Úradný vestník
Európskej únie

SK
Séria L

2024/1772

25.6.2024

DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2024/1772

z 13. marca 2024,

ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 ([1]), a najmä na jeho článok 18 ods. 4 tretí pododsek,

keďže:

(1) Cieľom nariadenia (EÚ) 2022/2554 je harmonizovať a zefektívniť požiadavky na nahlasovanie incidentov súvisiacich s IKT a prevádzkových alebo bezpečnostných incidentov súvisiacich s platbami, ktoré sa týkajú úverových inštitúcií, platobných inštitúcií, poskytovateľov služieb informovania o účte a inštitúcií elektronického peňažníctva (ďalej len „incidenty“). Keďže požiadavky na nahlasovanie sa vzťahujú na 20 rôznych typov finančných subjektov, klasifikačné kritériá a prahové hodnoty významnosti na určenie závažných incidentov a významných kybernetických hrozieb by sa mali stanoviť jednoduchým, harmonizovaným a konzistentným spôsobom, v ktorom sa zohľadňujú osobitosti služieb a činností všetkých príslušných finančných subjektov.

(2) S cieľom zabezpečiť proporcionalitu by klasifikačné kritériá a prahové hodnoty významnosti mali odrážať veľkosť a celkový rizikový profil, ako aj povahu, rozsah a zložitosť služieb všetkých finančných subjektov. Kritériá a prahové hodnoty významnosti by okrem toho mali byť navrhnuté tak, aby sa uplatňovali konzistentne na všetky finančné subjekty bez ohľadu na ich veľkosť a rizikový profil a aby v súvislosti s nahlasovaním nepredstavovali pre menšie finančné subjekty neprimeranú záťaž. S cieľom riešiť situácie, keď je určitým incidentom, ktorý sám osebe nepresahuje uplatniteľnú prahovú hodnotu, ovplyvnený významný počet klientov, by sa však mala stanoviť absolútna prahová hodnota zameraná najmä na väčšie finančné subjekty.

(3) V súvislosti s rámcami nahlasovania incidentov, ktoré existovali pred nadobudnutím účinnosti nariadenia (EÚ) 2022/2554, by sa mala zabezpečiť kontinuita pre finančné subjekty. Klasifikačné kritériá a prahové hodnoty významnosti by sa preto mali zosúladiť a inšpirovať usmerneniami orgánu EBA o nahlasovaní závažných incidentov podľa smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 ([2]), usmerneniami o pravidelnom informovaní a oznamovaní závažných zmien, ktoré majú orgánu ESMA predkladať archívy obchodných údajov, rámcom ECB/SSM pre nahlasovanie kybernetických incidentov a inými príslušnými usmerneniami. Klasifikačné kritériá a prahové hodnoty by mali byť vhodné aj pre finančné subjekty, na ktoré sa pred nariadením (EÚ) 2022/2554 nevzťahovali požiadavky na nahlasovanie incidentov.

(4) Pokiaľ ide o klasifikačné kritérium „výška a počet transakcií, ktoré sú ovplyvnené incidentom“, pojem transakcie je široký a zahŕňa rôzne činnosti a služby v rámci odvetvových aktov uplatniteľných na finančné subjekty. Na účely uvedeného klasifikačného kritéria by mali byť doň zahrnuté platobné transakcie a všetky formy výmeny finančných nástrojov, kryptoaktív, komodít alebo akýchkoľvek iných aktív, a to aj vo forme marže, kolaterálu alebo záväzku, a to tak za hotovosť, ako aj za akékoľvek iné aktívum. Na účely klasifikácie by sa mali brať do úvahy všetky transakcie, ktoré zahŕňajú aktíva, ktorých hodnota môže byť vyjadrená v peňažnej sume.

([1]) Ú. v. EÚ L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.
([2]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Klasifikačné kritériá by mali zabezpečiť, aby boli zachytené všetky relevantné druhy závažných incidentov. Kybernetické útoky súvisiace s vniknutím do siete alebo informačných systémov nemusia byť nevyhnutne zachytené mnohými klasifikačnými kritériami. Tieto sú však dôležité, pretože každé vniknutie do siete a informačných systémov môže poškodiť finančný subjekt. Klasifikačné kritériá „kritickosť zasiahnutých služieb“ a „straty údajov“ by sa preto mali špecifikovať tak, aby zachytávali tieto druhy závažných incidentov, najmä neoprávnené vniknutia, ktoré – hoci ich vplyvy nie sú okamžite známe – môžu mať závažné dôsledky, najmä pokiaľ ide o porušenie ochrany údajov a úniky údajov.

(6) Keďže úverové inštitúcie podliehajú rámcu klasifikácie incidentov podľa článku 18 nariadenia (EÚ) 2022/2554, ako aj rámcu operačného rizika podľa delegovaného nariadenia Komisie (EÚ) 2018/959 ([3]), prístup k posudzovaniu hospodárskeho vplyvu incidentu založený na výpočte nákladov a strát by mal byť v čo najväčšej možnej miere konzistentný podľa oboch rámcov, aby sa zabránilo zavádzaniu nezlučiteľných alebo konfliktných požiadaviek.

(7) Kritérium týkajúce sa geografického rozloženia incidentu stanovené v článku 18 ods. 1 písm. c) nariadenia (EÚ) 2022/2554 by sa malo zameriavať na cezhraničný vplyv incidentu, keďže vplyv incidentu na činnosti finančného subjektu v rámci jednej jurisdikcie bude zachytený inými kritériami stanovenými v uvedenom článku.

(8) Keďže klasifikačné kritériá sú navzájom závislé a prepojené, prístup k identifikácii závažných incidentov, ktoré sa majú oznamovať v súlade s článkom 19 ods. 1 nariadenia (EÚ) 2022/2554, by mal byť založený na kombinácii kritérií, pričom niektoré kritériá, ktoré úzko súvisia s vymedzením pojmov „incident súvisiaci s IKT“ a „závažný incident súvisiaci s IKT“, ako sa stanovuje v článku 3 bodoch 8 a 10 nariadenia (EÚ) 2022/2554, by mali mať pri klasifikácii závažných incidentov väčšiu váhu ako iné kritériá.

(9) S cieľom zabezpečiť, aby správy o závažných incidentoch a oznámenia o závažných incidentoch prijaté príslušnými orgánmi podľa článku 19 ods. 1 nariadenia (EÚ) 2022/2554 slúžili na účely dohľadu aj na predchádzanie nákazlivému účinku v celom finančnom sektore, by prahové hodnoty významnosti mali umožňovať zachytenie závažných incidentov, a to okrem iného zameraním sa na vplyv na kritické služby špecifické pre daný finančný subjekt, konkrétne absolútne a relatívne prahové hodnoty klientov alebo finančných protistrán, na transakcie, ktoré naznačujú významný vplyv na finančný subjekt, ako aj na význam vplyvu v iných členských štátoch.

(10) Za incidenty ovplyvňujúce kritické služby finančných subjektov by sa mali považovať incidenty, ktoré ovplyvňujú IKT služby alebo sieť a informačné systémy, ktoré podporujú kritické alebo dôležité funkcie, alebo finančné služby, ktoré si vyžadujú povolenie, alebo škodlivý neoprávnený prístup do sietí a informačných systémov, ktoré podporujú kritické alebo dôležité funkcie. Za závažný incident, ktorý sa má vždy oznamovať, by sa mal považovať škodlivý neoprávnený prístup do siete a informačných systémov, ktoré podporujú kritické alebo dôležité funkcie finančných subjektov, pretože takýto prístup predstavuje závažné riziko pre daný finančný subjekt, keďže môže ovplyvniť iné finančné subjekty.

(11) Opakujúce sa incidenty, ktoré sú prepojené podobnou zjavnou hlavnou príčinou a ktoré jednotlivo nie sú závažnými incidentmi, môžu poukazovať na závažné nedostatky a slabé miesta v postupoch finančného subjektu v oblasti riadenia incidentov a rizík. Opakujúce sa incidenty by sa preto mali považovať za kolektívne závažné, ak k nich dochádza opakovane počas určitého obdobia.

(12) Keďže kybernetické hrozby môžu mať negatívny vplyv na finančný subjekt a sektor, významné kybernetické hrozby, ktorým môžu byť finančné subjekty vystavené, by mali poukazovať na pravdepodobnosť významnosti a kritickosť potenciálneho vplyvu. S cieľom zabezpečiť jasné a konzistentné posudzovanie významnosti kybernetických hrozieb by preto klasifikácia kybernetickej hrozby ako významnej mala závisieť od pravdepodobnosti, že klasifikačné kritériá závažných incidentov a ich prahová hodnota by boli splnené pri naplnení hrozby, od druhu kybernetickej hrozby a od informácií, ktoré má finančný subjekt k dispozícii.

([3]) Delegované nariadenie Komisie (EÚ) 2018/959 zo 14. marca 2018, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013, pokiaľ ide o regulačné technické predpisy týkajúce sa špecifikácie metodiky posudzovania, na základe ktorej príslušné orgány povoľujú inštitúciám používať na operačné riziko pokročilé prístupy merania (Ú. v. EÚ L 169, 6.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Keďže príslušným orgánom v iných členských štátoch sa majú oznamovať incidenty, ktoré majú vplyv na finančné subjekty a zákazníkov v ich jurisdikcii, posudzovanie vplyvu v inej jurisdikcii v súlade s článkom 19 ods. 7 nariadenia (EÚ) 2022/2554 by malo vychádzať z hlavnej príčiny incidentu, potenciálneho nákazlivého účinku na externých poskytovateľov a z infraštruktúr finančného trhu, ako aj z vplyvu incidentu na významné skupiny klientov alebo finančných protistrán.

(14) Postupy nahlasovania a oznamovania uvedené v článku 19 ods. 6 a 7 nariadenia (EÚ) 2022/2554 by mali príslušným príjemcom umožniť posúdiť vplyv incidentov. Zasielané informácie by preto mali zahŕňať všetky podrobnosti uvedené v správach o incidentoch, ktoré finančný subjekt predložil príslušnému orgánu.

(15) Ak incident predstavuje porušenie ochrany osobných údajov podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 ([4]) a smernice Európskeho parlamentu a Rady 2002/58/ES ([5]), toto nariadenie by nemalo mať vplyv na povinnosti týkajúce sa zaznamenávania a oznamovania v prípade porušenia ochrany osobných údajov, ako sa stanovuje v uvedených právnych predpisoch Únie. Príslušné orgány by mali spolupracovať a vymieňať si informácie o všetkých relevantných záležitostiach s orgánmi uvedenými v nariadení (EÚ) 2016/679 a smernici 2002/58/ES.

(16) Toto nariadenie vychádza z návrhu regulačných technických predpisov, ktorý Komisii predložili európske orgány dohľadu po konzultácii s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) a Európskou centrálnou bankou (ECB).

(17) Spoločný výbor európskych orgánov uvedený v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([6]), v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010 ([7]) a v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1095/2010 ([8]) uskutočnil otvorené verejné konzultácie k návrhu regulačných technických predpisov, z ktorých toto nariadenie vychádza, analyzoval potenciálne náklady a prínosy navrhovaných predpisov a požiadal o poradenstvo Skupinu zainteresovaných strán v bankovníctve zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010, Skupinu zainteresovaných strán v poisťovníctve a zaisťovníctve a skupinu zainteresovaných strán v dôchodkovom poistení zamestnancov zriadené v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010 a Skupinu zainteresovaných strán v oblasti cenných papierov a trhov zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1095/2010.

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Smernica Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov), a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1095/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/77/ES (Ú. v. EÚ L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([9]) prebehli konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal svoje stanovisko 24. januára 2024,

PRIJALA TOTO NARIADENIE:

KAPITOLA I

KLASIFIKAČNÉ KRITÉRIÁ

Článok 1

Klienti, finančné protistrany a transakcie ovplyvnené incidentom

1. Počet klientov ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, odráža počet všetkých ovplyvnených klientov, či už fyzických alebo právnických osôb, ktorí počas incidentu nemôžu alebo nemohli využívať službu poskytovanú finančným subjektom, alebo ktorých incident nepriaznivo ovplyvnil. Tento počet zahŕňa aj tretie strany, na ktoré sa výslovne vzťahuje zmluvná dohoda medzi finančným subjektom a klientom, ako príjemcov ovplyvnenej služby.

2. Počet finančných protistrán ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, odráža počet všetkých ovplyvnených finančných protistrán, ktoré s finančným subjektom uzavreli zmluvnú dohodu.

3. Pokiaľ ide o relevantnosť klientov a finančných protistrán ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, finančný subjekt zohľadňuje rozsah, v akom vplyv na klienta alebo finančnú protistranu ovplyvní plnenie obchodných cieľov finančného subjektu, ako aj potenciálny vplyv incidentu na efektívnosť trhu.

4. Pokiaľ ide o výšku alebo počet transakcií ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, finančný subjekt zohľadňuje všetky ovplyvnené transakcie zahŕňajúce peňažnú sumu, ak sa aspoň jedna časť transakcie vykonáva v Únii.

5. Ak nemožno určiť skutočný počet ovplyvnených klientov alebo finančných protistrán alebo skutočný počet alebo sumu ovplyvnených transakcií, finančný subjekt odhadne uvedené počty alebo sumy na základe dostupných údajov z porovnateľných referenčných období.

Článok 2

Vplyv na dobré meno

1. Na účely určenia vplyvu incidentu na dobré meno, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, došlo podľa finančných subjektov k vplyvu na dobré meno, ak je splnené aspoň jedno z týchto kritérií:

a) incident bol predmetom mediálneho spravodajstva;

b) incident viedol k opakovaným sťažnostiam rôznych klientov alebo finančných protistrán, ktoré sa týkali služieb vyžadujúcich si priamy kontakt so zákazníkom alebo kritických obchodných vzťahov;

c) finančný subjekt si v dôsledku incidentu nebude môcť alebo pravdepodobne nebude môcť splniť regulačné požiadavky;

d) finančný subjekt v dôsledku incidentu stratí alebo pravdepodobne stratí klientov alebo finančné protistrany, čo môže mať významný vplyv na jeho obchodnú činnosť.

([9]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Finančné subjekty zohľadňujú pri posudzovaní vplyvu incidentu na svoje dobré meno mieru publicity, ktorú incident nadobudne alebo pravdepodobne nadobudne v súvislosti s každým kritériom uvedeným v odseku 1.

Článok 3

Trvanie incidentu súvisiaceho s IKT a výpadok služby

1. Finančné subjekty merajú trvanie incidentu súvisiaceho s IKT, ako sa uvádza v článku 18 ods. 1 písm. b) nariadenia (EÚ) 2022/2554, od momentu, keď incident nastane, až do momentu jeho vyriešenia.

Ak finančné subjekty nedokážu určiť moment, keď k incidentu došlo, merajú trvanie incidentu od momentu, keď sa zistil. Ak sa finančné subjekty dozvedia, že incident sa vyskytol pred jeho odhalením, merajú jeho trvanie od momentu zaznamenania incidentu v záznamových protokoloch siete alebo systému alebo v iných zdrojoch údajov.

Ak finančné subjekty ešte nevedia, kedy sa incident vyrieši, alebo nedokážu overiť záznamy v záznamových protokoloch alebo iných zdrojoch údajov, uplatňujú odhady.

2. Finančné subjekty merajú výpadok služby v dôsledku incidentu, ako sa uvádza v článku 18 ods. 1 písm. b) nariadenia (EÚ) 2022/2554, od momentu, keď je služba pre klientov, finančné protistrany alebo iných interných či externých používateľov úplne alebo čiastočne nedostupná, až do momentu, keď sa bežné činnosti alebo operácie obnovili na úroveň služby, ktorá bola poskytovaná pred incidentom. Ak výpadok služby spôsobí omeškanie pri poskytovaní služby po obnovení bežných činností alebo operácií, výpadok sa meria od začiatku incidentu do momentu, keď sa uvedená meškajúca služba plne poskytuje.

Ak finančné subjekty nedokážu určiť moment, keď sa začal výpadok služby, merajú trvanie výpadku služby od momentu, keď sa výpadok zistil.

Článok 4

Geografické rozloženie

Na účely určenia geografického rozloženia, pokiaľ ide o oblasti postihnuté incidentom, ako sa uvádza v článku 18 ods. 1 písm. c) nariadenia (EÚ) 2022/2554, finančné subjekty posúdia, či incident má alebo mal vplyv v iných členských štátoch, a najmä význam vplyvu vo vzťahu ku ktorémukoľvek z týchto subjektov:

a) klienti a finančné protistrany v iných členských štátoch;

b) pobočky alebo iné finančné subjekty v rámci skupiny vykonávajúce činnosti v iných členských štátoch;

c) infraštruktúry finančného trhu alebo externí poskytovatelia, ktoré/ktorí môžu mať vplyv na finančné subjekty v iných členských štátoch, ktorým poskytujú služby, a to v rozsahu, v akom sú takéto informácie k dispozícii.

Článok 5

Straty údajov

Na účely určenia strát údajov, ktoré incident so sebou prináša, ako sa uvádza v článku 18 ods. 1 písm. d) nariadenia (EÚ) 2022/2554, finančné subjekty zohľadňujú tieto aspekty:

a) v súvislosti s dostupnosťou údajov, či sa v dôsledku incidentu stali údaje poskytované na požiadanie finančného subjektu, jeho klientov alebo jeho protistrán dočasne alebo trvalo nedostupné alebo nepoužiteľné;

b) v súvislosti s pravosťou údajov, či incident ohrozil dôveryhodnosť zdroja údajov;

c) v súvislosti s integritou údajov, či incident viedol k nepovolenej zmene údajov, v dôsledku ktorej sa údaje stali znehodnotenými alebo neúplnými;

d) v súvislosti s dôvernosťou údajov, či incident viedol k prístupu k údajom alebo k ich sprístupneniu neoprávnenej strane alebo systému.

Článok 6

Kritickosť zasiahnutých služieb

Na účely určenia kritickosti zasiahnutých služieb, ako sa uvádza v článku 18 ods. 1 písm. e) nariadenia (EÚ) 2022/2554, finančné subjekty zohľadňujú, či incident:

a) ovplyvňuje alebo ovplyvnil IKT služby alebo sieť a informačné systémy, ktoré podporujú kritické alebo dôležité funkcie finančného subjektu;

b) ovplyvňuje alebo ovplyvnil finančné služby, ktoré poskytuje finančný subjekt a ktoré si vyžadujú povolenie, registráciu alebo ktoré podliehajú dohľadu príslušných orgánov;

c) predstavuje alebo predstavoval úspešný, škodlivý a neoprávnený prístup do siete a informačných systémov finančného subjektu.

Článok 7

Hospodársky vplyv

1. Na účely určenia hospodárskeho vplyvu incidentu, ako sa uvádza v článku 18 ods. 1 písm. f) nariadenia (EÚ) 2022/2554, finančné subjekty zohľadňujú, bez zohľadnenia spätne získaných finančných prostriedkov, tieto druhy priamych a nepriamych nákladov a strát, ktoré im vznikli v dôsledku incidentu:

a) vyvlastnené finančné prostriedky alebo finančné aktíva, za ktoré zodpovedajú, vrátane aktív stratených v dôsledku krádeže;

b) náklady na výmenu alebo premiestnenie softvéru, hardvéru alebo infraštruktúry;

c) náklady na zamestnancov vrátane nákladov spojených s nahradením alebo premiestnením zamestnancov, prijímaním ďalších zamestnancov, odmeňovaním nadčasov a obnovením stratených alebo zhoršených zručností;

d) poplatky z dôvodu nedodržania zmluvných záväzkov;

e) náklady na nápravu a odškodnenie zákazníkov;

f) straty v dôsledku ušlých príjmov;

g) náklady spojené s vnútornou a vonkajšou komunikáciou;

h) náklady na poradenstvo vrátane nákladov spojených s právnym poradenstvom, forenznými službami a sanačnými službami.

2. Náklady a straty uvedené v odseku 1 nezahŕňajú náklady, ktoré sú potrebné na každodennú prevádzku podniku, najmä:

a) náklady na všeobecnú údržbu infraštruktúry, vybavenia, hardvéru a softvéru, ani náklady na aktualizáciu zručností zamestnancov;

b) interné alebo externé náklady, ktorých cieľom je zlepšiť podnikanie po incidente vrátane modernizácie, zlepšení, iniciatív na posúdenie rizika;

c) poistné.

3. Finančné subjekty vypočítavajú výšku nákladov a strát na základe údajov dostupných v čase nahlasovania. Ak skutočnú výšku nákladov a strát nemožno určiť, finančné subjekty tieto sumy odhadnú.

4. Pri posudzovaní hospodárskeho vplyvu incidentu finančné subjekty spočítajú náklady a straty uvedené v odseku 1.

KAPITOLA II

ZÁVAŽNÉ INCIDENTY A PRAHOVÉ HODNOTY VÝZNAMNOSTI

Článok 8

Závažné incidenty

1. Incident sa na účely článku 19 ods. 1 nariadenia (EÚ) 2022/2554 za závažný považuje vtedy, ak ovplyvnil kritické služby uvedené v článku 6 a ak je splnená niektorá z týchto podmienok:

a) je splnená prahová hodnota významnosti uvedená v článku 9 ods. 5 písm. b);

b) sú splnené dve alebo viaceré ďalšie prahové hodnoty významnosti uvedené v článku 9 ods. 1 až 6.

2. Opakujúce sa incidenty, ktoré sa jednotlivo nepovažujú za závažný incident v súlade s odsekom 1, sa považujú za jeden závažný incident, ak spĺňajú všetky tieto podmienky:

a) vyskytli sa aspoň dvakrát za šesť mesiacov;

b) majú rovnakú zjavnú hlavnú príčinu, ako sa uvádza v článku 20 prvého pododseku písm. b) nariadenia (EÚ) 2022/2554;

c) kolektívne spĺňajú kritériá na to, aby sa považovali za závažný incident podľa odseku 1.

Existenciu opakujúcich sa incidentov finančné subjekty posudzujú každý mesiac.

Tento odsek sa nevzťahuje na mikropodniky a finančné subjekty uvedené v článku 16 ods. 1 nariadenia (EÚ) 2022/2554.

Článok 9

Prahové hodnoty významnosti na určenie závažných incidentov

1. Prahová hodnota významnosti pre kritérium „klienti, finančné protistrany a transakcie ovplyvnené incidentom“ je splnená, ak je splnená ktorákoľvek z týchto podmienok:

a) počet ovplyvnených klientov je vyšší ako 10 % všetkých klientov využívajúcich ovplyvnenú službu;

b) počet ovplyvnených klientov využívajúcich ovplyvnenú službu je vyšší ako 100 000;

c) počet ovplyvnených finančných protistrán je vyšší ako 30 % všetkých finančných protistrán vykonávajúcich činnosti súvisiace s poskytovaním ovplyvnenej služby;

d) počet ovplyvnených transakcií je vyšší ako 10 % denného priemerného počtu transakcií vykonávaných finančným subjektom v súvislosti s ovplyvnenou službou;

e) suma ovplyvnených transakcií je vyššia ako 10 % dennej priemernej hodnoty transakcií vykonávaných finančným subjektom v súvislosti s ovplyvnenou službou;

f) ovplyvnení boli klienti alebo finančné protistrany, ktorí/ktoré boli v súlade s článkom 1 ods. 3 identifikované ako dôležití/dôležité.

Ak nemožno určiť skutočný počet ovplyvnených klientov alebo finančných protistrán alebo skutočný počet alebo sumu ovplyvnených transakcií, finančný subjekt odhadne uvedené počty alebo sumy na základe dostupných údajov z porovnateľných referenčných období.

2. Prahová hodnota významnosti pre kritérium „vplyv na dobré meno“ je splnená, ak je splnená ktorákoľvek z podmienok stanovených v článku 2 písm. a) až d).

3. Prahová hodnota významnosti pre kritérium „trvanie incidentu súvisiaceho s IKT a výpadok služby“ je splnená, ak je splnená ktorákoľvek z týchto podmienok:

a) incident trvá dlhšie ako 24 hodín;

b) v prípade služieb IKT, ktoré podporujú kritické alebo dôležité funkcie, je výpadok služby dlhší ako 2 hodiny.

4. Prahová hodnota významnosti pre kritérium „geografické rozloženie“ je splnená, ak má incident vplyv v dvoch alebo viacerých členských štátoch v súlade s článkom 4.

5. Prahová hodnota významnosti pre kritérium „straty údajov“ je splnená, ak je splnená ktorákoľvek z týchto podmienok:

a) každý vplyv uvedený v článku 5 na dostupnosť, pravosť, integritu alebo dôvernosť údajov má alebo bude mať nepriaznivý vplyv na plnenie obchodných cieľov finančného subjektu alebo na jeho schopnosť spĺňať regulačné požiadavky;

b) sieť a informačné systémy sú zasiahnuté úspešným, škodlivým a neoprávneným prístupom, na ktorý sa nevzťahuje písmeno a), ak takýto prístup môže viesť k stratám údajov.

6. Prahová hodnota významnosti pre kritérium „hospodársky vplyv“ je splnená, ak náklady a straty, ktoré vznikli finančnému subjektu v dôsledku incidentu, prekročili alebo pravdepodobne prekročia 100 000 EUR.

KAPITOLA III

VÝZNAMNÉ KYBERNETICKÉ HROZBY

Článok 10

Vysoké prahové hodnoty významnosti na určenie významných kybernetických hrozieb

Na účely článku 18 ods. 2 nariadenia (EÚ) 2022/2554 sa kybernetická hrozba považuje za významnú, ak sú splnené všetky tieto podmienky:

a) kybernetická hrozba, ak by k nej došlo, mohla ovplyvniť alebo by mohla ovplyvniť kritické alebo dôležité funkcie finančného subjektu alebo iné finančné subjekty, externých poskytovateľov, klientov alebo finančné protistrany, a to na základe informácií, ktoré má finančný subjekt k dispozícii;

b) existuje vysoká pravdepodobnosť naplnenia kybernetickej hrozby vo finančnom subjekte alebo v iných finančných subjektoch, pričom sa zohľadňujú aspoň tieto prvky:

   i) uplatniteľné riziká súvisiace s kybernetickou hrozbou uvedenou v písmene a) vrátane potenciálnych zraniteľných miest systémov finančného subjektu, ktoré možno zneužiť;

   ii) spôsobilosti a úmysel aktérov hrozby v rozsahu, ktorý je finančnému subjektu známy;

   iii) pretrvávanie hrozby a všetky získané poznatky o incidentoch, ktoré ovplyvnili finančný subjekt alebo jeho externého poskytovateľa, klientov alebo finančné protistrany;

c) ak by došlo ku kybernetickej hrozbe, mohla by spĺňať ktorúkoľvek z týchto podmienok:

   i) kritérium týkajúce sa kritickosti zasiahnutých služieb stanovené v článku 18 ods. 1 písm. e) nariadenia (EÚ) 2022/2554, ako sa bližšie určuje v článku 6 tohto nariadenia;

   ii) prahovú hodnotu významnosti stanovenú v článku 9 ods. 1;

   iii) prahovú hodnotu významnosti stanovenú v článku 9 ods. 4.

Ak, v závislosti od druhu kybernetickej hrozby a dostupných informácií, finančný subjekt dospeje k záveru, že by sa mohli dosiahnuť prahové hodnoty významnosti stanovené v článku 9 ods. 2, 3, 5 a 6, môžu sa zohľadniť aj tieto prahové hodnoty.

KAPITOLA IV

RELEVANTNOSŤ ZÁVAŽNÝCH INCIDENTOV PRE PRÍSLUŠNÉ ORGÁNY V INÝCH ČLENSKÝCH ŠTÁTOCH A PODROBNOSTI SPRÁV, KTORÉ SA MAJÚ POSKYTNÚŤ INÝM PRÍSLUŠNÝM ORGÁNOM

Článok 11

Relevantnosť závažných incidentov pre príslušné orgány v iných členských štátoch

Posúdenie toho, či je závažný incident relevantný pre príslušné orgány v iných členských štátoch, ako sa uvádza v článku 19 ods. 7 nariadenia (EÚ) 2022/2554, vychádza z toho, či má incident hlavnú príčinu pochádzajúcu z iného členského štátu alebo či incident má alebo mal významný vplyv v inom členskom štáte v súvislosti s ktorýmkoľvek z týchto aspektov:

a) klienti alebo finančné protistrany;

b) pobočka finančného subjektu alebo iný finančný subjekt v rámci skupiny;

c) infraštruktúra finančného trhu alebo externý poskytovateľ, ktoré/ktorí môže mať vplyv na finančné subjekty, ktorým poskytujú služby.

Článok 12

Podrobnosti o závažných incidentoch, ktoré sa majú poskytnúť iným príslušným orgánom

Podrobnosti o závažných incidentoch, ktoré majú príslušné orgány predložiť iným príslušným orgánom v súlade s článkom 19 ods. 6 nariadenia (EÚ) 2022/2554, a oznámenia, ktoré majú predložiť orgány EBA, ESMA alebo EIOPA, ako aj ECB dotknutým príslušným orgánom v iných členských štátoch v súlade s článkom 19 ods. 7 uvedeného nariadenia, musia bez akejkoľvek anonymizácie obsahovať rovnakú úroveň informácií ako oznámenia a správy o závažných incidentoch získané od finančných subjektov v súlade s článkom 19 ods. 4 nariadenia (EÚ) 2022/2554.

KAPITOLA V

ZÁVEREČNÉ USTANOVENIA

Článok 13

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 13. marca 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN