Uradni list
Evropske unije

SL
Serija L

2024/1772

25.6.2024

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1772

z dne 13. marca 2024

o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi o določitvi meril za razvrščanje incidentov, povezanih z IKT, in kibernetskih groženj, ter pragov pomembnosti in podrobnosti poročil o večjih incidentih

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 ([1]) ter zlasti člena 18(4), tretji pododstavek, Uredbe,

ob upoštevanju naslednjega:

(1) Cilj Uredbe (EU) 2022/2554 je harmonizirati in racionalizirati zahteve glede poročanja o incidentih, povezanih z IKT, ter operativnih ali varnostnih incidentih, povezanih s plačili, ki zadevajo kreditne institucije, plačilne institucije, ponudnike storitev zagotavljanja informacij o računih in institucije za izdajo elektronskega denarja (v nadaljnjem besedilu: incidenti). Glede na to, da zahteve glede poročanja zajemajo 20 različnih vrst finančnih subjektov, bi bilo treba merila za razvrščanje in pragove pomembnosti za določanje večjih incidentov in pomembnih kibernetskih groženj določiti na preprost, usklajen in dosleden način, ki upošteva posebnosti storitev in dejavnosti vseh zadevnih finančnih subjektov.

(2) Za zagotovitev sorazmernosti bi morala merila za razvrščanje in pragovi pomembnosti odražati velikost in splošni profil tveganja ter naravo, obseg in kompleksnost storitev vseh finančnih subjektov. Poleg tega bi morali biti merila in pragovi pomembnosti oblikovani tako, da se dosledno uporabljajo za vse finančne subjekte, ne glede na njihovo velikost in profil tveganja, in ne pomenijo nesorazmernega bremena poročanja za manjše finančne subjekte. Vendar bi bilo treba za obravnavo primerov, ko incident, ki sam po sebi ne presega veljavnega praga, prizadene znatno število strank, določiti absolutni prag, namenjen predvsem večjim finančnim subjektom.

(3) V zvezi z okviri za poročanje o incidentih, ki so obstajali pred začetkom veljavnosti Uredbe (EU) 2022/2554, bi bilo treba finančnim subjektom zagotoviti kontinuiteto. Zato bi bilo treba merila za razvrščanje in pragove pomembnosti uskladiti s smernicami EBA o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 Evropskega parlamenta in Sveta ([2]), smernicami o rednih informacijah in obveščanju o pomembnih spremembah, ki jih morajo repozitoriji sklenjenih poslov predložiti ESMA, okvirom ECB/SSM za poročanje o kibernetskih incidentih in drugimi ustreznimi smernicami. Merila in pragovi za razvrščanje bi morali biti primerni tudi za finančne subjekte, za katere pred Uredbo (EU) 2022/2554 niso veljale zahteve glede poročanja o incidentih.

(4) Kar zadeva merilo za razvrščanje „količina in število prizadetih transakcij“, je pojem transakcij širok in zajema različne dejavnosti in storitve v sektorskih aktih, ki se uporabljajo za finančne subjekte. Za namene tega merila za razvrščanje bi morale biti zajete plačilne transakcije in vse oblike menjave finančnih instrumentov, kriptosredstev, blaga ali drugih sredstev, tudi v obliki kritja, zavarovanja s premoženjem ali zastavne pravice, tako za gotovino kot za katero koli drugo sredstvo. Pri razvrščanju bi bilo treba upoštevati vse transakcije, ki vključujejo sredstva, katerih vrednost se lahko izrazi v denarnem znesku.

([1]) UL L 333, 27.12.2022, str. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.
([2]) Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (UL L 337, 23.12.2015, str. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Merila za razvrščanje bi morala zagotoviti, da so zajete vse ustrezne vrste večjih incidentov. Številna merila za razvrščanje ne zajamejo nujno kibernetskih napadov, povezanih z vdorom v omrežne ali informacijske sisteme. Kljub temu so pomembni, saj lahko vsak vdor v omrežne in informacijske sisteme škodi finančnemu subjektu. V skladu s tem bi bilo treba merili za razvrščanje „prizadete kritične storitve“ in „izgube podatkov“ določiti tako, da bi zajeli te vrste večjih incidentov, zlasti nepooblaščene vdore, ki lahko povzročijo resne posledice, zlasti kršitve varstva podatkov in uhajanje podatkov, tudi če učinki niso takoj znani.

(6) Ker za kreditne institucije veljata okvir za razvrščanje incidentov v skladu s členom 18 Uredbe (EU) 2022/2554 in okvir operativnega tveganja iz Delegirane uredbe Komisije (EU) 2018/959 ([3]), bi moral biti pristop za ocenjevanje gospodarskega učinka incidenta na podlagi izračuna stroškov in izgub v največji možni meri skladen v obeh okvirih, da bi se izognili uvedbi zahtev, ki so nezdružljive ali si nasprotujejo.

(7) Merilo v zvezi z geografsko razpršenostjo incidenta iz člena 18(1), točka (c), Uredbe (EU) 2022/2554 bi moralo biti osredotočeno na čezmejni učinek incidenta, saj bodo učinek incidenta na dejavnosti finančnega subjekta znotraj ene jurisdikcije zajela druga merila iz navedenega člena.

(8) Glede na to, da so merila za razvrščanje soodvisna in medsebojno povezana, bi moral pristop za identifikacijo večjih incidentov, o katerih je treba poročati v skladu s členom 19(1) Uredbe (EU) 2022/2554, temeljiti na kombinaciji meril, pri čemer bi morala imeti nekatera merila, ki so tesno povezana z opredelitvami incidenta, povezanega z IKT, in večjega incidenta, povezanega z IKT, iz člena 3(8) in (10) Uredbe (EU) 2022/2554 večji pomen pri razvrščanju večjih incidentov kot druga merila.

(9) Za zagotovitev, da se poročila in uradna obvestila o večjih incidentih, ki jih prejmejo pristojni organi v skladu s členom 19(1) Uredbe (EU) 2022/2554, uporabljajo tako za namene nadzora kot za preprečevanje širjenja negativnih učinkov v finančnem sektorju, bi morali pragovi pomembnosti omogočati zajetje večjih incidentov, med drugim z osredotočanjem na učinek na kritične storitve, specifične za subjekt, specifične absolutne in relativne pragove strank ali finančnih partnerjev, transakcije, ki kažejo na pomemben učinek na finančni subjekt, in na pomembnost učinka v drugih državah članicah.

(10) Incidente, ki prizadenejo storitve IKT ali omrežne in informacijske sisteme, ki podpirajo kritične ali pomembne funkcije, ali finančne storitve, za katere je potrebno dovoljenje, ali zlonameren nepooblaščen dostop do omrežnih in informacijskih sistemov, ki podpirajo kritične ali pomembne funkcije, bi bilo treba šteti za incidente, ki vplivajo na kritične storitve finančnih subjektov. Zlonameren, nepooblaščen dostop do omrežnih in informacijskih sistemov, ki podpirajo kritične ali pomembne funkcije finančnih subjektov, pomeni resno tveganje za finančni subjekt in bi ga bilo treba vedno šteti za večji incident, o katerem je treba poročati, ker lahko vpliva na druge finančne subjekte.

(11) Ponavljajoči se incidenti, povezani s podobnim očitnim temeljnim vzrokom, ki posamično niso večji incidenti, lahko kažejo na znatne pomanjkljivosti in slabosti v postopkih finančnega subjekta za obvladovanje incidentov in tveganj. Zato bi bilo treba ponavljajoče se incidente skupaj šteti za večje, kadar se zgodijo večkrat v določenem časovnem obdobju.

(12) Glede na to, da lahko kibernetske grožnje negativno vplivajo na finančni subjekt in sektor, bi bilo treba pri pomembnih kibernetskih grožnjah, ki jih lahko predložijo finančni subjekti, navesti verjetnost uresničitve in kritičnost potencialnega učinka. V skladu s tem bi morala biti za zagotovitev jasne in dosledne ocene pomembnosti kibernetskih groženj razvrstitev kibernetske grožnje kot pomembne odvisna od verjetnosti, da bi bili izpolnjena merila za razvrščanje večjih incidentov in njihov prag, če bi se grožnja uresničila, od vrste kibernetske grožnje in informacij, ki so na voljo finančnemu subjektu.

([3]) Delegirana uredba Komisije (EU) 2018/959 z dne 14. marca 2018 o dopolnitvi Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi opredelitve metodologije ocenjevanja, v skladu s katero pristojni organi institucijam dovolijo uporabo naprednih pristopov merjenja operativnega tveganja (UL L 169, 6.7.2018, str. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Glede na to, da je treba pristojne organe v drugih državah članicah uradno obvestiti o incidentih, ki vplivajo na finančne subjekte in stranke v njihovi jurisdikciji, bi morala ocena učinka v drugi jurisdikciji v skladu s členom 19(7) Uredbe (EU) 2022/2554 temeljiti na temeljnem vzroku incidenta, morebitnem širjenju negativnih učinkov prek tretjih ponudnikov in na infrastrukture finančnega trga ter učinku incidenta na pomembne skupine strank ali finančnih partnerjev.

(14) Postopki poročanja in uradnega obveščanja iz člena 19(6) in (7) Uredbe (EU) 2022/2554 bi morali zadevnim prejemnikom omogočiti, da ocenijo učinek incidentov. Zato bi morale poslane informacije zajemati vse podrobnosti iz poročil o incidentih, ki jih finančni subjekt predloži pristojnemu organu.

(15) Kadar incident pomeni kršitev varstva osebnih podatkov v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ([4]) in Direktivo 2002/58/ES Evropskega parlamenta in Sveta ([5]), ta uredba ne bi smela vplivati na obveznosti evidentiranja in obveščanja o kršitvah varstva osebnih podatkov, določene v navedeni zakonodaji Unije. Pristojni organi bi morali sodelovati in si izmenjevati informacije o vseh pomembnih zadevah z organi iz Uredbe (EU) 2016/679 in Direktive 2002/58/ES.

(16) Ta uredba temelji na osnutku regulativnih tehničnih standardov, ki so ga Komisiji predložili evropski nadzorni organi v posvetovanju z Agencijo Evropske unije za kibernetsko varnost (ENISA) in Evropsko centralno banko (ECB).

(17) Skupni odbor evropskih nadzornih organov iz člena 54 Uredbe (EU) št. 1093/2010 Evropskega parlamenta in Sveta ([6]), člena 54 Uredbe (EU) št. 1094/2010 Evropskega parlamenta in Sveta ([7]) ter člena 54 Uredbe (EU) št. 1095/2010 Evropskega parlamenta in Sveta ([8]) je organiziral odprta javna posvetovanja o osnutku regulativnih tehničnih standardov, na katerem temelji ta uredba, analiziral morebitne stroške in koristi predlaganih standardov ter zaprosil za nasvet interesno skupino za bančništvo, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1093/2010, interesno skupino za zavarovanja in pozavarovanja ter interesno skupino za poklicne pokojninske sklade, ustanovljeni v skladu s členom 37 Uredbe (EU) št. 1094/2010, ter interesno skupino za vrednostne papirje in trge, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1095/2010.

([4]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Direktiva 2002/58/ES evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Uredba (EU) št. 1094/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/79/ES (UL L 331, 15.12.2010, str. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Uredba (EU) št. 1095/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/77/ES (UL L 331, 15.12.2010, str. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([9]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 24. januarja 2024 –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

MERILA ZA RAZVRSTITEV

Člen 1

Stranke, finančni partnerji in transakcije

1. Število strank, ki jih je prizadel incident, iz člena 18(1), točka (a), Uredbe (EU) 2022/2554 odraža število vseh prizadetih strank, bodisi fizičnih bodisi pravnih oseb, ki med incidentom ne morejo ali niso mogle uporabljati storitve, ki jo zagotavlja finančni subjekt, ali na katere je incident negativno vplival. To število kot upravičenke do prizadete storitve vključuje tudi tretje osebe, ki so izrecno zajete v pogodbenem dogovoru med finančnim subjektom in stranko.

2. Število finančnih partnerjev, ki jih je prizadel incident, iz člena 18(1), točka (a), Uredbe (EU) 2022/2554 odraža število vseh prizadetih finančnih partnerjev, ki so s finančnim subjektom sklenili pogodbeni dogovor.

3. V zvezi s pomembnostjo strank in finančnih partnerjev, ki jih je prizadel incident, iz člena 18(1), točka (a), Uredbe (EU) 2022/2554 finančni subjekt upošteva, v kolikšni meri bo učinek na stranko ali finančnega partnerja prizadel izvajanje poslovnih ciljev finančnega subjekta, pa tudi morebitni učinek incidenta na učinkovitost trga.

4. Finančni subjekt v zvezi s količino ali številom transakcij, na katere je vplival incident, iz člena 18(1), točka (a), Uredbe (EU) 2022/2554 upošteva vse prizadete transakcije, ki vključujejo denarni znesek, kadar se vsaj en del transakcije izvede v Uniji.

5. Če dejanskega števila prizadetih strank ali finančnih partnerjev ali dejanskega števila ali količine prizadetih transakcij ni mogoče določiti, finančni subjekt oceni to število ali količino na podlagi razpoložljivih podatkov iz primerljivih referenčnih obdobij.

Člen 2

Vpliv na ugled

1. Za namene določanja vpliva incidenta na ugled iz člena 18(1), točka (a), Uredbe (EU) 2022/2554 finančni subjekti štejejo, da je prišlo do vpliva na ugled, kadar je izpolnjeno vsaj eno od naslednjih meril:

(a) o incidentu se je poročalo v medijih;

(b) incident je povzročil ponavljajoče se pritožbe različnih strank ali finančnih partnerjev v zvezi s storitvami, namenjenimi strankam, ali ključnimi poslovnimi odnosi;

(c) finančni subjekt zaradi incidenta ne bo mogel ali verjetno ne bo mogel izpolniti regulativnih zahtev;

(d) finančni subjekt bo ali bo verjetno zaradi incidenta izgubil stranke ali finančne partnerje, kar bo pomembno vplivalo na njegovo poslovanje.

([9]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Finančni subjekti pri ocenjevanju vpliva incidenta na ugled upoštevajo stopnjo prepoznavnosti, ki jo je incident dobil ali bi jo lahko dobil v zvezi z vsakim merilom iz odstavka 1.

Člen 3

Trajanje in nedelovanje storitve

1. Finančni subjekti merijo trajanje incidenta iz člena 18(1), točka (b), Uredbe (EU) 2022/2554 od trenutka, ko se incident zgodi, do takrat, ko se odpravi.

Kadar finančni subjekti ne morejo določiti trenutka, ko se je incident zgodil, merijo trajanje incidenta od trenutka, ko je bil odkrit. Kadar finančni subjekti ugotovijo, da se je incident zgodil, preden se je odkril, merijo trajanje od trenutka, ko je incident zabeležen v omrežnih ali sistemskih dnevnikih ali drugih virih podatkov.

Če finančni subjekti še ne vedo, kdaj bo incident odpravljen, ali ne morejo preveriti evidenc v dnevnikih ali drugih virih podatkov, uporabijo ocene.

2. Finančni subjekti merijo čas nedelovanja storitve zaradi incidenta iz člena 18(1), točka (b), Uredbe (EU) 2022/2554 od trenutka, ko storitev v celoti ali delno ni na voljo strankam, finančnim partnerjem ali drugim notranjim ali zunanjim uporabnikom, do trenutka, ko so bili redne dejavnosti ali delovanje obnovljeni na raven storitve, ki je bila zagotovljena pred incidentom. Kadar nedelovanje storitve povzroči zamudo pri zagotavljanju storitev po obnovitvi rednih dejavnosti ali delovanja, se čas nedelovanja meri od začetka incidenta do trenutka, ko je navedena zapoznela storitev v celoti zagotovljena.

Kadar finančni subjekti ne morejo določiti trenutka, ko se je začelo nedelovanje storitve, merijo trajanje nedelovanja storitve od trenutka, ko je bilo odkrito.

Člen 4

Geografska razpršenost

Za namene določitve geografske razpršenosti območij, ki jih je prizadel incident, iz člena 18(1), točka (c), Uredbe (EU) 2022/2554 finančni subjekti ocenijo, ali incident ima ali je imel učinek v drugih državah članicah, in zlasti pomen učinka na kar koli od naslednjega:

(a) stranke in finančne partnerje v drugih državah članicah;

(b) podružnice ali druge finančne subjekte v skupini, ki opravljajo dejavnosti v drugih državah članicah;

(c) infrastrukture finančnega trga ali tretje ponudnike, ki lahko vplivajo na finančne subjekte v drugih državah članicah, za katere opravljajo storitve, če so take informacije na voljo.

Člen 5

Izgube podatkov

Za namene določitve izgub podatkov, ki jih povzroči incident, iz člena 18(1), točka (d), Uredbe (EU) 2022/2554 finančni subjekti upoštevajo naslednje:

(a) v zvezi z razpoložljivostjo podatkov, ali so zaradi incidenta podatki na zahtevo finančnega subjekta, njegovih strank ali partnerjev začasno ali trajno nedostopni ali neuporabni;

(b) v zvezi z avtentičnostjo podatkov, ali je incident ogrozil zanesljivost vira podatkov;

(c) v zvezi s celovitostjo podatkov, ali je incident povzročil nepooblaščeno spremembo podatkov, zaradi katere so postali netočni ali nepopolni;

(d) v zvezi z zaupnostjo podatkov, ali je incident povzročil, da je do podatkov dostopala nepooblaščena stranka ali sistem oziroma da so bili podatki razkriti nepooblaščeni osebi ali sistemu.

Člen 6

Kritičnost prizadetih storitev

Za namene določitve kritičnosti prizadetih storitev, ki jih povzroči incident, iz člena 18(1), točka (e), Uredbe (EU) 2022/2554 finančni subjekti ocenijo, ali incident:

(a) prizadene ali je prizadel storitve IKT ali omrežne in informacijske sisteme, ki podpirajo kritične ali pomembne funkcije finančnega subjekta;

(b) prizadene ali je prizadel finančne storitve, ki jih zagotavlja finančni subjekt in za katere se zahteva dovoljenje ali registracija ali ki jih nadzorujejo pristojni organi;

(c) pomeni ali je pomenil uspešen, zlonameren in nepooblaščen dostop do omrežnih in informacijskih sistemov finančnega subjekta.

Člen 7

Gospodarski učinek

1. Za namene določanja gospodarskega učinka incidenta iz člena 18(1), točka (f), Uredbe (EU) 2022/2554 finančni subjekti brez obračunavanja finančnih izterjav upoštevajo naslednje vrste neposrednih in posrednih stroškov in izgub, ki so jih imeli zaradi incidenta:

(a) razlaščena ali finančna sredstva, za katera so odgovorni, vključno s sredstvi, izgubljenimi zaradi kraje;

(b) stroške zamenjave ali premestitve programske opreme, strojne opreme ali infrastrukture;

(c) stroške zaposlenih, vključno s stroški, povezanimi z zamenjavo ali premestitvijo zaposlenih, zaposlovanjem dodatnih zaposlenih, plačilom nadur in ponovno pridobitvijo izgubljenih ali oslabljenih spretnosti;

(d) nadomestila zaradi neizpolnjevanja pogodbenih obveznosti;

(e) stroške za odpravo škode in nadomestila za stranke;

(f) izgube zaradi izpada prihodkov;

(g) stroške, povezane z notranjo in zunanjo komunikacijo;

(h) stroške svetovanja, vključno s stroški, povezanimi s pravnim svetovanjem, forenzičnimi storitvami in storitvami ponovne vzpostavitve.

2. Stroški in izgube iz odstavka 1 ne vključujejo stroškov, ki so potrebni za tekoče poslovanje podjetja, zlasti:

(a) stroškov splošnega vzdrževanja infrastrukture, opreme, strojne in programske opreme ter stroškov posodabljanja spretnosti zaposlenih;

(b) notranjih ali zunanjih stroškov za izboljšanje poslovanja po incidentu, vključno s pobudami za nadgradnje, izboljšave in ocene tveganja;

(c) zavarovalnih premij.

3. Finančni subjekti izračunajo zneske stroškov in izgub na podlagi podatkov, ki so na voljo v času poročanja. Kadar dejanskih zneskov stroškov in izgub ni mogoče določiti, finančni subjekti te zneske ocenijo.

4. Finančni subjekti pri ocenjevanju gospodarskega učinka incidenta seštejejo stroške in izgube iz odstavka 1.

POGLAVJE II

VEČJI INCIDENTI IN PRAGOVI POMEMBNOSTI

Člen 8

Večji incidenti

1. Incident se šteje za večji incident za namene člena 19(1) Uredbe (EU) 2022/2554, če je prizadel kritične storitve iz člena 6 in če je izpolnjen eden od naslednjih pogojev:

(a) dosežen je prag pomembnosti iz člena 9(5), točka (b);

(b) izpolnjena sta dva ali več drugih pragov pomembnosti iz člena 9(1) do (6).

2. Ponavljajoči se incidenti, ki se posamično ne štejejo za večji incident v skladu z odstavkom 1, se štejejo za en večji incident, če izpolnjujejo vse naslednje pogoje:

(a) zgodili so se vsaj dvakrat v šestih mesecih;

(b) imajo isti očitni temeljni vzrok, kot je navedeno v členu 20, prvi pododstavek, točka (b), Uredbe (EU) 2022/2554;

(c) skupaj izpolnjujejo merila za to, da se štejejo za večji incident iz odstavka 1.

Finančni subjekti vsak mesec ocenijo obstoj ponavljajočih se incidentov.

Ta odstavek se ne uporablja za mikropodjetja in finančne subjekte iz člena 16(1) Uredbe (EU) 2022/2554.

Člen 9

Pragovi pomembnosti za določanje večjih incidentov

1. Prag pomembnosti za merilo „stranke, finančni partnerji in transakcije“ je izpolnjen, če je izpolnjen kateri koli od naslednjih pogojev:

(a) število prizadetih strank je večje od 10 % vseh strank, ki uporabljajo prizadeto storitev;

(b) število prizadetih strank, ki uporabljajo prizadeto storitev, je večje od 100 000;

(c) število prizadetih finančnih partnerjev je večje od 30 % vseh finančnih partnerjev, ki izvajajo dejavnosti, povezane z opravljanjem prizadete storitve;

(d) število prizadetih transakcij je večje od 10 % povprečnega dnevnega števila transakcij, ki jih izvede finančni subjekt v zvezi s prizadeto storitvijo;

(e) količina prizadetih transakcij je večja od 10 % povprečne dnevne vrednosti transakcij, ki jih izvede finančni subjekt v zvezi s prizadeto storitvijo;

(f) prizadete so bile stranke ali finančni partnerji, ki so bili identificirani kot relevantni v skladu s členom 1(3).

Če dejanskega števila prizadetih strank ali finančnih partnerjev ali dejanskega števila ali količine prizadetih transakcij ni mogoče določiti, finančni subjekt oceni to število ali količino na podlagi razpoložljivih podatkov iz primerljivih referenčnih obdobij.

2. Prag pomembnosti za merilo „vpliv na ugled“ je izpolnjen, če je izpolnjen kateri koli od pogojev iz člena 2, točke (a) do (d).

3. Prag pomembnosti za merilo „trajanje in nedelovanje storitve“ je izpolnjen, če je izpolnjen kateri koli od naslednjih pogojev:

(a) incident traja več kot 24 ur;

(b) nedelovanje storitve je daljše od dveh ur za storitve IKT, ki podpirajo kritične ali pomembne funkcije.

4. Prag pomembnosti za merilo „geografska razpršenost“ je izpolnjen, kadar ima incident učinek v dveh ali več državah članicah v skladu s členom 4.

5. Prag pomembnosti za merilo „izgube podatkov“ je izpolnjen, če je izpolnjen kateri koli od naslednjih pogojev:

(a) vsak učinek iz člena 5 na razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov negativno vpliva ali bo negativno vplival na izvajanje poslovnih ciljev finančnega subjekta ali na njegovo zmožnost izpolnjevanja regulativnih zahtev;

(b) vsak uspešen, zlonameren in nepooblaščen dostop, ki ni zajet v točki (a), do omrežnih in informacijskih sistemov, kadar lahko tak dostop povzroči izgube podatkov.

6. Prag pomembnosti za merilo „gospodarski učinek“ je izpolnjen, če so stroški in izgube, ki jih je imel finančni subjekt zaradi incidenta, presegli ali bodo verjetno presegli 100 000 EUR.

POGLAVJE III

POMEMBNE KIBERNETSKE GROŽNJE

Člen 10

Visoki pragovi pomembnosti za določanje pomembnih kibernetskih groženj

Za namene člena 18(2) Uredbe (EU) 2022/2554 se kibernetska grožnja šteje za pomembno, če so izpolnjeni vsi naslednji pogoji:

(a) če se kibernetska grožnja uresniči, lahko prizadene ali bi lahko prizadela kritične ali pomembne funkcije finančnega subjekta ali druge finančne subjekte, tretje ponudnike, stranke ali finančne partnerje, na podlagi informacij, ki so na voljo finančnemu subjektu;

(b) zelo verjetno je, da se bo kibernetska grožnja v finančnem subjektu ali drugih finančnih subjektih uresničila, pri čemer se upoštevajo vsaj naslednji elementi:

  (i) potencialna tveganja, povezana s kibernetsko grožnjo, iz točke (a), vključno z morebitnimi ranljivostmi sistemov finančnega subjekta, ki jih je mogoče izkoristiti;

  (ii) zmožnosti in namen akterjev groženj v obsegu, ki ga pozna finančni subjekt;

  (iii) trdovratnost grožnje in kakršno koli pridobljeno znanje o incidentih, ki so vplivali na finančni subjekt ali njegovega tretjega ponudnika, stranke ali finančne partnerje;

(c) če bi se kibernetska grožnja uresničila, bi lahko izpolnila kar koli od naslednjega:

  (i) merilo v zvezi s kritičnostjo storitev iz člena 18(1), točka (e), Uredbe (EU) 2022/2554, iz člena 6 te uredbe;

  (ii) prag pomembnosti iz člena 9(1);

  (iii) prag pomembnosti iz člena 9(4).

Kadar finančni subjekt glede na vrsto kibernetske grožnje in razpoložljive informacije sklene, da bi lahko bili doseženi pragovi pomembnosti iz člena 9(2), (3), (5) in (6), se lahko upoštevajo tudi ti pragovi.

POGLAVJE IV

POMEN VEČJIH INCIDENTOV ZA PRISTOJNE ORGANE V DRUGIH DRŽAVAH ČLANICAH IN PODROBNOSTI POROČIL, KI JIH JE TREBA DELITI Z DRUGIMI PRISTOJNIMI ORGANI

Člen 11

Pomen večjih incidentov za pristojne organe v drugih državah članicah

Ocena, ali večji incident zadeva pristojne organe v drugih državah članicah, kot je navedeno v členu 19(7) Uredbe (EU) 2022/2554, temelji na tem, ali ima incident temeljni vzrok, ki izvira iz druge države članice, oziroma ali incident v drugi državi članici pomembno vpliva ali je vplival na kar koli od naslednjega:

(a) stranke ali finančne partnerje;

(b) podružnico finančnega subjekta ali drugega finančnega subjekta v skupini;

(c) infrastrukturo finančnega trga ali tretjega ponudnika, ki lahko prizadene finančne subjekte, za katere opravlja storitve.

Člen 12

Podrobnosti o večjih incidentih, ki jih je treba deliti z drugimi pristojnimi organi

Podrobnosti o večjih incidentih, ki jih morajo pristojni organi zagotoviti drugim pristojnim organom v skladu s členom 19(6) Uredbe (EU) 2022/2554, in uradna obvestila, ki jih morajo EBA, ESMA ali EIOPA in ECB zagotoviti ustreznim pristojnim organom v drugih državah članicah v skladu s členom 19(7) navedene uredbe, vsebujejo enako raven informacij brez anonimizacije kot uradna obvestila in poročila o večjih incidentih, ki jih prejmejo od finančnih subjektov v skladu s členom 19(4) Uredbe (EU) 2022/2554.

POGLAVJE V

KONČNE DOLOČBE

Člen 13

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 13. marca 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN