2024/1772

25.6.2024

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2024/1772

av den 13 mars 2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar kriterierna för klassificering av IKT-relaterade incidenter och cyberhot, fastställande av väsentlighetströsklar och närmare uppgifter om rapporter om allvarliga incidenter

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 ([1]), särskilt artikel 18.4 tredje stycket, och

av följande skäl:

(1) Förordning (EU) 2022/2554 syftar till att harmonisera och effektivisera rapporteringskraven för IKT-relaterade incidenter och för betalningsrelaterade operativa incidenter eller säkerhetsincidenter som rör kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar (*incidenter*). Med tanke på att rapporteringskraven omfattar 20 olika typer av finansiella entiteter bör klassificeringskriterierna och väsentlighetströsklarna för att fastställa allvarlig incidenter och betydande cyberhot specificeras på ett enkelt, harmoniserat och konsekvent sätt som tar hänsyn till särdragen i alla relevanta finansiella entiteters tjänster och verksamheter.

(2) För att säkerställa proportionalitet bör klassificeringskriterierna och väsentlighetströsklarna återspegla alla finansiella entiteters storlek och övergripande riskprofil samt karaktären på, omfattningen av och komplexiteten i deras tjänster. Dessutom bör kriterierna och väsentlighetströsklarna utformas på ett sådant sätt att de tillämpas konsekvent på alla finansiella entiteter, oavsett storlek och riskprofil, och inte medför en oproportionell rapporteringsbörda för mindre finansiella entiteter. För att hantera situationer där ett betydande antal kunder påverkas av en incident som i sig inte överskrider det tillämpliga tröskelvärdet, bör dock ett absolut tröskelvärde fastställas som främst riktar sig till större finansiella entiteter.

(3) När det gäller ramverk för incidentrapportering som har funnits före ikraftträdandet av förordning (EU) 2022/2554, bör kontinuiteten för finansiella entiteter säkerställas. Därför bör klassificeringskriterierna och väsentlighetströsklarna anpassas till och inspireras av EBA:s riktlinjer om rapportering av allvarliga incidenter enligt Europaparlamentets och rådets direktiv (EU) 2015/2366 ([2]), riktlinjerna om regelbunden information och anmälan av väsentliga förändringar som ska lämnas till Esma av transaktionsregister, tillsynsnämndens ramverk för rapportering av cyberincidenter och andra relevanta riktlinjer. Klassificeringskriterierna och tröskelvärdena bör också vara lämpliga för de finansiella entiteter som inte har varit föremål för krav på incidentrapportering före förordning (EU) 2022/2554.

(4) När det gäller klassificeringskriteriet *mängd och antal transaktioner som påverkas* är begreppet transaktioner brett och omfattar olika verksamheter och tjänster i de sektorsspecifika rättsakter som är tillämpliga på finansiella entiteter. Detta klassificeringskriterium bör tillämpas på betalningstransaktioner och alla former av utbyte av finansiella instrument, kryptotillgångar, råvaror eller andra tillgångar, även i form av marginalsäkerheter, säkerheter eller pant, både mot kontanter och mot andra tillgångar. Alla transaktioner som omfattar tillgångar vars värde kan uttryckas i ett penningbelopp bör beaktas vid klassificeringen.

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

([2]) Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Klassificeringskriterierna bör säkerställa att alla relevanta typer av allvarliga incidenter fångas upp. Cyberangrepp som rör intrång i nätverk eller informationssystem fångas inte nödvändigtvis upp av många klassificeringskriterier. De är dock viktiga eftersom intrång i nätverks- och informationssystem kan skada den finansiella entiteten. Klassificeringskriterierna *kritiska tjänster som påverkas* och *dataförluster* bör därför specificeras på ett sådant sätt att de omfattar dessa typer av allvarliga incidenter, särskilt obehöriga intrång som även om effekterna inte är omedelbart kända kan leda till allvarliga konsekvenser, särskilt dataintrång och dataläckage.

(6) Eftersom kreditinstitut omfattas både av ramen för klassificering av incidenter enligt artikel 18 i förordning (EU) 2022/2554 och av ramen för operativ risk enligt kommissionens delegerade förordning (EU) 2018/959 ([3]), bör metoden för att bedöma den ekonomiska effekten av en incident baserat på beräkningen av kostnader och förluster i största möjliga utsträckning vara konsekvent inom båda ramarna för att undvika att införa oförenliga eller motsägelsefulla krav.

(7) Kriteriet avseende den geografiska spridningen av en incident i artikel 18.1 c i förordning (EU) 2022/2554 bör fokusera på incidentens gränsöverskridande påverkan, eftersom påverkan av en incident på en finansiell entitets verksamhet inom en enda jurisdiktion kommer att fångas upp av de andra kriterier som anges i den artikeln.

(8) Med tanke på att klassificeringskriterierna är beroende av och kopplade till varandra bör metoden för att identifiera allvarliga incidenter som ska rapporteras i enlighet med artikel 19.1 i förordning (EU) 2022/2554 baseras på en kombination av kriterier, där vissa kriterier som är nära kopplade till definitionerna av en IKT-relaterad incident och en allvarlig IKT-relaterad incident i artikel 3.8 och 3.10 i förordning (EU) 2022/2554 bör ha större betydelse vid klassificeringen av allvarliga incidenter än andra kriterier.

(9) I syfte att säkerställa att de rapporter om och anmälningar av allvarliga incidenter som de behöriga myndigheterna mottar enligt artikel 19.1 i förordning (EU) 2022/2554 används både för tillsynsändamål och för att förhindra spridning inom den finansiella sektorn, bör väsentlighetströsklarna göra det möjligt att fånga upp allvarliga incidenter genom att bland annat fokusera på inverkan på enhetsspecifika kritiska tjänster, de specifika absoluta och relativa trösklarna för kunder eller finansiella motparter, transaktioner som tyder på en betydande inverkan på den finansiella entiteten och inverkans betydelse i andra medlemsstater.

(10) Incidenter som påverkar IKT-tjänster eller nätverks- och informationssystem som stöder kritiska eller viktiga funktioner, eller finansiella tjänster som kräver godkännande eller skadlig obehörig åtkomst till nätverks- och informationssystem som stöder kritiska eller viktiga funktioner, bör betraktas som incidenter som påverkar de finansiella entiteternas kritiska tjänster. Skadlig, obehörig åtkomst till nätverks- och informationssystem som stöder kritiska eller viktiga funktioner hos finansiella entiteter utgör allvarliga risker för den finansiella entiteten och bör, eftersom de kan påverka andra finansiella entiteter, alltid betraktas som allvarliga incidenter som ska rapporteras.

(11) Återkommande incidenter som är kopplade till varandra genom en liknande uppenbar grundorsak, men som var för sig inte är allvarliga incidenter, kan tyda på betydande brister och svagheter i den finansiella entitetens incident- och riskhanteringsförfaranden. Därför bör återkommande incidenter betraktas som viktiga kollektivt om de inträffar upprepade gånger under en viss tidsperiod.

(12) Med tanke på att cyberhot kan ha en negativ inverkan på den finansiella entiteten och sektorn, bör de betydande cyberhot som finansiella entiteter kan lämna in ange sannolikheten för materialisering och hur kritisk den potentiella inverkan är. För att säkerställa en tydlig och konsekvent bedömning av cyberhotens betydelse bör klassificeringen av ett cyberhot som betydande därför vara beroende av sannolikheten för att klassificeringskriterierna för allvarliga incidenter och deras tröskelvärde skulle uppfyllas om hotet hade materialiserats, av typen av cyberhot och av den information som är tillgänglig för den finansiella entiteten.

([3]) Kommissionens delegerade förordning (EU) 2018/959 av den 14 mars 2018 om komplettering av Europaparlamentets och rådets förordning (EU) nr 575/2013 vad gäller tekniska tillsynsstandarder för specificeringen av de metoder som de behöriga myndigheterna använder för att bedöma om institut ska tillåtas att använda internmätningsmetoder för operativ risk (EUT L 169, 6.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Med tanke på att behöriga myndigheter i andra medlemsstater ska underrättas om incidenter som påverkar finansiella entiteter och kunder i deras jurisdiktion, bör bedömningen av påverkan i en annan jurisdiktion i enlighet med artikel 19.7 i förordning (EU) 2022/2554 baseras på grundorsaken till incidenten, på potentiell spridning genom tredjepartsleverantörer och på finansmarknadsinfrastrukturer samt på incidentens inverkan på betydande grupper av kunder eller finansiella motparter.

(14) De rapporterings- och anmälningsförfaranden som avses i artikel 19.6 och 19.7 i förordning (EU) 2022/2554 bör göra det möjligt för respektive mottagare att bedöma incidenternas inverkan. Den översända informationen bör därför omfatta alla uppgifter i de incidentrapporter som den finansiella entiteten lämnar till den behöriga myndigheten.

(15) Om en incident utgör en personuppgiftsincident enligt Europaparlamentets och rådets förordning (EU) 2016/679 ([4]) och Europaparlamentets och rådets direktiv 2002/58/EG ([5]) bör den här förordningen inte påverka de skyldigheter att registrera och anmäla personuppgiftsincidenter som fastställs i denna unionslagstiftning. De behöriga myndigheterna bör samarbeta och utbyta information om alla relevanta frågor med de myndigheter som avses i förordning (EU) 2016/679 och direktiv 2002/58/EG.

(16) Denna förordning grundar sig på det förslag till tekniska standarder för tillsyn som de europeiska tillsynsmyndigheterna har överlämnat till kommissionen i samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa) och Europeiska centralbanken (ECB).

(17) Den gemensamma kommittén för de europeiska tillsynsmyndigheterna, som avses i artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([6]), i artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1094/2010 ([7]) och i artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([8]), har genomfört öppna offentliga samråd om det förslag till tekniska standarder för tillsyn som den här förordningen grundar sig på, analyserat de potentiella kostnaderna och fördelarna med de föreslagna standarderna och begärt råd från den bankintressentgrupp som inrättats i enlighet med artikel 37 i förordning (EU) nr 1093/2010, den intressentgrupp för försäkring och återförsäkring och den intressentgrupp för tjänstepensioner som inrättats i enlighet med artikel 37 i förordning (EU) nr 1094/2010 samt den intressentgrupp för värdepapper och marknader som inrättats i enlighet med artikel 37 i förordning (EU) nr 1095/2010.

([4]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([9]) och avgav ett yttrande den 24 januari 2024.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

KLASSIFICERINGSKRITERIER

Artikel 1

Kunder, finansiella motparter och transaktioner

1. Antalet kunder som påverkas av en incident enligt artikel 18.1 a i förordning (EU) 2022/2554 ska återspegla det totala antalet kunder som påverkas, oavsett om de är fysiska eller juridiska personer, och som inte kan eller kunde använda den tjänst som den finansiella entiteten tillhandahöll under incidenten eller som påverkades negativt av incidenten. Detta antal ska även omfatta tredje parter som uttryckligen omfattas av det kontraktsmässiga arrangemanget mellan den finansiella entiteten och kunden som mottagare av den berörda tjänsten.

2. Antalet finansiella motparter som påverkas av incidenten enligt artikel 18.1 a i förordning (EU) 2022/2554 ska återspegla det totala antalet berörda finansiella motparter som har ingått ett kontraktsmässigt arrangemang med den finansiella entiteten.

3. När det gäller betydelsen av kunder och finansiella motparter som påverkas av incidenten enligt artikel 18.1 a i förordning (EU) 2022/2554 ska den finansiella entiteten ta hänsyn till i vilken utsträckning påverkan på en kund eller en finansiell motpart kommer att påverka genomförandet av den finansiella entitetens verksamhetsmål, samt incidentens potentiella påverkan på marknadseffektiviteten.

4. När det gäller mängden eller antalet transaktioner som påverkas av incidenten enligt i artikel 18.1 a i förordning (EU) 2022/2554 ska den finansiella entiteten ta hänsyn till alla berörda transaktioner som omfattar ett monetärt belopp där minst en del av transaktionen genomförs i unionen.

5. Om det faktiska antalet kunder eller finansiella motparter som påverkas eller det faktiska antalet eller den faktiska mängden transaktioner som påverkas inte kan fastställas, ska den finansiella entiteten uppskatta dessa på grundval av tillgängliga uppgifter från jämförbara referensperioder.

Artikel 2

Påverkan på anseendet

1. Vid fastställandet av incidentens påverkan på anseendet enligt artikel 18.1 a i förordning (EU) 2022/2554 ska finansiella entiteter anse att en påverkan på anseendet har uppstått om minst ett av följande kriterier är uppfyllt:

a) Incidenten har återspeglats i medierna.

b) Incidenten har lett till upprepade klagomål från olika kunder eller finansiella motparter om tjänster riktade mot kunder eller kritiska affärsförbindelser.

c) Den finansiella entiteten kommer inte att kunna eller kommer sannolikt inte att kunna uppfylla lagstadgade krav till följd av incidenten.

d) Den finansiella entiteten kommer att eller kommer sannolikt att förlora kunder eller finansiella motparter med en väsentlig inverkan på dess verksamhet till följd av incidenten.

([9]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Vid bedömningen av incidentens påverkan på anseendet ska finansiella entiteter ta hänsyn till den grad av synlighet som incidenten har fått eller sannolikt kommer att få i förhållande till varje kriterium som förtecknas i punkt 1.

Artikel 3

Varaktighet och driftstopp

1. Finansiella entiteter ska mäta varaktigheten av en incident enligt artikel 18.1 b i förordning (EU) 2022/2554, från den tidpunkt då incidenten inträffar till den tidpunkt då den är löst.

Om finansiella entiteter inte kan fastställa tidpunkten för incidenten ska de mäta incidentens varaktighet från det att den upptäcktes. Om finansiella entiteter blir medvetna om att incidenten inträffade innan den upptäcktes, ska de mäta varaktigheten från den tidpunkt då incidenten registreras i nät- eller systemloggar eller andra datakällor.

Om finansiella entiteter ännu inte vet när incidenten kommer att lösas eller inte kan verifiera poster i loggar eller andra datakällor ska de göra skattningar.

2. Finansiella entiteter ska mäta driftstoppet för en incident som avses i artikel 18.1 b i förordning (EU) 2022/2554, från det ögonblick då tjänsten är helt eller delvis otillgänglig för kunder, finansiella motparter eller andra interna eller externa användare till det ögonblick då den ordinarie verksamheten eller driften har återställts till den tjänstenivå som tillhandahölls före incidenten. Om driftstoppet orsakar en försening i tillhandahållandet av tjänsten efter att reguljär verksamhet har återställts, ska driftstoppet mätas från incidentens början till den tidpunkt då den försenade tjänsten tillhandahålls fullt ut.

Om finansiella entiteter inte kan fastställa tidpunkten för driftstoppet ska de mäta driftstoppet från det att det upptäcktes.

Artikel 4

Geografisk spridning

I syfte att fastställa den geografiska spridningen med avseende på de områden som påverkas av incidenten enligt artikel 18.1 c i förordning (EU) 2022/2554 ska finansiella entiteter bedöma huruvida incidenten har eller hade en inverkan i andra medlemsstater, och i synnerhet betydelsen av inverkan i förhållande till något av följande:

a) Kunder och finansiella motparter i andra medlemsstater.

b) Filialer eller andra finansiella entiteter inom koncernen som bedriver verksamhet i andra medlemsstater.

c) Finansmarknadsinfrastrukturer eller tredjepartsleverantörer, som kan påverka finansiella entiteter i andra medlemsstater till vilka de tillhandahåller tjänster, i den mån sådan information finns tillgänglig.

Artikel 5

Dataförluster

I syfte att fastställa de dataförluster som incidenten medför enligt artikel 18.1 d i förordning (EU) 2022/2554 ska finansiella entiteter ta hänsyn till följande:

a) När det gäller tillgången till uppgifter, huruvida incidenten har gjort de uppgifter som efterfrågas av den finansiella entiteten, dess kunder eller dess motparter tillfälligt eller permanent otillgängliga eller oanvändbara.

b) När det gäller uppgifternas äkthet, huruvida incidenten har äventyrat uppgifternas tillförlitlighet.

c) När det gäller uppgifternas integritet, huruvida incidenten har lett till en icke-auktoriserad ändring av uppgifter som har gjort dem felaktiga eller ofullständiga.

d) När det gäller uppgifternas konfidentialitet, huruvida incidenten har lett till att uppgifter har kommits åt av eller lämnats ut till en obehörig part eller ett obehörigt system.

Artikel 6

De berörda tjänsternas kritikalitet

För att fastställa de berörda tjänsternas kritikalitet enligt artikel 18.1 e i förordning (EU) 2022/2554 ska finansiella entiteter bedöma huruvida incidenten

a) påverkar eller har påverkat IKT-relaterade tjänster eller nätverks- och informationssystem som stöder kritiska eller viktiga funktioner hos den finansiella entiteten,

b) påverkar eller har påverkat finansiella tjänster som tillhandahålls av den finansiella entiteten och som kräver tillstånd eller registrering eller som står under tillsyn av behöriga myndigheter,

c) utgör eller har utgjort en framgångsrik, skadlig och obehörig åtkomst till den finansiella entitetens nätverks- och informationssystem.

Artikel 7

Ekonomiska effekter

1. För att fastställa de ekonomiska effekterna av incidenten enligt artikel 18.1 f i förordning (EU) 2022/2554 ska finansiella entiteter, utan att redovisa finansiella återvinningar, beakta följande typer av direkta och indirekta kostnader och förluster som de har ådragit sig till följd av incidenten:

a) Exproprierade medel eller finansiella tillgångar som de är ansvariga för, inbegripet tillgångar som förlorats genom stöld.

b) Kostnader för utbyte eller omlokalisering av programvara, maskinvara eller infrastruktur.

c) Personalkostnader, inklusive kostnader i samband med ersättning eller omplacering av personal, rekrytering av extra personal, ersättning för övertid och återställande av förlorad eller försämrad kompetens.

d) Avgifter på grund av att avtalsförpliktelserna inte har fullgjorts.

e) Kostnader för gottgörelse och ersättning till kunder.

f) Förluster på grund av uteblivna intäkter.

g) Kostnader för intern och extern kommunikation.

h) Rådgivningskostnader, inklusive kostnader i samband med juridisk rådgivning, kriminaltekniska tjänster och saneringstjänster.

2. De kostnader och förluster som avses i punkt 1 ska inte omfatta kostnader som är nödvändiga för den dagliga driften av verksamheten, särskilt följande:

a) Kostnader för allmänt underhåll av infrastruktur, utrustning, hårdvara och programvara samt kostnader för att hålla personalens kompetens uppdaterad.

b) Interna eller externa kostnader för att förbättra verksamheten efter incidenten, inklusive uppgraderingar, förbättringar och riskbedömningsinitiativ.

c) Försäkringspremier.

3. Finansiella entiteter ska beräkna kostnads- och förlustbeloppen på grundval av uppgifter som är tillgängliga vid tidpunkten för rapporteringen. Om de faktiska kostnaderna och förlusterna inte kan fastställas ska de finansiella entiteterna uppskatta dessa belopp.

4. Vid bedömningen av de ekonomiska konsekvenserna av incidenten ska de finansiella entiteterna summera de kostnader och förluster som avses i punkt 1.

KAPITEL II

ALLVARLIGA INCIDENTER OCH VÄSENTLIGHETSTRÖSKLAR

Artikel 8

Allvarliga incidenter

1. En incident ska betraktas som en allvarlig incident enligt artikel 19.1 i förordning (EU) 2022/2554 om den har påverkat kritiska tjänster enligt artikel 6 och om något av följande villkor är uppfyllt:

a) Väsentlighetströskeln enligt artikel 9.5 b har uppfyllts.

b) Två eller flera av de andra väsentlighetströsklar som avses i artikel 9.1–9.6 är uppfyllda.

2. Återkommande incidenter som var för sig inte betraktas som en allvarlig incident i enlighet med punkt 1 ska betraktas som en allvarlig incident om de uppfyller samtliga följande villkor:

a) De har uppstått minst två gånger inom sex månader.

b) De har samma uppenbara grundorsak enligt artikel 20 första stycket b i förordning (EU) 2022/2554.

c) De uppfyller tillsammans kriterierna för att betraktas som en allvarlig incident enligt punkt 1.

Finansiella entiteter ska varje månad bedöma förekomsten av återkommande incidenter.

Denna punkt är inte tillämplig på mikroföretag och finansiella entiteter som förtecknas i artikel 16.1 i förordning (EU) 2022/2554.

Artikel 9

Väsentlighetströsklar för att fastställa allvarliga incidenter

1. Väsentlighetströskeln för kriteriet *kunder, finansiella motparter och transaktioner* är uppfylld om något av följande villkor är uppfyllt:

a) Antalet kunder som påverkas är högre än 10 % av alla kunder som använder den berörda tjänsten.

b) Antalet kunder som påverkas som använder den berörda tjänsten är högre än 100 000.

c) Antalet finansiella motparter som påverkas är högre än 30 % av alla finansiella motparter som bedriver verksamhet i samband med tillhandahållandet av den berörda tjänsten.

d) Antalet transaktioner som påverkas är högre än 10 % av det dagliga genomsnittliga antal transaktioner som utförs av den finansiella entiteten i samband med den berörda tjänsten.

e) Antalet berörda transaktioner överstiger 10 % av det dagliga genomsnittsvärdet av de transaktioner som utförs av den finansiella entiteten i samband med den berörda tjänsten.

f) Kunder eller finansiella motparter som har identifierats som relevanta i enlighet med artikel 1.3 har påverkats.

Om det faktiska antalet kunder eller finansiella motparter som påverkas eller det faktiska antalet eller den faktiska mängden transaktioner som påverkas inte kan fastställas, ska den finansiella entiteten uppskatta dessa på grundval av tillgängliga uppgifter från jämförbara referensperioder.

2. Väsentlighetströskeln för kriteriet *påverkan på anseendet* är uppfylld om något av villkoren i artikel 2.1 a–d är uppfyllt.

3. Väsentlighetströskeln för kriteriet *varaktighet och driftstopp* är uppfylld om något av följande villkor är uppfyllt:

a) Incidentens varaktighet är längre än 24 timmar.

b) Tiden för driftstoppet är längre än 2 timmar för IKT-tjänster som stöder kritiska eller viktiga funktioner.

4. Väsentlighetströskeln för kriteriet *geografisk spridning* är uppfylld om incidenten har en inverkan i två eller flera medlemsstater i enlighet med artikel 4.

5. Väsentlighetströskeln för kriteriet *dataförluster* är uppfylld om något av följande villkor är uppfyllt:

a) Varje inverkan som avses i artikel 5 på uppgifternas tillgänglighet, äkthet, integritet eller konfidentialitet har eller kommer att ha en negativ inverkan på genomförandet av den finansiella entitetens affärsmål eller dess förmåga att uppfylla lagstadgade krav.

b) All framgångsrik, skadlig och obehörig åtkomst som inte omfattas av led a till nätverks- och informationssystem, där sådan åtkomst kan leda till dataförluster.

6. Väsentlighetströskeln för kriteriet *ekonomiska effekter* är uppfylld om den finansiella entitetens kostnader och förluster på grund av incidenten har överstigit eller sannolikt kommer att överstiga 100 000 euro.

KAPITEL III

BETYDANDE CYBERHOT

Artikel 10

Höga väsentlighetströsklar för att fastställa betydande cyberhot

Vid tillämpningen av artikel 18.2 i förordning (EU) 2022/2554 ska ett cyberhot anses vara betydande om samtliga följande villkor är uppfyllda:

a) Cyberhotet, om det materialiseras, kan påverka eller kan ha påverkat kritiska eller viktiga funktioner hos den finansiella entiteten, eller kan påverka andra finansiella entiteter, tredjepartsleverantörer, kunder eller finansiella motparter, baserat på information som är tillgänglig för den finansiella entiteten;

b) Cyberhotet har en hög sannolikhet att materialiseras hos den finansiella entiteten eller hos andra finansiella entiteter, med beaktande av åtminstone följande faktorer:

   i) Tillämpliga risker i samband med det cyberhot som avses i led a, inbegripet potentiella sårbarheter i den finansiella entitetens system som kan utnyttjas;

   ii) Hotaktörernas kapacitet och avsikter i den utsträckning som den finansiella entiteten känner till dem.

   iii) Hotets varaktighet och all samlad kunskap om incidenter som har påverkat den finansiella entiteten eller dess tredjepartsleverantör, kunder eller finansiella motparter.

c) Cyberhotet kan, om det materialiseras, uppfylla något av följande:

   i) Kriteriet avseende tjänsternas kritikalitet enligt artikel 18.1 e i förordning (EU) 2022/2554, i enlighet med artikel 6 i den här förordningen.

   ii) Väsentlighetströskeln enligt artikel 9.1.

   iii) Väsentlighetströskeln enligt artikel 9.4.

Om den finansiella entiteten, beroende på typen av cyberhot och tillgänglig information, drar slutsatsen att de väsentlighetströsklar som anges i artikel 9.2, 9.3, 9.5 och 9.6 skulle kunna uppfyllas, får dessa trösklar också beaktas.

KAPITEL IV

ALLVARLIGA INCIDENTERS RELEVANS FÖR BEHÖRIGA MYNDIGHETER I ANDRA MEDLEMSSTATER OCH UPPGIFTER OM RAPPORTER SOM SKA DELAS MED ANDRA BEHÖRIGA MYNDIGHETER

Artikel 11

Allvarliga incidenters relevans för behöriga myndigheter i andra medlemsstater

Bedömningen av huruvida den allvarliga incidenten är relevant för behöriga myndigheter i andra medlemsstater enligt artikel 19.7 i förordning (EU) 2022/2554 ska baseras på huruvida incidenten har en grundorsak som har sitt ursprung i en annan medlemsstat eller om den har eller har haft en betydande inverkan i en annan medlemsstat i förhållande till något av följande:

a) Kunder eller finansiella motparter.

b) En filial till den finansiella entiteten eller en annan finansiell entitet inom koncernen.

c) En finansmarknadsinfrastruktur eller en tredjepartsleverantör som kan påverka finansiella entiteter som de tillhandahåller tjänster till.

Artikel 12

Uppgifter om allvarliga incidenter som ska delas med andra behöriga myndigheter

De uppgifter om allvarliga incidenter som behöriga myndigheter ska lämna till andra behöriga myndigheter i enlighet med artikel 19.6 i förordning (EU) 2022/2554 och de underrättelser som EBA, Esma eller Eiopa och ECB ska lämna till de relevanta behöriga myndigheterna i andra medlemsstater i enlighet med artikel 19.7 i den förordningen ska innehålla samma informationsnivå, utan någon anonymisering, som de underrättelser och rapporter om allvarliga incidenter som erhålls från finansiella entiteter i enlighet med artikel 19.4 i förordning (EU) 2022/2554.

KAPITEL V

SLUTBESTÄMMELSER

Artikel 13

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 13 mars 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande