sa stanovuje v rámci politiky Eurosystému v oblasti dohľadu ([14]). Platobné systémy a iné mechanizmy podliehajúce dohľadu Eurosystému nie sú výslovne zahrnuté do rozsahu pôsobnosti navrhovanej smernice ([15]). Vzhľadom na to, že navrhovaná smernica je nástrojom minimálnej harmonizácie ([16]), vykonávacie právne predpisy prijaté členskými štátmi by sa mohli v konečnom dôsledku prelínať s právomocami Eurosystému v oblasti dohľadu. Aby sa tomu zabránilo, v odôvodneniach navrhovanej smernice by sa mali výslovne uznať právomoci ESCB podľa zmluvy a štatútu ESCB, ako aj právomoci Eurosystému podľa nariadenia o SDPS a vo všeobecnosti podľa rámca politiky Eurosystému v oblasti dohľadu.

([7]) Odôvodnenie 13 navrhovanej smernice.
([8]) Článok 2 ods. 3a prvý pododsek písm. b) všeobecného smerovania Rady k navrhovanej smernici.
([9]) Článok 127 ods. 2 ZFEÚ a článok 3.1 štatútu ESCB.
([10]) Článok 22 štatútu ESCB.
([11]) Nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami (ECB/2014/28) (Ú. v. EÚ L 217, 23.7.2014, s. 16).
([12]) Pozri odporúčania Výboru pre platobné systémy a systémy vyrovnania (CPSS)/ Technického výboru Medzinárodnej organizácie komisií pre cenné papiere (IOSCO), „Principles for financial market infrastructures“ (Zásady pre infraštruktúry finančného trhu) z apríla 2012, dostupné na webovom sídle Banky pre medzinárodné zúčtovanie www.bis.org. V zodpovednosti D uvedeného odporúčania sa uvádza, že od všetkých členov CPSS a IOSCO sa očakáva, že tieto zásady budú uplatňovať na príslušné infraštruktúry finančného trhu vo svojich jurisdikciách v čo najväčšom rozsahu, ktorý umožňujú právne predpisy v ich jurisdikcii.
([13]) Článok 15 nariadenia (EÚ) č. 795/2014 (ECB/2014/28).
([14]) Pozri dokument „Eurosystem oversight policy framework“, revidované znenie (júl 2016) dostupný na webovom sídle ECB www.ecb.europa.eu.
([15]) Článok 2 navrhovanej smernice a prílohy I a II k navrhovanej smernici.
([16]) Článok 3 navrhovanej smernice.

3. **IKT riziko tretej strany, riadenie incidentov a kríz veľkého rozsahu, výmena informácií a národná stratégia kybernetickej bezpečnosti**

3.1 *Riadenie IKT rizika tretej strany*

3.1.1 Navrhovaná smernica splnomocňuje príslušné orgány, aby pri vykonávaní svojich právomocí na presadzovanie práva v súvislosti s kľúčovými subjektmi vydávali záväzné pokyny alebo príkazy, ktorými sa od týchto subjektov vyžaduje napraviť zistené nedostatky alebo porušenia povinností stanovených v navrhovanej smernici ([17]). „Hlavný orgán dozoru“ určený podľa nariadenia DORA môže adresovať odporúčania externým poskytovateľom kritických IKT služieb s cieľom riadiť potenciálne systémové riziká súvisiace so zvýšenou mierou externého zabezpečovania funkcií a koncentráciou externých poskytovateľov IKT ([18]).

3.1.2 Vzhľadom na to, že kľúčový subjekt podľa navrhovanej smernice možno určiť aj za externého poskytovateľa kritických IKT služieb podľa nariadenia DORA, ECB opätovne zdôrazňuje ([19]), že by sa malo zabrániť vydávaniu protichodných odporúčaní a záväzných pokynov. ECB v tejto súvislosti víta všeobecné smerovanie Rady k navrhovanej smernici. Podľa uvedeného smerovania majú príslušné orgány pri výkone svojich právomocí v oblasti dohľadu a presadzovania vo vzťahu ku kľúčovému subjektu určenému ako externý poskytovateľ kritických IKT služieb podľa nariadenia DORA informovať „fórum pre dozor“ zriadené podľa nariadenia DORA ([20]).

3.2 *Riadenie incidentov a kríz veľkého rozsahu*

3.2.1 V súlade s navrhovanou smernicou ([21]) musia členské štáty určiť jeden alebo viac príslušných orgánov zodpovedných za riadenie incidentov a kríz veľkého rozsahu. Ako sa objasňuje v odôvodneniach navrhovanej smernice, incident veľkého rozsahu by mal znamenať incident s významným dosahom na najmenej dva členské štáty alebo incident, ktorý svojim narušením presahuje schopnosť členského štátu reagovať naň. Incidenty veľkého rozsahu môžu naplno prepuknúť v krízu, ktorá narúša riadne fungovanie vnútorného trhu ([22]).

3.2.2 Zatiaľ čo príslušné orgány určené podľa nariadenia DORA zostávajú zodpovedné za riadenie kybernetickobezpečnostných incidentov týkajúcich sa finančných subjektov, spolupráca so štruktúrami a orgánmi zriadenými podľa navrhovanej smernice bude rozhodujúca pre zabezpečenie koordinovanej reakcie v celej Únii. ECB by preto uvítala účasť príslušných orgánov určených podľa nariadenia DORA vrátane ECB v Európskej sieti styčných organizácií pre kybernetické krízy (EU-CyCLONe) ([23]), keď majú kybernetickobezpečnostné incidenty a krízy veľkého rozsahu vplyv na finančný sektor.

3.3 *Výmena informácií*

3.3.1 Ako už bolo uvedené, ECB jednoznačne podporuje spoluprácu medzi príslušnými orgánmi určenými podľa nariadenia DORA so štruktúrami a orgánmi zriadenými podľa navrhovanej smernice. Výmena informácií medzi orgánmi môže predovšetkým umožniť medziodvetvovú výmenu znalostí, prispieť k prevencii a účinnému riadeniu kybernetických útokov a podporiť konzistentné posudzovanie rizík súvisiacich s IKT v celej Únii. ECB však zdôrazňuje, že výmena informácií by sa mala uskutočňovať len v prípade, že sú jasne zavedené mechanizmy klasifikácie a výmeny informácií spolu s primeranými zárukami na zabezpečenie dôvernosti ([24]). ECB víta všeobecné

([17]) Článok 29 ods. 4 písm. b) navrhovanej smernice.
([18]) Článok 31 nariadenia DORA.
([19]) Pozri odsek 1.2 stanoviska CON/2021/20.
([20]) Článok 29 ods. 10 všeobecného smerovania Rady k navrhovanej smernici.
([21]) Článok 7 ods. 1 navrhovanej smernice.
([22]) Odôvodnenie 27 navrhovanej smernice.
([23]) Článok 14 navrhovanej smernice.
([24]) Pozri odsek 1.5 stanoviska CON/2021/20.

smerovanie Rady k navrhovanej smernici, v ktorom sa navrhuje pravidelná výmena relevantných informácií medzi orgánmi ([25]), uzatvorenie dohôd o spolupráci, v ktorých sa upraví mechanizmus výmeny informácií ([26]), a automatické a priame postupovanie oznámení o incidentoch ([27]). V tejto súvislosti by sa malo zabezpečiť, aby sa informácie, ktoré sú dôverné podľa ustanovení o služobnom tajomstve podľa nariadenia DORA ([28]) alebo príslušných právnych predpisov špecifických pre dané odvetvie ([29]), mohli vymieňať s príslušnými orgánmi uvedenými v navrhovanej smernici len vtedy, ak je táto výmena potrebná na to, aby príslušné orgány mohli uplatňovať ustanovenia navrhovanej smernice ([30]).

3.4 *Národná stratégia kybernetickej bezpečnosti*

3.4.1 Podľa navrhovanej smernice sú členské štáty povinné prijať národné stratégie kybernetickej bezpečnosti, v ktorých sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti ([31]). Ako sa uvádza v odôvodneniach navrhovanej smernice, členské štáty by mali naďalej začleňovať finančné odvetvie do svojich stratégií kybernetickej bezpečnosti ([32]). Členské štáty by mali v rámci svojich národných stratégií kybernetickej bezpečnosti prijať politiky zamerané na kybernetickú bezpečnosť v dodávateľskom reťazci produktov a služieb IKT, ktoré subjekty využívajú na poskytovanie svojich služieb. Pokiaľ ide o finančné odvetvie, národné stratégie kybernetickej bezpečnosti by mali byť v súlade s regulačným rámcom, ktorý vychádza z nariadenia DORA. V tejto súvislosti sa ECB domnieva, že je potrebná podrobnejšia úprava na zabezpečenie, aby národné stratégie kybernetickej bezpečnosti boli v súlade s právnymi predpismi špecifickými pre dané odvetvie.

V prípadoch, kde ECB odporúča zmenu navrhovanej smernice, navrhované znenie príslušných zmien je uvedené spolu s odôvodnením v osobitnom technickom pracovnom dokumente. Technický pracovný dokument je dostupný v anglickom jazyku na webových stránkach EUR-Lex.

Vo Frankfurte nad Mohanom 11. apríla 2022

Prezidentka ECB
Christine LAGARDE

([25]) Článok 11 ods. 5 všeobecného smerovania Rady k navrhovanej smernici.
([26]) Odôvodnenie 23a všeobecného smerovania Rady k navrhovanej smernici.
([27]) Odôvodnenie 13 všeobecného smerovania Rady k navrhovanej smernici.
([28]) Článok 49 nariadenia DORA.
([29]) Články 53 až 62 smernice Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).
([30]) Článok 2 ods. 5 a článok 11 ods. 4 navrhovanej smernice.
([31]) Článok 5 navrhovanej smernice.
([32]) Odôvodnenie 13 navrhovanej smernice.