2024/1772

25.6.2024 г.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2024/1772 НА КОМИСИЯТА

от 13 март 2024 година

за допълнение на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти, с които се определят подробно критериите за класифициране на инциденти с ИКТ и киберзаплахи, праговете на съществености и информацията в докладите за съществени инциденти

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 ([1]), и по-специално член 18, параграф 4, трета алинея от него,

като има предвид, че:

(1) Регламент (ЕС) 2022/2554 има за цел да се хармонизират и рационализират изискванията за докладване на инциденти с ИКТ и на съществени операционни или свързани със сигурността инциденти, свързани с плащания, засягащи кредитни институции, платежни институции, доставчици на услуги по предоставяне на информация за сметки и институции за електронни пари („инциденти“). Като се има предвид, че изискванията за докладване обхващат 20 различни вида финансови субекти, критериите за класифициране и праговете на съществености за определяне на съществени инциденти и значителни киберзаплахи следва да бъдат определени по прост, хармонизиран и последователен начин, който отчита спецификите на услугите и дейностите на всички съответни финансови субекти.

(2) За да се гарантира пропорционалност, критериите за класифициране и праговете на съществености следва да отразяват размера и цялостния рисков профил, както и естеството, мащаба и сложността на услугите на всички финансови субекти. Освен това критериите и праговете на съществености следва да бъдат разработени по такъв начин, че да се прилагат последователно за всички финансови субекти, независимо от техния размер и рисков профил, и да не създават непропорционална тежест при докладването от страна на по-малките финансови субекти. За да се отговори обаче на ситуации, при които значителен брой клиенти са засегнати от инцидент, който сам по себе си не надвишава приложимия праг, следва да се определи абсолютен праг, насочен главно към по-големите финансови субекти.

(3) По отношение на рамките за докладване на инциденти, които са се прилагали преди влизането в сила на Регламент (ЕС) 2022/2554, следва да се осигури приемственост за финансовите субекти. Поради това критериите за класифициране и праговете на съществености следва да бъдат приведени в съответствие и съобразени с Насоките на ЕБО относно докладването на съществени инциденти съгласно Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета ([2]), Насоките за периодично информиране и уведомяване за съществени промени, които трябва да бъдат представени на ЕОЦКП от регистрите на трансакции, Рамката на ЕЦБ/ЕНМ за докладване на киберинциденти и други подходящи насоки. Критериите и праговете за класифициране следва да са подходящи и за финансовите субекти, които не са били обект на изисквания за докладване на инциденти преди Регламент (ЕС) 2022/2554.

(4) По отношение на критерия за класифициране „размер и брой засегнати трансакции“, понятието трансакции е широко и обхваща различни дейности и услуги в секторните актове, приложими за финансовите субекти. За целите на този критерий за класифициране следва да бъдат обхванати платежните трансакции и всички форми на обмен на финансови инструменти, криптоактиви, стоки или всякакви други активи, в това число под формата на маржин, обезпечение или залог, както върху парични средства, така и върху всеки друг актив. Всички трансакции, които включват активи, чиято стойност може да бъде изразена в парична сума, следва да се вземат предвид за целите на класифицирането.

([1]) ОВ L 333, 27.12.2022 г., стр. 1, ELI:http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 г. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО (ОВ L 337, 23.12.2015 г., стр. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Критериите за класифициране следва да гарантират, че всички съответни видове съществени инциденти са обхванати. Кибератаките, свързани с проникване в мрежови или информационни системи, може да не са непременно обхванати от много критерии за класифициране. Те обаче са важни, тъй като всяко проникване в мрежови и информационни системи може да навреди на финансовия субект. Съответно критериите за класифициране „засегнати критични услуги“ и „загуби на данни“ следва да бъдат определени по такъв начин, че да обхващат тези видове съществени инциденти, по-специално непозволени прониквания, които, дори ако въздействията не са известни веднага, може да доведат до сериозни последствия, по-специално нарушения на сигурността на данните и изтичане на данни.

(6) Тъй като кредитните институции са предмет както на рамката за класифициране на инциденти съгласно член 18 от Регламент (ЕС) 2022/2554, така и на рамката за операционния риск съгласно Делегиран регламент (ЕС) 2018/959 на Комисията ([3]), подходът за оценка на икономическото въздействие на даден инцидент въз основа на изчисляване на разходите и загубите следва да бъде последователен във възможно най-голяма степен спрямо двете рамки, за да се избегне въвеждането на несъвместими или противоречиви изисквания.

(7) Критерият във връзка с географския обхват на даден инцидент, посочен в член 18, параграф 1, буква в) от Регламент (ЕС) 2022/2554, следва да е съсредоточен върху трансграничното въздействие на инцидента, тъй като въздействието на инцидента върху дейностите на даден финансов субект в рамките на една юрисдикция ще бъде обхванато от другите критерии, посочени в този член.

(8) С оглед на това, че критериите за класифициране са взаимозависими и взаимносвързани, подходът за идентифициране на съществени инциденти, които трябва да бъдат докладвани в съответствие с член 19, параграф 1 от Регламент (ЕС) 2022/2554, следва да се основава на комбинация от критерии, като някои от критериите, които са тясно свързани с определенията за инцидент с ИКТ и съществен инцидент с ИКТ, посочени в член 3, параграфи 8 и 10 от Регламент (ЕС) 2022/2554, следва да имат по-голяма тежест при класифицирането на съществени инциденти в сравнение с други критерии.

(9) С цел да се гарантира, че докладите и уведомленията за съществени инциденти, получени от компетентните органи съгласно член 19, параграф 1 от Регламент (ЕС) 2022/2554, служат както за надзорни цели, така и за предотвратяване на разпространението им в целия финансов сектор, праговете на същественост следва да дават възможност за обхващане на съществените инциденти и да бъдат насочени, наред с другото, към въздействието върху специфичните критични услуги на субекта, специфичните абсолютни и относителни прагове на клиентите или финансовите контрагенти, трансакциите, които показват съществено въздействие върху финансовия субект, и значимостта на въздействието в други държави членки.

(10) Инциденти, които засягат услуги в областта на ИКТ или мрежови и информационни системи, поддържащи критични или важни функции, или финансови услуги, изискващи разрешение, или злонамерен непозволен достъп до мрежови и информационни системи, поддържащи критични или важни функции, следва да се смятат за инциденти, засягащи критични услуги на финансовите субекти. Злонамереният, непозволен достъп до мрежови и информационни системи, поддържащи критични или важни функции на финансовите субекти, създава сериозни рискове за финансовия субект, и, тъй като те могат да засегнат други финансови субекти, винаги следва да се смята за съществен инцидент, който трябва да бъде докладван.

(11) Повтарящи се инциденти, свързани чрез сходна очевидна първопричина, които поотделно не са съществени инциденти, може да показват значителни недостатъци и слабости в процедурите на финансовия субект за управление на инциденти и за управление на риска. Поради това повтарящите се инциденти следва да се разглеждат съвкупно като съществени, когато настъпват многократно за определен период от време.

(12) Като се има предвид, че киберзаплахите могат да окажат отрицателно въздействие върху финансовия субект и сектора, значителните киберзаплахи, за които финансовите субекти могат да представят уведомление, следва да показват вероятността от осъществяване и критичността на потенциалното въздействие. Съответно, за да се осигури ясна и последователна оценка на значимостта на киберзаплахите, класифицирането на дадена киберзаплаха като значителна следва да зависи от вероятността за това критериите за класифициране на съществени инциденти да бъдат изпълнени, а праговете им да бъдат достигнати, ако заплахата се осъществи, от вида на киберзаплахата и от информацията, с която разполага финансовият субект.

([3]) Делегиран регламент (ЕС) 2018/959 на Комисията от 14 март 2018 г. за допълнение на Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти за определяне на методологията за оценка, съгласно която компетентните органи разрешават на институциите да използват усъвършенствани подходи за измерване на операционния риск (ОВ L 169, 6.7.2018 г., стр. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) С оглед на това, че компетентните органи в други държави членки трябва да бъдат уведомявани за инциденти, които засягат финансови субекти и клиенти в тяхната юрисдикция, оценката на въздействието в друга юрисдикция в съответствие с член 19, параграф 7 от Регламент (ЕС) 2022/2554 следва да се извършва въз основа на първопричината за инцидента, на потенциалното разпространение чрез трети страни доставчици и на инфраструктурите на финансовите пазари, както и въз основа на въздействието на инцидента върху значителни групи клиенти или финансови контрагенти.

(14) Процесите на докладване и уведомяване, посочени в член 19, параграфи 6 и 7 от Регламент (ЕС) 2022/2554, следва да позволяват на съответните получатели да оценяват въздействието на инцидентите. Следователно предадената информация трябва да обхваща всички подробности, съдържащи се в докладите за инциденти, представени от финансовия субект на компетентния орган.

(15) Когато даден инцидент представлява нарушение на сигурността на личните данни съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([4]) и Директива 2002/58/ЕО на Европейския парламент и на Съвета ([5]), настоящият регламент не следва да засяга задълженията за записване и уведомяване за нарушения на сигурността на личните данни, посочени в тези закони на Съюза. Компетентните органи следва да си сътрудничат и да обменят информация по всички съответни въпроси с органите, посочени в Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО.

(16) Настоящият регламент се основава на проектите на регулаторни технически стандарти, представени на Комисията от европейските банкови органи в консултации с Европейската агенция за киберсигурност (ENISA) и Европейската централна банка (ЕЦБ).

(17) Съвместният комитет на европейските надзорни органи, посочен в член 54 от Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета ([6]), в член 54 от Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета ([7]) и в член 54 от Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета, ([8]) проведе открити обществени консултации по проектите на регулаторни технически стандарти, въз основа на които е изготвен настоящият регламент, анализира потенциалните разходи и ползи от предложените стандарти и поиска мнението на Групата на участниците от банковия сектор, създадена в съответствие с член 37 от Регламент (ЕС) № 1093/2010, Групата на участниците от сектора на застраховането и презастраховането, създадена в съответствие с член 37 от Регламент (ЕС) № 1094/2010, и Групата на участниците от сектора на ценните книжа и пазарите, създадена в съответствие с член 37 от Регламент (ЕС) № 1095/2010.

([4]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за застраховане и професионално пенсионно осигуряване), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/79/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за ценни книжа и пазари), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/77/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([9]) беше проведена консултация с Европейския надзорен орган по защита на данните, който прие становище на 24 януари 2024 г.,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

КРИТЕРИИ ЗА КЛАСИФИЦИРАНЕ

Член 1

Клиенти, финансови контрагенти и трансакции

1. Броят на клиентите, засегнати от инцидента, както е посочено в член 18, параграф 1, буква а) от Регламент (ЕС) 2022/2554, отразява броя на всички засегнати клиенти, независимо дали са физически или юридически лица, които не могат или не са могли да се възползват от услугата, предоставяна от финансовия субект, по време на инцидента, или са били неблагоприятно повлияни от инцидента. Този брой включва също така трети страни, изрично обхванати от договорното споразумение между финансовия субект и клиента като получатели на засегнатата услуга.

2. Броят на финансовите контрагенти, засегнати от инцидента, както е посочено в член 18, параграф 1, буква а) от Регламент (ЕС) 2022/2554, отразява броя на всички засегнати финансови контрагенти, които са сключили договорно споразумение с финансовия субект.

3. По отношение на значимостта на клиентите и финансовите контрагенти, засегнати от инцидента, както е посочено в член 18, параграф 1, буква а) от Регламент (ЕС) 2022/2554, финансовият субект взема под внимание степента, до която въздействието върху даден клиент или финансов контрагент ще се отрази на изпълнението на стопанските цели на финансовия субект, както и потенциалното въздействие на инцидента върху пазарната ефективност.

4. Във връзка с размера или броя на трансакциите, засегнати от инцидента, както е посочено в член 18, параграф 1, буква а) от Регламент (ЕС) 2022/2554, финансовият субект взема под внимание всички засегнати трансакции, включващи парична сума, когато поне една част от трансакцията се извършва в Съюза.

5. Когато действителният брой на засегнатите клиенти или финансови контрагенти или действителният брой или размер на засегнатите трансакции не могат да бъдат определени, финансовият субект оценява тези числа или суми въз основа на наличните данни от сравними референтни периоди.

Член 2

Въздействие върху репутацията

1. За целите на определянето на въздействието на инцидента върху репутацията, както е посочено в член 18, параграф 1, буква а) от Регламент (ЕС) 2022/2554, финансовите субекти приемат, че въздействие върху репутацията е налице, когато е изпълнен поне един от следните критерии:

а) инцидентът е отразен в медиите;

б) инцидентът е довел до повтарящи се оплаквания от различни клиенти или финансови контрагенти относно насочени към клиента услуги или критични стопански отношения;

в) в резултат на инцидента финансовият субект няма да е в състояние или е вероятно да не е в състояние да изпълнява регулаторните изисквания;

г) в резултат на инцидента финансовият субект ще загуби или е вероятно да загуби клиенти или финансови контрагенти със съществено въздействие върху дейността му.

([9]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. При оценката на въздействието на инцидента върху репутацията финансовите субекти вземат под внимание нивото на видимост, което инцидентът е придобил или е вероятно да придобие по отношение на всеки от критериите, изброени в параграф 1.

Член 3

Продължителност и прекъсване на услугата

1. Финансовите субекти определят продължителността на инцидент, както е посочено в член 18, параграф 1, буква б) от Регламент (ЕС) 2022/2554, от момента на възникване на инцидента до момента на разрешаването му.

Когато финансовите субекти не могат да определят момента, в който е настъпил инцидентът, те определят продължителността на инцидента от момента, в който е бил открит. Когато финансовите субекти узнаят, че инцидентът е настъпил, преди да бъде открит, те определят продължителността му от момента, в който инцидентът е записан в мрежовите или системните регистри или в други източници на данни.

Когато финансовите субекти все още не знаят кога ще бъде разрешен инцидентът или не са в състояние да проверят записите в регистрите или в други източници на данни, те прилагат приблизителни оценки.

2. Финансовите субекти определят периода на прекъсване на услугата при инцидент, както е посочено в член 18, параграф 1, буква б) от Регламент (ЕС) 2022/2554, от момента, в който услугата е напълно или частично недостъпна за клиенти, финансови контрагенти или други вътрешни или външни потребители, до момента, в който редовните дейности или операции бъдат възстановени до предоставяното преди инцидента ниво на услугата. Когато прекъсването на услугата води до забавяне при предоставянето на услугата, след като редовните дейности или операции са били възстановени, периодът на прекъсване се определя от началото на инцидента до момента, в който тази забавена услуга бъде предоставена изцяло.

Когато финансовите субекти не могат да определят момента, в който е започнало прекъсването на услугата, те определят периода на прекъсване на услугата от момента на неговото откриване.

Член 4

Географски обхват

За целите на определянето на географския обхват по отношение на районите, засегнати от инцидента, както е посочено в член 18, параграф 1, буква в) от Регламент (ЕС) 2022/2554, финансовите субекти оценяват дали инцидентът има или е имал въздействие в други държави членки, и по-специално значимостта на въздействието във връзка с някое от следните:

а) клиенти и финансови контрагенти в други държави членки;

б) клонове или други финансови субекти в рамките на групата, извършващи дейности в други държави членки;

в) инфраструктури на финансовите пазари или трети страни доставчици, които може да засегнат финансови субекти в други държави членки, на които те предоставят услуги, доколкото такава информация е налична.

Член 5

Загуби на данни

За целите на определянето на загубите на данни в резултат на инцидента, както е посочено в член 18, параграф 1, буква г) от Регламент (ЕС) 2022/2554, финансовите субекти вземат под внимание следното:

а) по отношение на наличността на данни, дали инцидентът е довел до това данните, поискани от финансовия субект, негови клиенти или негови контрагенти, да бъдат временно или системно недостъпни или неизползваеми;

б) по отношение на автентичността на данните, дали инцидентът е компрометирал достоверността на източника на данни;

в) по отношение на цялостността на данните, дали инцидентът е довел до непозволена промяна на данните, в резултат на която те са станали неточни или непълни;

г) по отношение на поверителността на данните, дали инцидентът е довел до достъп до данни или до разкриване на данни на неупълномощена страна или система.

Член 6

Критичност на засегнатите услуги

За целите на определянето на критичността на засегнатите услуги, както е посочено в член 18, параграф 1, буква д) от Регламент (ЕС) 2022/2554, финансовите субекти оценяват дали инцидентът:

а) засяга или е засегнал услуги в областта на ИКТ или мрежови и информационни системи, поддържащи критични или важни функции на финансовия субект;

б) засяга или е засегнал финансови услуги, предоставяни от финансовия субект, които изискват разрешение, регистрация или които са предмет на надзор от компетентните органи;

в) представлява или е представлявал успешен злонамерен и непозволен достъп до мрежовите и информационните системи на финансовия субект.

Член 7

Икономическо въздействие

1. За целите на определянето на икономическото въздействие на инцидента, както е посочено в член 18, параграф 1, буква е) от Регламент (ЕС) 2022/2554, финансовите субекти, без да отчитат финансовите възстановявания, вземат под внимание следните видове преки и непреки разходи и загуби, които са понесли в резултат на инцидента:

а) иззети средства или финансови активи, за които носят отговорност, включително загубени активи в резултат на кражба;

б) разходи за замяна или преместване на софтуер, хардуер или инфраструктура;

в) разходи за персонал, включително разходи, свързани със замяна или преместване на персонал, наемане на допълнителен персонал, възнаграждение за извънреден труд и възстановяване на загубени или нарушени умения;

г) такси поради неспазване на договорни задължения;

д) разходи за правна защита и обезщетение на клиенти;

е) загуби поради пропуснати приходи;

ж) разходи, свързани с вътрешна и външна комуникация;

з) консултантски разходи, включително разходи, свързани с правни консултации, криминалистични анализи и услуги за възстановяване.

2. Разходите и загубите, посочени в параграф 1, не включват разходи, които са необходими за всекидневното осъществяване на дейността, по-специално следното:

а) разходи за обща поддръжка на инфраструктура, оборудване, хардуер и софтуер и разходи за поддържане на уменията на персонала на актуално ниво;

б) вътрешни или външни разходи за подобряване на дейността след инцидента, включително обновявания, подобрения и инициативи за оценка на риска;

в) застрахователни премии.

3. Финансовите субекти изчисляват размера на разходите и загубите въз основа на данните, налични към момента на докладването. Когато действителният размер на разходите и загубите не може да бъде определен, финансовите субекти правят оценки за тях.

4. Когато оценяват икономическото въздействие на инцидента, финансовите субекти сумират разходите и загубите, посочени в параграф 1.

ГЛАВА II

СЪЩЕСТВЕНИ ИНЦИДЕНТИ И ПРАГОВЕ НА СЪЩЕСТВЕНОСТ

Член 8

Съществени инциденти

1. Даден инцидент се смята за съществен инцидент за целите на член 19, параграф 1 от Регламент (ЕС) 2022/2554, когато е засегнал критични услуги, както е посочено в член 6, и когато е изпълнено едно от следните условия:

а) достигнат е прагът на същественост, посочен в член 9, параграф 5, буква б);

б) достигнати са два или повече от другите прагове на същественост, посочени в член 9, параграфи 1—6.

2. Повтарящи се инциденти, които поотделно не се смятат за съществен инцидент в съответствие с параграф 1, се смятат за един съществен инцидент, когато отговарят на всяко от следните условия:

а) възникнали са поне два пъти в рамките на 6 месеца;

б) имат същата очевидна първопричина, както е посочено в член 20, първа алинея, буква б) от Регламент (ЕС) 2022/2554;

в) съвкупно отговарят на критериите да бъдат смятани за съществен инцидент, посочени в параграф 1.

Финансовите субекти оценяват наличието на повтарящи се инциденти на месечна основа.

Настоящият параграф не се прилага за микропредприятия и финансови субекти, изброени в член 16, параграф 1 от Регламент (ЕС) 2022/2554.

Член 9

Прагове на същественост за определянето на съществени инциденти

1. Прагът на същественост за критерия „клиенти, финансови контрагенти и трансакции“ е достигнат, когато е изпълнено някое от следните условия:

а) броят на засегнатите клиенти е по-голям от 10 % от всички клиенти, използващи засегнатата услуга;

б) броят на засегнатите клиенти, използващи засегнатата услуга, е повече от 100 000;

в) броят на засегнатите финансови контрагенти е повече от 30 % от всички финансови контрагенти, извършващи дейности, свързани с предоставянето на засегнатата услуга;

г) броят на засегнатите трансакции е по-голям от 10 % от среднодневния брой трансакции, извършени от финансовия субект, свързани със засегнатата услуга;

д) размерът на засегнатите трансакции е по-голям от 10 % от среднодневната стойност на трансакциите, извършени от финансовия субект, свързани със засегнатата услуга;

е) клиенти или финансови контрагенти, които са определени като значими в съответствие с член 1, параграф 3, са били засегнати.

Когато действителният брой на засегнатите клиенти или финансови контрагенти или действителният брой или размер на засегнатите трансакции не могат да бъдат определени, финансовият субект оценява този брой или размер въз основа на наличните данни от сравними референтни периоди.

2. Прагът на същественост за критерия „въздействие върху репутацията“ е достигнат, когато е изпълнено някое от условията, посочени в член 2, букви а)—г).

3. Прагът на същественост за критерия „продължителност и прекъсване на услугата“ е достигнат, когато е изпълнено някое от следните условия:

а) продължителността на инцидента е повече от 24 часа;

б) прекъсването на услугата е над 2 часа за услуги в областта на ИКТ, поддържащи критични или важни функции.

4. Прагът на същественост за критерия „географски обхват“ е достигнат, когато инцидентът има въздействие в две или повече държави членки в съответствие с член 4.

5. Прагът на същественост за критерия „загуба на данни“ е достигнат, когато е изпълнено някое от следните условия:

а) всяко посочено в член 5 въздействие върху наличността, автентичността, цялостността или поверителността на данните има или ще има неблагоприятно въздействие върху изпълнението на стопанските цели на финансовия субект или върху способността му да отговаря на регулаторните изисквания;

б) всеки успешен злонамерен и непозволен достъп до мрежови и информационни системи, който не е обхванат от буква а), когато такъв достъп може да доведе до загуба на данни.

6. Прагът на същественост за критерия „икономическо въздействие“ е достигнат, когато разходите и загубите, понесени от финансовия субект поради инцидента, са надвишили или е вероятно да надвишат 100 000 евро.

ГЛАВА III

ЗНАЧИТЕЛНИ КИБЕРЗАПЛАХИ

Член 10

Високи прагове на същественост при определяне на значителни киберзаплахи

За целите на член 18, параграф 2 от Регламент (ЕС) 2022/2554 дадена киберзаплаха се смята за значителна, когато са изпълнени всички посочени по-долу условия:

а) въз основа на информацията, с която разполага финансовият субект, ако киберзаплахата се осъществи, тя би могла да засегне или може да е засегнала критични или важни функции на финансовия субект, или би могла да засегне други финансови субекти, трети страни доставчици, клиенти или финансови контрагенти;

б) има голяма вероятност киберзаплахата да се осъществи по отношение на финансовия субект или на други финансови субекти, като се отчитат най-малко следните елементи:

i) приложимите рискове, свързани с киберзаплахата, посочена в буква а), включително потенциални уязвими места на системите на финансовия субект, които може да бъдат използвани;

ii) способностите и намеренията на участниците в заплахата, доколкото са известни на финансовия субект;

iii) продължаването на заплахата и всяко натрупано знание за инциденти, които са засегнали финансовия субект или неговия доставчик трета страна, клиенти или финансови контрагенти;

в) ако се осъществи, киберзаплахата би могла да отговаря на някое от следните условия:

i) на критерия относно критичността на услугите, посочен в член 18, параграф 1, буква д) от Регламент (ЕС) 2022/2554, както е посочено в член 6 от настоящия регламент;

ii) на прага на същественост, определен в член 9, параграф 1;

iii) на прага на същественост, определен в член 9, параграф 4.

Когато в зависимост от вида на киберзаплахата и наличната информация финансовият субект стигне до заключението, че праговете на същественост, посочени в член 9, параграфи 2, 3, 5 и 6, може да бъдат достигнати, тези прагове също може да се вземат под внимание.

ГЛАВА IV

ЗНАЧИМОСТ НА СЪЩЕСТВЕНИТЕ ИНЦИДЕНТИ ЗА КОМПЕТЕНТНИТЕ ОРГАНИ В ДРУГИ ДЪРЖАВИ ЧЛЕНКИ И ИНФОРМАЦИЯ В ДОКЛАДИТЕ, КОЯТО ТРЯБВА ДА СЕ СПОДЕЛЯ С ДРУГИ КОМПЕТЕНТНИ ОРГАНИ

Член 11

Значимост на съществените инциденти за компетентните органи в други държави членки

Оценката на това дали съществениият инцидент е от значение за компетентните органи в други държави членки, както е посочено в член 19, параграф 7 от Регламент (ЕС) 2022/2554, се основава на това дали инцидентът е с първопричина, произтичаща от друга държава членка, или инцидентът има или е имал значително въздействие в друга държава членка във връзка с някое от следните:

а) клиенти или финансови контрагенти;

б) клон на финансовия субект или друг финансов субект в рамките на групата;

в) инфраструктура на финансов пазар или трета страна доставчик, която може да засегне финансови субекти, на които те предоставят услуги.

Член 12

Информация за съществени инциденти, която трябва да се споделя с други компетентни органи

Подробностите за съществени инциденти, които компетентните органи трябва да предоставят на други компетентни органи в съответствие с член 19, параграф 6 от Регламент (ЕС) 2022/2554, и уведомленията, които трябва да се подават от ЕБО, ЕОЦКП или ЕОЗППО и ЕЦБ до съответните компетентни органи в други държави членки в съответствие с член 19, параграф 7 от посочения регламент, съдържат същото ниво на информация, без анонимизиране, каквато се съдържа в уведомленията и докладите за съществени инциденти, получени от финансови субекти в съответствие с член 19, параграф 4 от Регламент (ЕС) 2022/2554.

ГЛАВА V

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 13

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 13 март 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN