



2024/1772

25.6.2024.

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1772

od 13. ožujka 2024.

o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju kriteriji za klasifikaciju IKT incidenata i kiberprijetnji, pragovi značajnosti i pojedinosti izvješća o značajnim incidentima

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 ⁽¹⁾, a posebno njezin članak 18. stavak 4. treći podstavak,

budući da:

- (1) Cilj je Uredbe (EU) 2022/2554 uskladiti i pojednostavniti zahtjeve za izvješćivanje o IKT incidentima i operativnim ili sigurnosnim incidentima povezanim s plaćanjem koji se odnose na kreditne institucije, institucije za platni promet, pružatelje usluga pružanja informacija o računu i institucije za elektronički novac („incidenti”). S obzirom na to da zahtjevi za izvješćivanje obuhvaćaju 20 različitih vrsta financijskih subjekata, klasifikacijske kriterije i pragove značajnosti za značajne incidente i ozbiljne kiberprijetnje trebalo bi utvrditi na jednostavan, usklađen i dosljedan način kojim se uzimaju u obzir posebnosti usluga i aktivnosti svih relevantnih financijskih subjekata.
- (2) Kako bi se osigurala proporcionalnost, klasifikacijski kriteriji i pragovi značajnosti trebali bi odražavati veličinu i ukupni profil rizičnosti te prirodu, opseg i složenost usluga svih financijskih subjekata. Nadalje, kriteriji i pragovi značajnosti trebali bi biti osmišljeni tako da se dosljedno primjenjuju na sve financijske subjekte, bez obzira na njihovu veličinu i profil rizičnosti, te da se manje financijske subjekte ne opterećuje nerazmjerno u pogledu izvješćivanja. Međutim, kako bi se riješile situacije u kojima incident utječe na znatan broj klijenata, a ne prelazi primjenjivi prag, trebalo bi utvrditi apsolutni prag koji je uglavnom usmjeren na veće financijske subjekte.
- (3) Kad je riječ o okvirima za izvješćivanje o incidentima koji su se dogodili prije stupanja na snagu Uredbe (EU) 2022/2554, trebalo bi osigurati kontinuitet za financijske subjekte. Stoga bi klasifikacijski kriteriji i pragovi značajnosti trebali biti usklađeni sa Smjernicama EBA-e o izvješćivanju o značajnim incidentima u skladu s Direktivom (EU) 2015/2366 Europskog parlamenta i Vijeća ⁽²⁾, Smjernicama o periodičnim informacijama i obavješćivanju o značajnim promjenama koje trgovinski repozitoriji trebaju dostaviti ESMA-i, Okvirom ESB-a/SSM-a za izvješćivanje o kiberincidentima i drugim relevantnim smjernicama. Klasifikacijski kriteriji i pragovi trebali bi biti prikladni i za financijske subjekte koji nisu podliježali zahtjevima za izvješćivanje o incidentima prije Uredbe (EU) 2022/2554.
- (4) Kad je riječ o kriteriju klasifikacije „količina i broj zahvaćenih transakcija”, pojam transakcija širok je i obuhvaća različite aktivnosti i usluge u svim sektorskim aktima koji se primjenjuju na financijske subjekte. Za potrebe tog klasifikacijskog kriterija trebalo bi obuhvatiti platne transakcije i sve oblike razmjene financijskih instrumenata, kriptoomovine, robe ili bilo koje druge imovine, uključujući u obliku marže, kolaterala ili zaloga, na temelju gotovine i bilo koje druge imovine. Za potrebe klasifikacije trebalo bi uzeti u obzir sve transakcije koje uključuju imovinu čija se vrijednost može izraziti u novčanom iznosu.

⁽¹⁾ SL L 333, 27.12.2022., str. 1., ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

⁽²⁾ Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23.12.2015., str. 35., ELI: <http://data.europa.eu/eli/dir/2015/2366/oj>).

- (5) Klasifikacijskim kriterijima trebalo bi obuhvatiti sve relevantne vrste značajnih incidenata. Kibernetički napadi povezani s prodiranjem u mrežne ili informacijske sustave ne moraju nužno biti obuhvaćeni mnogim klasifikacijskim kriterijima. No važni su jer svako prodiranje u mrežne i informacijske sustave može naštetiti financijskom subjektu. U skladu s tim, klasifikacijske kriterije „zahvaćene ključne usluge” i „gubitak podataka” trebalo bi definirati tako da obuhvaćaju te vrste značajnih incidenata, posebno neovlaštene upade koji, čak i ako učinci nisu odmah poznati, mogu dovesti do ozbiljnih posljedica, posebno povrede podataka i curenja podataka.
- (6) Budući da se na kreditne institucije primjenjuje i okvir za klasifikaciju incidenata iz članka 18. Uredbe (EU) 2022/2554 i okvir za operativni rizik iz Delegirane uredbe Komisije (EU) 2018/959⁽³⁾, pristup procjeni ekonomskog učinka incidenta na temelju izračuna troškova i gubitaka trebao bi biti što dosljedniji s oba okvira kako bi se izbjeglo uvođenje neusklađenih ili proturječnih zahtjeva.
- (7) Kriterij koji se odnosi na zemljopisnu raširenost incidenta iz članka 18. stavka 1. točke (c) Uredbe (EU) 2022/2554 trebao bi biti usmjeren na prekogranični učinak incidenta jer će učinak incidenta na aktivnosti financijskog subjekta unutar jedne jurisdikcije biti obuhvaćen drugim kriterijima utvrđenima u tom članku.
- (8) S obzirom na to da su klasifikacijski kriteriji međusobno povezani, pristup za utvrđivanje značajnih incidenata o kojima treba izvješćivati u skladu s člankom 19. stavkom 1. Uredbe (EU) 2022/2554 trebao bi se temeljiti na kombinaciji kriterija, od kojih bi neki kriteriji usko povezani s definicijama IKT incidenta i značajnog IKT incidenta iz članka 3. stavaka 8. i 10. Uredbe (EU) 2022/2554 trebali u klasifikaciji značajnih incidenata biti važniji od drugih kriterija.
- (9) Kako bi izvješća o značajnim incidentima i obavijesti o njima koja prime nadležna tijela na temelju članka 19. stavka 1. Uredbe (EU) 2022/2554 služila i u nadzorne svrhe i za sprečavanje širenja zaraze u cijelom financijskom sektoru, pragovi značajnosti trebali bi omogućiti obuhvaćanje značajnih incidenata fokusiranjem, među ostalim, na učinak na ključne usluge specifične za subjekt, posebne apsolutne i relativne pragove kljenata ili partnerskih financijskih subjekata, transakcije koje upućuju na značajan učinak na financijski subjekt i značajnost učinka u drugim državama članicama.
- (10) Incidente koji utječu na IKT usluge ili mrežne i informacijske sustave kojima se podupiru ključne ili važne funkcije, ili financijske usluge za koje je potrebno odobrenje ili zlonamjerni neovlašten pristup mrežnim i informacijskim sustavima koji podupiru ključne ili važne funkcije trebalo bi smatrati incidentima koji utječu na ključne usluge financijskih subjekata. Zlonamjerni, neovlašteni pristup mrežnim i informacijskim sustavima kojima se podupiru ključne ili važne funkcije financijskih subjekata predstavlja ozbiljan rizik za financijski subjekt i, s obzirom na to da može utjecati na druge financijske subjekte, uvijek bi se trebali smatrati značajnim incidentima koje je potrebno prijaviti.
- (11) Incidenti koji se ponavljaju povezani sličnim očitim temeljnim uzrokom, koji pojedinačno nisu značajni incidenti, mogu ukazivati na znatne nedostatke i slabosti u postupcima upravljanja incidentima i rizicima financijskog subjekta. Stoga bi se incidenti koji se ponavljaju trebali smatrati kolektivno značajnima ako se ponavljaju tijekom određenog razdoblja.
- (12) S obzirom na to da kiberprijetnje mogu negativno utjecati na financijski subjekt i sektor, ozbiljne kiberprijetnje koje financijski subjekti mogu prijaviti trebale bi upućivati na vjerojatnost realizacije i ključnost potencijalnog učinka. U skladu s tim, kako bi se osigurala jasna i dosljedna procjena ozbiljnosti kiberprijetnji, klasifikacija kiberprijetnje kao ozbiljne trebala bi ovisiti o tome bi li klasifikacijski kriteriji za značajne incidente i njihov prag bili ispunjeni da se prijetnja realizirala, o vrsti kiberprijetnji i informacijama koje su dostupne financijskom subjektu.

⁽³⁾ Delegirana uredba Komisije (EU) 2018/959 od 14. ožujka 2018. o dopuni Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda za specifikaciju metodologije procjene prema kojoj nadležna tijela odobravaju institucijama primjenu naprednih pristupa za operativni rizik (SL L 169, 6.7.2018., str. 1., ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

- (13) S obzirom na to da nadležna tijela u drugim državama članicama treba obavijestiti o incidentima koji utječu na financijske subjekte i klijente u njihovoj jurisdikciji, procjena učinka u drugoj jurisdikciji u skladu s člankom 19. stavkom 7. Uredbe (EU) 2022/2554 trebala bi se temeljiti na temeljnom uzroku incidenta, potencijalnom širenju putem trećih strana koje su pružatelji usluga i na infrastrukturama financijskog tržišta te na učinku incidenta na značajne skupine klijenata ili partnerskih financijskih subjekata.
- (14) Postupci izvješćivanja i obavješćivanja iz članka 19. stavaka 6. i 7. Uredbe (EU) 2022/2554 trebali bi omogućiti odgovarajućim primateljima da procijene učinak incidenata. Stoga bi dostavljene informacije trebale uključivati sve pojedinosti sadržane u izvješćima o incidentima koje financijski subjekt podnosi nadležnom tijelu.
- (15) Ako incident predstavlja povredu osobnih podataka u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća ⁽⁴⁾ i Direktivom 2002/58/EZ Europskog parlamenta i Vijeća ⁽⁵⁾, ova Uredba ne bi trebala utjecati na obveze evidentiranja i obavješćivanja o povredama osobnih podataka utvrđene u tim propisima Unije. Nadležna tijela trebala bi surađivati i razmjenjivati informacije o svim relevantnim pitanjima s tijelima iz Uredbe (EU) 2016/679 i Direktive 2002/58/EZ.
- (16) Ova se Uredba temelji na nacrtu regulatornih tehničkih standarda koji su Komisiji dostavila europska nadzorna tijela uz savjetovanje s Agencijom Europske unije za kibersigurnost (ENISA) i Europskom središnjom bankom (ESB).
- (17) Zajednički odbor europskih nadzornih tijela iz članka 54. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća ⁽⁶⁾, članka 54. Uredbe (EU) br. 1094/2010 Europskog parlamenta i Vijeća ⁽⁷⁾ i članka 54. Uredbe (EU) br. 1095/2010 Europskog parlamenta i Vijeća ⁽⁸⁾ proveo je otvoreno javno savjetovanje o nacrtu regulatornih tehničkih standarda na kojem se temelji ova Uredba, analizirao je moguće troškove i koristi predloženih standarda te zatražio savjet Interesne skupine za bankarstvo osnovane u skladu s člankom 37. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća, Interesne skupine za osiguranje i reosiguranje i Interesne skupine za strukovno mirovinsko osiguranje osnovanih u skladu s člankom 37. Uredbe (EU) br. 1094/2010 Europskog parlamenta i Vijeća i Interesne skupine za vrijednosne papire i tržišta kapitala osnovane u skladu s člankom 37. Uredbe (EU) br. 1095/2010,

⁽⁴⁾ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1., ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

⁽⁵⁾ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37., ELI: <http://data.europa.eu/eli/dir/2002/58/oj>).

⁽⁶⁾ Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12., ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

⁽⁷⁾ Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju Europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48., ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

⁽⁸⁾ Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), izmjeni Odluke br. 716/2009/EZ i stavljanju izvan snage Odluke Komisije 2009/77/EZ (SL L 331, 15.12.2010., str. 84., ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

- (18) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ⁽⁹⁾ te je on dao mišljenje 24. siječnja 2024.,

DONIJELA JE OVU UREDBU:

POGLAVLJE I.

KLASIFIKACIJSKI KRITERIJI

Članak 1.

Klijenti, partnerski financijski subjekti i transakcije

1. Broj klijenata zahvaćenih incidentom iz članka 18. stavka 1. točke (a) Uredbe (EU) 2022/2554 odražava broj svih zahvaćenih klijenata, bez obzira na to jesu li oni fizičke ili pravne osobe, koji ne mogu ili nisu mogli iskoristiti uslugu koju je financijski subjekt pružio tijekom incidenta ili na koje je incident negativno utjecao. Taj broj uključuje i treće strane koje su izričito obuhvaćene ugovorom između financijskog subjekta i klijenta kao korisnici zahvaćene usluge.
2. Broj partnerskih financijskih subjekata zahvaćenih incidentom iz članka 18. stavka 1. točke (a) Uredbe (EU) 2022/2554 odražava broj svih zahvaćenih partnerskih financijskih subjekata koji su sklopili ugovorni aranžman s financijskim subjektom.
3. Kad je riječ o važnosti klijenata i partnerskih financijskih subjekata zahvaćenih incidentom iz članka 18. stavka 1. točke (a) Uredbe (EU) 2022/2554, financijski subjekt uzima u obzir u kojoj će mjeri učinak na klijenta ili partnerske financijske subjekte utjecati na provedbu poslovnih ciljeva financijskog subjekta, kao i mogući učinak incidenta na učinkovitost tržišta.
4. U odnosu na količinu ili broj transakcija zahvaćenih incidentom iz članka 18. stavka 1. točke (a) Uredbe (EU) 2022/2554, financijski subjekt uzima u obzir sve zahvaćene transakcije koje uključuju novčani iznos ako se barem dio transakcije provodi u Uniji.
5. Ako se ne može utvrditi stvarni broj zahvaćenih klijenata ili partnerskih financijskih subjekata ili stvarni broj ili količina zahvaćenih transakcija, financijski subjekt te brojeve ili količine procjenjuje na temelju dostupnih podataka iz usporedivih referentnih razdoblja.

Članak 2.

Učinak na ugled

1. Za potrebe utvrđivanja učinka incidenta na ugled, kako je navedeno u članku 18. stavku 1. točki (a) Uredbe (EU) 2022/2554, financijski subjekti smatraju da je do učinka na ugled došlo ako je ispunjen barem jedan od sljedećih kriterija:
 - (a) incident se spominjao u medijima;
 - (b) incident je doveo do više pritužbi različitih klijenata ili partnerskih financijskih subjekata na usluge usmjerene na klijente ili ključne poslovne odnose;
 - (c) financijski subjekt neće moći ili vjerojatno neće moći ispuniti regulatorne zahtjeve zbog incidenta;
 - (d) financijski subjekt zbog incidenta će izgubiti ili će vjerojatno izgubiti klijente ili partnerske financijske subjekte koji imaju značajan utjecaj na njegovo poslovanje.

⁽⁹⁾ Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

2. Pri procjeni učinka incidenta na ugled financijski subjekti uzimaju u obzir razinu stvarne ili potencijalne vidljivosti incidenta u odnosu na svaki kriterij iz stavka 1.

Članak 3.

Trajanje i prekid rada usluge

1. Financijski subjekti mjere trajanje incidenta iz članka 18. stavka 1. točke (b) Uredbe (EU) 2022/2554 od trenutka njegova nastanka do trenutka rješavanja.

Ako financijski subjekti ne mogu utvrditi trenutak nastanka incidenta, mjere trajanje incidenta od trenutka njegova otkrivanja. Ako financijski subjekti saznaju da se incident dogodio prije nego što su ga otkrili, mjere trajanje od trenutka kad je incident zabilježen u evidenciji mreže ili sustava ili u drugim izvorima podataka.

Ako financijski subjekti još ne znaju kad će se incident riješiti ili ako ne mogu provjeriti evidenciju ili druge izvore podataka, koriste se procjenama.

2. Financijski subjekti mjere prekid rada usluge zbog incidenta kako je navedeno u članku 18. stavku 1. točki (b) Uredbe (EU) 2022/2554 od trenutka kad usluga bude u potpunosti ili djelomično nedostupna klijentima, financijskim partnerima ili drugim unutarnjim ili vanjskim korisnicima do trenutka ponovne uspostave redovne aktivnosti ili operacije na razini usluge prije incidenta. Ako prekid rada usluge uzrokuje kašnjenje u pružanju usluge nakon ponovne uspostave redovitih aktivnosti ili operacija, prekid rada mjeri se od početka incidenta do trenutka kad je ta zakašnjela usluga u potpunosti pružena.

Ako financijski subjekti ne mogu odrediti kad je rad usluge prekinut, mjere ga od trenutka kad je otkriven.

Članak 4.

Zemljopisna raširenost

Za potrebe utvrđivanja zemljopisne raširenosti s obzirom na područja zahvaćena incidentom kako je navedeno u članku 18. stavku 1. točki (c) Uredbe (EU) 2022/2554 financijski subjekti procjenjuju ima li incident ili je imao učinak u drugim državama članicama, a posebno značajnost učinka u odnosu na bilo što od sljedećeg:

- (a) klijenti i partnerski financijski subjekti u drugim državama članicama;
- (b) podružnice ili drugi financijski subjekti unutar grupe koji obavljaju djelatnosti u drugim državama članicama;
- (c) infrastrukture financijskog tržišta ili treće strane koje mogu utjecati na financijske subjekte u drugim državama članicama kojima pružaju usluge, u mjeri u kojoj su takve informacije dostupne.

Članak 5.

Gubici podataka

Za potrebe utvrđivanja gubitaka podataka zbog incidenta, kako je navedeno u članku 18. stavku 1. točki (d) Uredbe (EU) 2022/2554, financijski subjekti uzimaju u obzir sljedeće:

- (a) u pogledu dostupnosti podataka, jesu li zbog incidenta podaci na zahtjev financijskog subjekta, njegovih klijenata ili drugih ugovornih strana bili privremeno ili trajno nedostupni ili neupotrebljivi;
- (b) u pogledu vjerodostojnosti podataka, je li incident ugrozio pouzdanost izvora podataka;

- (c) u pogledu cjelovitosti podataka, je li incident doveo do neodobrene izmjene podataka zbog kojih su oni postali netočni ili nepotpuni;
- (d) u pogledu povjerljivosti podataka, je li incident doveo do toga da su neovlaštena strana ili sustav pristupili podacima ili da su im otkriveni podaci.

Članak 6.

Ključnost zahvaćenih usluga

Za potrebe utvrđivanja ključnosti zahvaćenih usluga, kako je navedeno u članku 18. stavku 1. točki (e) Uredbe (EU) 2022/2554, financijski subjekti u vezi incidenta procjenjuju:

- (a) utječe li ili je utjecao na IKT usluge ili mrežne i informacijske sustave kojima se podupiru ključne ili važne funkcije financijskog subjekta;
- (b) utječe li ili je utjecao na financijske usluge koje pruža financijski subjekt za koje je potrebno odobrenje, registracija ili koje nadziru nadležna tijela;
- (c) predstavlja ili je predstavljao uspješan, zlonamjeran i neovlašten pristup mrežnim i informacijskim sustavima financijskog subjekta.

Članak 7.

Ekonomski učinak

1. Za potrebe utvrđivanja ekonomskog učinka incidenta iz članka 18. stavka 1. točke (f) Uredbe (EU) 2022/2554 financijski subjekti, bez uračunavanja financijskih povrata, uzimaju u obzir sljedeće vrste izravnih i neizravnih troškova i gubitaka koje su pretrpjeli kao posljedicu incidenta:

- (a) oduzeta sredstva ili financijska imovina za koju su odgovorni, uključujući imovinu izgubljenu zbog krađe;
- (b) troškovi zamjene ili premještanja softvera, hardvera ili infrastrukture;
- (c) troškovi osoblja, uključujući troškove povezane sa zamjenom ili preseljenjem osoblja, zapošljavanjem dodatnog osoblja, naknadama za prekovremeni rad i povratom izgubljenih ili oslabljenih vještina;
- (d) naknade zbog neispunjavanja ugovornih obveza;
- (e) troškovi pravne zaštite i naknade kupcima;
- (f) gubici zbog izgubljenih prihoda;
- (g) troškovi povezani s unutarnjom i vanjskom komunikacijom;
- (h) troškovi savjetovanja, uključujući troškove povezane s pravnim savjetovanjem, forenzičkim uslugama i uslugama sanacije.

2. Troškovi i gubici iz stavka 1. ne uključuju troškove nužne za svakodnevno poslovanje, posebno sljedeće:

- (a) troškovi općeg održavanja infrastrukture, opreme, hardvera i softvera te troškovi osvježavanje vještina osoblja;
- (b) unutarnji ili vanjski troškovi za poboljšanje poslovanja nakon incidenta, uključujući nadogradnje, poboljšanja i inicijative za procjenu rizika;
- (c) premije osiguranja.

3. Financijski subjekti izračunavaju iznose troškova i gubitaka na temelju podataka dostupnih u trenutku izvješćivanja. Ako se stvarni iznosi troškova i gubitaka ne mogu utvrditi, financijski subjekti procjenjuju te iznose.

4. Pri procjeni ekonomskog učinka incidenta financijski subjekti zbrajaju troškove i gubitke iz stavka 1.

POGLAVLJE II.

ZNAČAJNI INCIDENTI I PRAGOVİ ZNAČAJNOSTI

Članak 8.

Značajni incidenti

1. Incident se smatra značajnim incidentom za potrebe članka 19. stavka 1. Uredbe (EU) 2022/2554 ako je utjecao na ključne usluge iz članka 6. i ako je ispunjen bilo koji od sljedećih uvjeta:

- (a) dosegnut je prag značajnosti iz članka 9. stavka 5. točke (b);
- (b) dosegnuta su dva ili više drugih pragova značajnosti iz članka 9. stavaka od 1. do 6.

2. Incidenti koji se ponavljaju, a koji se pojedinačno ne smatraju značajnim incidentom u skladu sa stavkom 1. smatraju se jednim značajnim incidentom ako ispunjavaju sve sljedeće uvjete:

- (a) dogodili su se najmanje dva puta u šest mjeseci;
- (b) imaju isti očit temeljni uzrok kako je navedeno u članku 20. prvom stavku točki (b) Uredbe (EU) 2022/2554;
- (c) zajednički ispunjavaju kriterije za značajni incident iz stavka 1.

Financijski subjekti svaki mjesec procjenjuju postoje li incidenti koji se ponavljaju.

Ovaj se stavak ne primjenjuje na mikropoduzeća i financijske subjekte navedene u članku 16. stavku 1. Uredbe (EU) 2022/2554.

Članak 9.

Pragovi značajnosti za utvrđivanje značajnih incidenata

1. Prag značajnosti za kriterij „klijenti, partnerski financijski subjekti i transakcije” ispunjen je ako je ispunjen bilo koji od sljedećih uvjeta:

- (a) broj zahvaćenih klijenata veći je od 10 % svih klijenata koji koriste zahvaćenu uslugu;
- (b) broj zahvaćenih klijenata koji koriste zahvaćenu uslugu veći je od 100 000;
- (c) broj zahvaćenih partnerskih financijskih subjekata veći je od 30 % svih partnerskih financijskih subjekata koji se bave aktivnostima povezanim s pružanjem zahvaćene usluge;
- (d) broj zahvaćenih transakcija veći je od 10 % prosječnog dnevnog broja transakcija koje je financijski subjekt proveo u vezi sa zahvaćenom uslugom;
- (e) količina transakcija na koje to utječe veća je od 10 % prosječne dnevne vrijednosti transakcija koje je financijski subjekt proveo u vezi sa zahvaćenom uslugom;
- (f) zahvaćeni su klijenti ili partnerski financijski subjekti koji su u skladu s člankom 1. stavkom 3. utvrđeni kao relevantni.

Ako se ne može utvrditi stvarni broj zahvaćenih klijenata ili partnerskih financijskih subjekata ili stvarni broj ili količina zahvaćenih transakcija, financijski subjekt te brojeve ili količine procjenjuje na temelju dostupnih podataka iz usporedivih referentnih razdoblja.

2. Prag značajnosti za kriterij „učinak na ugled” ispunjen je ako je ispunjen bilo koji od uvjeta iz članka 2. točaka od (a) do (d).

3. Prag značajnosti za kriterij „trajanje i prekid rada usluge” ispunjen je ako je ispunjen bilo koji od sljedećih uvjeta:

- (a) incident traje dulje od 24 sata;

- (b) prekid rada usluge dulji je od dva sata za IKT usluge kojima se podupiru ključne ili važne funkcije.
4. Prag značajnosti za kriterij „zemljopisna raširenost” ispunjen je ako incident utječe na dvije ili više država članica u skladu s člankom 4.
5. Prag značajnosti za kriterij „gubitak podataka” ispunjen je ako je ispunjen bilo koji od sljedećih uvjeta:
- (a) svaki učinak iz članka 5. na dostupnost, vjerodostojnost, cjelovitost ili povjerljivost podataka ima ili će imati negativan učinak na provedbu poslovnih ciljeva financijskog subjekta ili na njegovu sposobnost ispunjavanja regulatornih zahtjeva;
- (b) svaki uspješan, zlonamjeran i neovlašten pristup koji nije obuhvaćen točkom (a) odnosi se na mrežne i informacijske sustave, ako takav pristup može dovesti do gubitka podataka.
6. Prag značajnosti za kriterij „ekonomski učinak” ispunjen je ako su troškovi i gubici financijskog subjekta nastali zbog incidenta premašili ili je vjerojatno da će premašiti 100 000 EUR.

POGLAVLJE III.

OZBILJNE KIBERPRIJETNJE

Članak 10.

Visoki pragovi značajnosti za utvrđivanje ozbiljnih kiberprijetnji

Za potrebe članka 18. stavka 2. Uredbe (EU) 2022/2554, kiberprijetnja smatra se ozbiljnom ako su ispunjeni svi sljedeći uvjeti:

- (a) ako se kiberprijetnja realizira mogla bi utjecati ili je mogla utjecati na ključne ili važne funkcije financijskog subjekta ili bi mogla utjecati na druge financijske subjekte, treće strane koji su pružatelji usluga, klijente ili partnerske financijske subjekte, na temelju informacija dostupnih financijskom subjektu;
- (b) kiberprijetnja koja bi se vjerojatno mogla realizirati kod financijskog subjekta ili drugih financijskih subjekata, uzimajući u obzir barem sljedeće elemente:
- primjenjive rizike povezane s kiberprijetnjama iz točke (a), uključujući moguće ranjivosti sustava financijskog subjekta koje se mogu iskoristiti;
 - sposobnosti i namjere aktera prijetnji u mjeri u kojoj je to poznato financijskom subjektu;
 - postojanost prijetnje i spoznaje o incidentima koji su utjecali na financijski subjekt ili njegovu treću stranu koja je pružatelj usluga, klijente ili partnerske financijske subjekte;
- (c) ako se kiberprijetnja realizira, zadovoljila bi bilo što od sljedećeg:
- kriterij u pogledu ključnosti usluga utvrđen u članku 18. stavku 1. točki (e) Uredbe (EU) 2022/2554, kako je navedeno u članku 6. ove Uredbe;
 - prag značajnosti iz članka 9. stavka 1.;
 - prag značajnosti iz članka 9. stavka 4.

Ako, ovisno o vrsti kiberprijetnji i dostupnim informacijama, financijski subjekt zaključi da bi se pragovi značajnosti utvrđeni u članku 9. stavcima 2., 3., 5. i 6. mogli dosegnuti, mogu se razmotriti i ti pragovi.

POGLAVLJE IV.

**RELEVANTNOST ZNAČAJNIH INCIDENATA ZA NADLEŽNA TIJELA U DRUGIM DRŽAVAMA ČLANICAMA I
POJEDINOSTI O IZVJEŠĆIMA KOJE TREBA PODIJELITI S DRUGIM NADLEŽNIM TIJELIMA***Članak 11.***Relevantnost značajnih incidenata za nadležna tijela u drugim državama članicama**

Procjena je li značajan incident relevantan za nadležna tijela u drugim državama članicama kako je navedeno u članku 19. stavku 7. Uredbe (EU) 2022/2554 temelji se na tome ima li incident temeljni uzrok koji potječe iz druge države članice ili ima li znatan učinak u drugoj državi članici u odnosu na bilo što od sljedećeg:

- (a) klijenti ili partnerski financijski subjekti;
- (b) podružnica financijskog subjekta ili drugog financijskog subjekta unutar grupe;
- (c) infrastruktura financijskog tržišta ili treće strana koja je pružatelj usluga koja može utjecati na financijske subjekte kojima pružaju usluge.

*Članak 12.***Pojedinosti o značajnim incidentima razmjenjuju se s drugim nadležnim tijelima**

Pojedinosti o značajnim incidentima koje nadležna tijela trebaju dostaviti drugim nadležnim tijelima u skladu s člankom 19. stavkom 6. Uredbe (EU) 2022/2554 i obavijesti koje EBA, ESMA ili EIOPA i ESB trebaju dostaviti relevantnim nadležnim tijelima u drugim državama članicama u skladu s člankom 19. stavkom 7. te uredbe sadržavaju istu razinu informacija, bez anonimizacije, kao obavijesti i izvješća o značajnim incidentima primljene od financijskih subjekata u skladu s člankom 19. stavkom 4. Uredbe (EU) 2022/2554.

POGLAVLJE V.

ZAVRŠNE ODREDBE*Članak 13.***Stupanje na snagu**

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 13. ožujka 2024.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN