EUROPEISKA
KOMMISSIONEN

Bryssel den 17.10.2024
C(2024) 7151 final

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) …/…

av den 17.10.2024

om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster

(Text av betydelse för EES)

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) …/…

av den 17.10.2024

om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster

(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 direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)[1], särskilt artiklarna 21.5 första stycket och 23.11 andra stycket, och

av följande skäl:

(1) När det gäller leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster. leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster som omfattas av artikel 3 i direktiv (EU) 2022/2555 (*berörda entiteter*) syftar denna förordning till att fastställa tekniska och metodologiska specifikationer för de åtgärder som avses i artikel 21.2 i direktiv (EU) 2022/2555 och närmare ange i vilka fall en incident ska anses vara betydande enligt artikel 23.3 i direktiv (EU) 2022/2555.

(2) Mot bakgrund av att tillhandahållare av betrodda tjänster bedriver tjänster av gränsöverskridande art, och för att säkerställa en enhetlig ram för tillhandahållare av betrodda tjänster, bör denna förordning med avseende på tillhandahållare av betrodda tjänster närmare ange i vilka fall en incident ska anses vara betydande, utöver att fastställa de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet.

(3) I enlighet med artikel 21.5 tredje stycket i direktiv (EU) 2022/2555 baseras de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet i

[1] EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

bilagan till denna förordning på europeiska och internationella standarder, såsom ISO/IEC 27001, ISO/IEC 27002 och ETSI EN 319 401, och tekniska specifikationer, såsom CEN/TS 18026:2024, som är relevanta för säkerheten i nätverks- och informationssystem.

(4) När det gäller genomförandet och tillämpningen av de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet enligt bilagan till denna förordning bör, i enlighet med proportionalitetsprincipen, vederbörlig hänsyn tas till skillnaderna i riskexponering för de berörda entiteterna, exempelvis den berörda entitetens kritikalitet, vilka risker den exponeras för, den berörda entitetens storlek och struktur samt sannolikheten för att incidenter ska inträffa och incidenternas allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser, vid uppfyllandet av de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet enligt bilagan till denna förordning.

(5) Om berörda entiteter på grund av sin storlek inte kan genomföra vissa av de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet, bör dessa entiteter i enlighet med proportionalitetsprincipen kunna vidta andra kompenserande åtgärder som är lämpliga för att uppnå dessa specifikationers syften. Vid fastställandet av roller, ansvarsområden och befogenheter för säkerheten i nätverks- och informationssystem inom den berörda entiteten kan exempelvis entiteter av mikrostorlek anse det svårt att separera arbetsuppgifter och ansvarsområden som står i strid med varandra. Sådana entiteter bör kunna överväga kompenserande åtgärder, såsom riktad tillsyn av entitetens ledning eller utökad övervakning och loggning.

(6) Vissa tekniska och metodologiska specifikationer som anges i bilagan till denna förordning bör tillämpas av de berörda entiteterna när så är lämpligt, om tillämpligt, eller i den mån det är genomförbart. Om en berörd entitet inte anser att det är lämpligt, tillämpligt eller genomförbart för den berörda entiteten att tillämpa vissa tekniska och metodologiska specifikationer enligt bilagan till denna förordning bör den berörda entiteten på ett begripligt sätt dokumentera sina skäl. Nationella behöriga myndigheter får, när de utövar sin tillsyn, beakta den tid som behövs för att de berörda entiteterna ska kunna genomföra de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet.

(7) Enisa eller de nationella behöriga myndigheterna enligt direktiv (EU) 2022/2555 kan ge vägledning för att stödja berörda entiteter vid identifieringen, analysen och bedömningen av risker i samband med genomförandet av de tekniska och metodologiska specifikationer som rör fastställandet och upprätthållandet av en ändamålsenlig riskhanteringsram. Denna vägledning kan exempelvis inbegripa nationella och sektorsvisa riskbedömningar samt riskbedömningar som är specifika för en viss typ av entitet. Vägledningen kan också inbegripa verktyg eller mallar för utvecklingen av riskhanteringsramar på de berörda entiteternas nivå. De berörda entiteterna kan också stödja sig på ramar, vägledningar eller andra mekanismer som föreskrivs i medlemsstaternas nationella lagstiftning och på europeiska och internationella standarder för att visa att de efterlever denna förordning. Enisa eller de nationella behöriga myndigheterna enligt direktiv (EU) 2022/2555 kan också stödja berörda entiteter vid identifieringen och genomförandet av ändamålsenliga lösningar för att hantera risker som identifieras i sådana riskbedömningar. Sådan vägledning bör inte påverka de berörda entiteternas skyldighet att identifiera och dokumentera riskerna för säkerheten i nätverks- och informationssystem eller de berörda entiteternas skyldighet att genomföra de tekniska och metodologiska specifikationer

för riskhanteringsåtgärder för cybersäkerhet som fastställs i bilagan till denna förordning, i enlighet med sina behov och resurser.

(8) Nätverkssäkerhetsåtgärder som avser i) övergång till den senaste generationen kommunikationsprotokoll i nätverksskiktet, ii) ibruktagande av internationellt överenskomna och interoperabla moderna standarder för e-postkommunikation, och iii) användning av bästa praxis för DNS-säkerhet samt för dirigeringssäkerhet och dirigeringshygien medför särskilda utmaningar när det gäller att identifiera bästa tillgängliga standarder och ibruktagningsmetoder. För att så snart som möjligt uppnå en hög gemensam nivå av cybersäkerhet i alla nätverk bör kommissionen, med stöd av Europeiska unionens cybersäkerhetsbyrå (Enisa) och i samarbete med behöriga myndigheter, näringslivet – däribland telekommunikationsbranschen – och andra berörda parter, stödja utvecklingen av ett flerpartsforum med uppgift att identifiera dessa bästa tillgängliga standarder och ibruktagningsmetoder. Denna flerpartsvägledning bör inte påverka de berörda entiteternas skyldighet att uppfylla de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet som fastställs i bilagan till denna förordning.

(9) I enlighet med artikel 21.2 a i direktiv (EU) 2022/2555 bör väsentliga och viktiga entiteter utöver sina strategier för riskanalys ha strategier för informationssystemens säkerhet, För detta ändamål bör de berörda entiteterna fastställa en strategi för säkerhet i nätverks- och informationssystem samt ämnesspecifika strategier, såsom strategier för åtkomstkontroll, som bör vara förenliga med strategin för säkerhet i nätverks- och informationssystem. Strategin för säkerhet i nätverks- och informationssystem bör vara det dokument på högsta nivå som fastställer de berörda entiteternas allmänna sätt att hantera sin säkerhet i nätverks- och informationssystem, och den bör godkännas av de berörda entiteternas ledningsorgan. De ämnesspecifika strategierna bör godkännas på lämplig ledningsnivå. Strategierna bör omfatta indikatorer och åtgärder för övervakning av genomförandet och den aktuella mognadsnivån när det gäller nätverks- och informationssäkerhet hos de berörda entiteterna, i synnerhet för att underlätta ledningsorganens tillsyn över genomförandet av riskhanteringsåtgärderna för cybersäkerhet.

(10) När det gäller de tekniska och metodologiska specifikationer som fastställs i bilagan till denna förordning bör begreppet *användare* omfatta alla juridiska och fysiska personer med åtkomst till entitetens nätverks- och informationssystem.

(11) För att identifiera och åtgärda risker för säkerheten i nätverks- och informationssystem bör de berörda entiteterna fastställa och upprätthålla en ändamålsenlig riskhanteringsram. Som ett led i riskhanteringsramen bör de berörda entiteterna fastställa, genomföra och övervaka en riskhanteringsplan. De berörda entiteterna får använda riskhanteringsplanen för att identifiera och prioritera riskhanteringsalternativ och riskhanteringsåtgärder. Alternativen för riskhantering handlar i synnerhet om att undvika, minska eller, i exceptionella fall, godta en risk. Valet av riskhanteringsalternativ bör beakta resultaten från den riskbedömning som utförts av den berörda entiteten och bör vara i enlighet med den berörda entitetens strategi för säkerhet i nätverks- och informationssystem. För att ge verkan åt de valda riskhanteringsalternativen bör de berörda entiteterna vidta lämpliga riskhanteringsåtgärder.

(12) För att upptäcka händelser, tillbud och incidenter bör de berörda entiteterna övervaka sina nätverks- och informationssystem och vidta åtgärder för att utvärdera händelser, tillbud och incidenter. Dessa åtgärder bör kunna möjliggöra snabb upptäckt av

nätbaserade attacker baserat på avvikande mönster för ingående eller utgående trafik och överbelastningsattacker.

(13) Om de berörda entiteterna gör en konsekvensanalys uppmanas de utföra en omfattande analys för att fastställa, såsom lämpligt, maximal acceptabel tid för driftstopp samt mål i fråga om återställningstid, återställningspunkt och tjänsteleverans.

(14) För att minska riskerna kopplade till en berörd entitets leveranskedja och dess förhållande till sina leverantörer bör de berörda entiteterna fastställa en säkerhetsstrategi för leveranskedjan som styr deras förbindelser med sina direkta leverantörer och tjänsteleverantörer. Dessa entiteter bör i avtalen med sina direkta leverantörer eller tjänsteleverantörer specificera adekvata säkerhetsklausuler, t.ex. genom att när så är lämpligt kräva riskhanteringsåtgärder för cybersäkerhet i enlighet med artikel 21.2 i direktiv (EU) 2022/2555 eller andra liknande rättsliga krav.

(15) De berörda entiteterna bör regelbundet utföra säkerhetstester baserade på en särskild strategi och förfaranden för att kontrollera om riskhanteringsåtgärderna för cybersäkerhet genomförs och fungerar korrekt. Säkerhetstester får utföras på enskilda nätverks- och informationssystem eller på den berörda entiteten som helhet och får innefatta automatiserade eller manuella tester, penetrationstester, sårbarhetsskanning, statiska och dynamiska applikationssäkerhetstester, konfigurationstester eller säkerhetsrevision. De berörda entiteterna får utföra säkerhetstester på sina nätverks- och informationssystem i samband med installationen, efter uppgraderingar eller modifieringar av infrastruktur eller applikationer som de anser vara betydande eller efter underhåll. Iakttagelserna från säkerhetstesterna bör ligga till grund för de berörda entiteternas strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärder för cybersäkerhet, tillsammans med oberoende granskningar av deras strategier för nätverks- och informationssäkerhet.

(16) För att undvika betydande störningar och skada till följd av utnyttjandet av oåtgärdade sårbarheter i nätverks- och informationssystem bör de berörda entiteterna fastställa och tillämpa ändamålsenliga förfaranden för programfixhantering som är anpassade till de berörda entiteternas förändringshanterings-, sårbarhetshanterings- och riskhanteringsförfaranden och andra relevanta förfaranden. Berörda entiteter bör vidta åtgärder som står i proportion till deras resurser för att säkerställa att programfixar inte inför ytterligare sårbarheter eller instabiliteter. Vid planerad otillgänglighet till tjänsten till följd av tillämpningen av programfixar uppmuntras de berörda entiteterna att vederbörligen informera kunderna i förväg.

(17) De berörda entiteterna bör hantera risker till följd av förvärv av IKT-produkter eller IKT-tjänster från leverantörer eller tjänsteleverantörer och bör se till att de får garantier för att de IKT-produkter eller IKT-tjänster som förvärvas uppnår en viss cybersäkerhetsskyddsnivå, t.ex. genom europeiska cybersäkerhetscertifikat och EU-försäkran om överensstämmelse för IKT-produkter eller IKT-tjänster som utfärdats inom ramen för ett europeiskt certifieringssystem för cybersäkerhet som antagits i enlighet med artikel 49 i Europaparlamentets och rådets förordning (EU) 2019/881[2]. Om de berörda entiteterna fastställer säkerhetskrav för de IKT-produkter som förvärvas bör de ta hänsyn till de väsentliga cybersäkerhetskrav som fastställs i

[2] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

Europaparlamentets och rådets förordning som fastställer övergripande cybersäkerhetskrav för produkter med digitala element.

(18) För att skydda sig mot cyberhot och stödja förebyggande och begränsning av dataintrång bör de berörda entiteterna genomföra nätsäkerhetslösningar. Exempel på typiska nätsäkerhetslösningar är användning av brandväggar för att skydda de berörda entiteternas interna nätverk, säkerställande av att anslutningarna och åtkomsten begränsas till tjänster för vilka anslutningar och åtkomst är absolut nödvändiga, samt användning av virtuella privata nätverk för fjärråtkomst och tillåta att tjänsteleverantörer ansluter sig först efter en begäran om behörighet och endast för en begränsad tidsperiod, såsom under den tid som ett underhållsarbete pågår.

(19) För att skydda de berörda entiteternas nätverk och informationssystem mot sabotageprogram och otillåten programvara bör dessa entiteter införa kontroller för att förhindra eller upptäcka användning av otillåten programvara och bör, när så är lämpligt, använda programvara för upptäckt och åtgärdande. De berörda entiteterna bör också överväga att vidta åtgärder för att minimera attackytan, minska de sårbarheter som kan utnyttjas av angripare, kontrollera körandet av applikationer på slutanvändarenheter samt använda filter för e-post och webbapplikationer för att minska exponeringen för skadligt innehåll.

(20) I enlighet med artikel 21.2 g i direktiv (EU) 2022/2555 bör medlemsstaterna säkerställa att väsentliga och viktiga entiteter säkerställer grundläggande praxis för cyberhygien och cybersäkerhetsutbildning. Grundläggande praxis för cyberhygien kan inbegripa nolltillitsprinciper, programuppdateringar, enhetskonfiguration, nätverkssegmentering, identitets- och åtkomsthantering eller användarmedvetenhet, anordnande av personalutbildning och åtgärder för att öka medvetenheten om cyberhot, nätfiske eller metoder för social manipulering. Cyberhygienpraxis ingår i olika tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet som anges i bilagan till denna förordning. När det gäller grundläggande praxis för cyberhygien för användare bör de berörda entiteterna överväga sådan praxis som en policy för tom bildskärm och renstädat skrivbord, användning av flerfaktorsautentisering eller andra autentiseringsmetoder, säker e-postanvändning och webbsökning, skydd mot nätfiske och social manipulering samt säkra rutiner för distansarbete.

(21) För att förhindra obehörig åtkomst till de berörda entiteternas tillgångar bör de berörda entiteterna fastställa och genomföra en ämnesspecifik strategi för att hantera åtkomsten för personer och för nätverks- och informationssystem, t.ex. applikationer.

(22) För att motverka att arbetstagarna missbrukar exempelvis åtkomsträttigheter hos den berörda entiteten för skadliga ändamål bör berörda entiteter överväga ändamålsenliga åtgärder för hantering av personalsäkerhet och öka personalens medvetenhet om sådana risker. De berörda entiteterna bör inrätta, kommunicera och upprätthålla ett disciplinärt förfarande för att hantera överträdelser av den berörda entitetens säkerhetsstrategier för nätverks- och informationssystem, vilket kan vara en del av andra disciplinära förfaranden som inrättats av de berörda entiteterna. Kontroll av bakgrunden för de berörda entiteternas anställda och om tillämpligt för deras direkta leverantörer och tjänsteleverantörer bör bidra till målet om personalsäkerhet hos de berörda entiteterna och kan innefatta sådana åtgärder som kontroll av den berörda personen i belastningsregistret eller av personens tidigare yrkesutövning, såsom lämpligt med tanke på personens uppgifter hos den berörda entiteten och i enlighet med den berörda entitetens strategi för säkerhet i nätverks- och informationssystem.

(23) Flerfaktorsautentisering kan förbättra entiteternas cybersäkerhet och bör övervägas av entiteterna i synnerhet när användarna har åtkomst till nätverks- och informationssystem på distans eller när de har åtkomst till känslig information eller konton med särskild behörighet och systemadministrationskonton. Flerfaktorsautentisering kan kombineras med andra metoder för att kräva ytterligare faktorer under särskilda omständigheter, baserat på fördefinierade regler och mönster, såsom åtkomst från en ovanlig plats, från en ovanlig enhet eller vid en ovanlig tidpunkt.

(24) De berörda entiteterna bör förvalta och skydda de tillgångar som är av värde för dem genom en robust tillgångshantering, som också bör ligga till grund för riskanalysen och kontinuitetshanteringen. De berörda entiteterna bör förvalta både materiella och immateriella tillgångar och bör upprätta en tillgångsinventering, fastställa en definierad klassificeringsnivå för tillgångarna, hantera och spåra tillgångarna samt vidta åtgärder för att skydda tillgångarna under hela deras livscykel.

(25) Förvaltningen av tillgångar bör inbegripa att tillgångarna klassificeras efter typ, känslighet, risknivå och säkerhetskrav samt att ändamålsenliga åtgärder och kontroller används för att säkerställa deras tillgänglighet, integritet, konfidentialitet och autenticitet. Genom att klassificera tillgångarna efter risknivå bör de berörda entiteterna kunna tillämpa ändamålsenliga säkerhetsåtgärder och kontroller för att skydda tillgångarna, t.ex. kryptering, åtkomstkontroll inklusive perimeterkontroll och kontroll av fysiskt och logiskt tillträde, säkerhetskopiering, loggning och övervakning, lagring och radering. När de berörda entiteterna genomför en konsekvensanalys kan de fastställa klassificeringsnivån baserat på hur en entitet påverkas av ett avbrott i tillgångarna. Alla entiteternas anställda som hanterar tillgångar bör känna till strategierna och anvisningarna för hantering av tillgångar.

(26) Detaljnivån för inventeringen av tillgångar bör vara anpassad till de berörda entiteternas behov. En omfattande inventering av tillgångar kan exempelvis, för varje tillgång, inkludera åtminstone en unik identitetsbeteckning, tillgångens ägare, en beskrivning av tillgången, tillgångens lokalisering, typen av tillgång, typ och klassificering för information som behandlas i tillgången, dagen för tillgångens senaste uppdatering eller programfix, tillgångens riskbedömningsklassificering och slutet av livscykeln för tillgången. När ägaren till en tillgång identifieras bör de berörda entiteterna också identifiera den person som har ansvaret för att skydda denna tillgång.

(27) Tilldelningen och organisationen av cybersäkerhetsroller, ansvarsområden och behörigheter bör innebära att en konsekvent struktur inrättas för styrningen och genomförandet av cybersäkerhet inom de berörda entiteterna, vilket bör säkerställa effektiv kommunikation vid incidenter. När ansvaret för vissa roller fastställs och anförtros bör de berörda entiteterna överväga sådana roller som informationssäkerhetschef, informationssäkerhetsansvarig, incidenthanterare och revisor, eller motsvarande. Berörda entiteter får anförtro externa parter, såsom tredjepartsleverantörer av IKT-tjänster, roller och ansvarsområden.

(28) I enlighet med artikel 21.2 i direktiv (EU) 2022/2555 bör riskhanteringsåtgärder för cybersäkerhet baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot sådana händelser som stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysiskt tillträde till och skada eller störning på en väsentlig eller viktig entitets information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller

behandlade data eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. De tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet bör därför också omfatta nätverks- och informationssystemens fysiska och miljömässiga säkerhet genom att inbegripa åtgärder för att skydda sådana system från systemfel, mänskliga fel, skadliga handlingar eller naturfenomen. Andra exempel på fysiska och miljömässiga hot kan vara jordbävningar, explosioner, sabotage, insiderhot, oroligheter i samhället, toxiskt avfall och miljöutsläpp. Åtgärder för att förhindra förlust eller skador eller förhindra att nätverks- och informationssystem komprometteras eller driften avbryts på grund av fel och avbrott i försörjningstjänster bör bidra till driftskontinuiteten hos de berörda entiteterna. Skydd mot fysiska och miljömässiga hot bör också bidra till säkerheten vid underhåll av nätverks- och informationssystem i de berörda entiteterna.

(29) Berörda entiteter bör utforma och genomföra skyddsåtgärder mot fysiska och miljömässiga hot och fastställa de lägsta och högsta kontrolltrösklarna för fysiska och miljömässiga hot och övervaka miljöparametrar. Exempelvis bör de överväga att installera system för att i ett tidigt stadium upptäcka översvämningar i områden där nätverks- och informationssystem är lokaliserade. När det gäller brandrisk bör de berörda entiteterna överväga att inrätta en separat brandcell för datacentralen och att använda brandsäkra material, använda sensorer för att övervaka temperatur och fuktighet, ansluta byggnaden till ett brandlarmsystem som automatiskt underrättar den lokala brandkåren samt ha system för tidig upptäckt och släckning av bränder. De berörda entiteterna bör också genomföra regelbundna brandövningar och brandinspektioner. För att säkerställa elförsörjningen bör de berörda entiteterna överväga överspänningsskydd och motsvarande nödkraftförsörjning, i enlighet med relevanta standarder. Eftersom överhettning utgör en risk för tillgången till nätverks- och informationssystem kan berörda entiteter, i synnerhet leverantörer av datacentraltjänster, överväga adekvata, kontinuerliga och redundanta luftkonditioneringssystem.

(30) I denna förordning anges närmare de fall då en incident bör anses som betydande vid tillämpningen av artikel 23.3 i direktiv (EU) 2022/2555. Kriterierna bör vara sådana att berörda entiteter kan bedöma om en incident är betydande, för att anmäla incidenten i enlighet med direktiv (EU) 2022/2555. De kriterier som fastställs i denna förordning bör vidare anses som uttömmande, utan att det påverkar tillämpningen av artikel 5 i direktiv (EU) 2022/2555. I denna förordning specificeras i vilka fall som en incident bör anses som betydande, genom fastställandet av både övergripande och entitetsspecifika fall.

(31) I enlighet med artikel 23.4 i direktiv (EU) 2022/2555 bör de berörda entiteterna vara skyldiga att anmäla betydande incidenter inom de tidsfrister som fastställs i den bestämmelsen. Dessa tidsfrister börjar löpa vid den tidpunkt då entiteten får kännedom om sådana betydande incidenter. Den berörda entiteten är därför skyldig att rapportera incidenter som, baserat på dess inledande bedömning, skulle kunna orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. När en berörd entitet har upptäckt en misstänkt händelse, eller efter att den har uppmärksammats på en potentiell incident av en tredje part, såsom en individ, en kund, en entitet, en myndighet, en medieorganisation eller en annan källa, bör den berörda entiteten därför i rätt tid bedöma den misstänkta händelsen för att fastställa om den utgör en incident och om så är fallet fastställa dess art och allvarlighetsgrad. Den berörda entiteten anses därför ha fått ”kännedom” om den

betydande incidenten när den, efter en sådan inledande bedömning, med en rimlig grad av säkerhet har fastställt att en betydande incident har ägt rum.

(32) För att fastställa om en incident är betydande bör de berörda entiteterna, när så är relevant, räkna antalet användare som påverkas av incidenten, med beaktande av företagskunder och slutkunder med vilka de berörda entiteterna har ett avtalsförhållande samt fysiska och juridiska personer som är kopplade till företagskunder. Om en berörd entitet inte kan beräkna antalet användare som påverkas bör den berörda entitetens uppskattning av det möjliga högsta antalet påverkade användare beaktas för beräkningen av det totala antal användare som påverkas av incidenten. Betydelsen av en incident som involverar en betrodd tjänst bör inte bara fastställas baserat på antalet användare utan även på antalet förlitande parter, eftersom dessa kan påverkas lika mycket av en betydande incident som involverar en betrodd tjänst när det gäller driftsstörning och materiell eller immateriell skada. Därför bör leverantörer av betrodda tjänster, om tillämpligt, även ta hänsyn till antalet förlitande parter när de fastställer om en incident är betydande. I detta sammanhang bör förlitande parter förstås som fysiska eller juridiska personer som förlitar sig på en betrodd tjänst.

(33) Underhållsarbeten som leder till begränsad tillgänglighet eller otillgänglighet för tjänsten bör inte anses som betydande incidenter om tjänstens begränsade tillgänglighet eller otillgänglighet inträffar i enlighet med en planerad underhållsinsats. Om en tjänst är otillgänglig på grund av planerade avbrott såsom avbrott eller otillgänglighet som baseras på förutbestämda avtalsenliga överenskommelser bör inte heller det anses som en betydande incident.

(34) Varaktigheten för en incident som påverkar tillgången till en tjänst bör mätas från den tidpunkt då det korrekta tillhandahållandet av tjänsten avbryts till tidpunkten för återställningen. Om en berörd entitet inte kan fastställa det ögonblick då störningen inleddes bör incidentens varaktighet mätas från det ögonblick då incidenten upptäcktes eller från det ögonblick då incidenten registrerades i nätverks- eller systemloggar eller andra datakällor, beroende på vilket som inträffar först.

(35) Total otillgänglighet till en tjänst bör mätas från det ögonblick då tjänsten blir helt otillgänglig för användare till det ögonblick då reguljär verksamhet eller drift har återställts till den tjänstenivå som tillhandhölls före incidenten. Om en berörd entitet inte kan fastställa när en tjänsts totala otillgänglighet inleddes bör otillgängligheten mätas från det ögonblick då den upptäcktes av den entiteten.

(36) När det gäller att fastställa de direkta ekonomiska förlusterna till följd av en incident bör berörda entiteter ta hänsyn till alla ekonomiska förluster som incidenten har orsakat för dem, såsom kostnaderna för utbyte eller omlokalisering av programvara, maskinvara eller infrastruktur, personalkostnader – inklusive kostnader i samband med ersättning eller omplacering av personal, rekrytering av extra personal, övertidsersättning och återställande av förlorad eller försämrad kompetens, avgifter på grund av att avtalsförpliktelserna inte har fullgjorts, kostnader för gottgörelse och ersättning till kunder, förluster på grund av uteblivna intäkter, kostnader för intern och extern kommunikation, rådgivningskostnader – inklusive kostnader i samband med juridisk rådgivning, kriminaltekniska tjänster och saneringstjänster – samt andra kostnader kopplade till incidenten. Straffavgifter och kostnader som är nödvändiga för den dagliga verksamheten bör dock inte anses som ekonomiska förluster till följd av en incident, och detta innefattar kostnader för allmänt underhåll av infrastruktur, utrustning, maskinvara och programvara, åtgärder för att hålla personalens kompetens

uppdaterad, interna eller externa kostnader för att förbättra verksamheten efter incidenten, inklusive uppgraderingar, förbättringar och riskbedömningsinitiativ, samt försäkringspremier. De berörda entiteterna bör beräkna de ekonomiska förlustbeloppen på grundval av tillgängliga data, och om de faktiska ekonomiska förlustbeloppen inte kan fastställas bör entiteterna göra en uppskattning.

(37) Berörda entiteter bör också vara skyldiga att rapportera incidenter som har orsakat eller kan orsaka dödsfall för fysiska personer eller betydande skada för fysiska personers hälsa, eftersom sådana incidenter är särskilt allvarliga fall som medför betydande materiell eller immateriell skada. En incident som påverkar en berörd entitet kan exempelvis medföra att hälso- och sjukvårdstjänster eller räddningstjänster inte är tillgängliga, eller orsaka konfidentialitets- eller integritetsförlust för data med konsekvenser för fysiska personers hälsa. Vid fastställandet av om en incident har orsakat eller kan orsaka betydande skada för en fysisk persons hälsa bör de berörda entiteterna ta hänsyn till om incidenten orsakat eller kan orsaka allvarliga fysiska skador och ohälsa. I detta sammanhang bör de berörda entiteterna inte vara skyldiga att inhämta ytterligare information som de inte har tillgång till.

(38) Begränsad tillgänglighet bör anses förekomma i synnerhet om en tjänst som tillhandahålls av en berörd entitet är betydligt långsammare än den genomsnittliga svarstiden eller om inte alla funktioner hos en tjänst är tillgängliga. När så är möjligt bör objektiva kriterier baserade på den genomsnittliga svarstiden för tjänster som tillhandahålls av de berörda entiteterna användas vid bedömningen av fördröjd svarstid. En tjänsts funktion kan exempelvis vara en chattfunktion eller en bildsökningsfunktion.

(39) En framgångsrik, misstänkt skadlig och obehörig åtkomst till en berörd entitets nätverks- och informationssystem bör anses som en betydande incident om denna åtkomst kan orsaka allvarliga driftsstörningar. Om exempelvis en cyberhotsaktör i förväg positionerar sig i en berörd entitets nätverks- och informationssystem i syfte att orsaka driftsstörningar i framtiden så ska incidenten anses som betydande.

(40) Återkommande incidenter som hänger samman på grund av samma uppenbara grundorsak och som individuellt inte uppfyller kriterierna för en betydande incident bör kollektivt anses som en betydande incident om de kollektivt uppfyller kriteriet för ekonomiska förluster och de har inträffat minst två gånger på sex månader. Sådana återkommande incidenter kan tyda på betydande brister och svagheter i den berörda entitetens riskhanteringsförfaranden för cybersäkerhet och deras cybersäkerhetsmognadsgrad. Sådana återkommande incidenter kan dessutom orsaka den berörda entiteten betydande ekonomiska förluster.

(41) Kommissionen har utbytt råd och samarbetat med samarbetsgruppen och Enisa om utkastet till genomförandeakt, i enlighet med artiklarna 21.5 och 23.11 i direktiv (EU) 2022/2555.

(42) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725[3] och avgav ett yttrande den 1 september 2024.

---

[3] 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).

(43) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats i enlighet med artikel 39 i direktiv (EU) 2022/2555.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Innehåll

När det gäller leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster. leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster (*berörda entiteter*) fastställer denna förordning tekniska och metodologiska specifikationer för de åtgärder som avses i artikel 21.2 i direktiv (EU) 2022/2555 och anger närmare i vilka fall en incident ska anses vara betydande enligt artikel 23.3 i direktiv (EU) 2022/2555.

Artikel 2

Tekniska och metodologiska specifikationer

1. I bilagan till denna förordning fastställs för de berörda entiteterna de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet enligt artikel 21.2 a–j i direktiv (EU) 2022/2555.

2. De berörda entiteterna ska för nätverks- och informationssystem säkerställa en säkerhetsnivå som är lämplig för de risker som finns när de genomför och tillämpar de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet som fastställs i bilagan till denna förordning. De ska därför ta vederbörlig hänsyn till sin riskexponeringsgrad, sin storlek, sannolikheten för att incidenter ska inträffa och incidenternas allvarlighetsgrad, inklusive de samhälleliga och ekonomiska konsekvenserna, när de uppfyller de tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet som fastställs i bilagan till denna förordning.

   Om bilagan till denna förordning föreskriver att en teknisk eller metodologisk specifikation för en riskhanteringsåtgärd för cybersäkerhet ska tillämpas ”när så är lämpligt”, ”om tillämpligt” eller ”i den mån det är genomförbart”, och om en berörd entitet inte anser att det är lämpligt, tillämpligt eller genomförbart för den berörda entiteten att tillämpa vissa tekniska och metodologiska specifikationer, ska den berörda entiteten på ett begripligt sätt dokumentera sina skäl.

Artikel 3

Betydande incidenter

1. När det gäller de berörda entiteterna ska en incident anses som betydande vid tillämpningen av artikel 23.3 i direktiv 2022/2555 om ett eller flera av följande kriterier är uppfyllda:

(a) Incidenten har orsakat eller kan orsaka en ekonomisk förlust för den berörda entiteten som överstiger 500 000 EUR eller 5 % av den berörda entitetens totala årsomsättning under föregående räkenskapsår, beroende på vilket som är lägst.

(b) Incidenten har orsakat eller kan orsaka att företagshemligheter enligt artikel 2.1 i direktiv (EU) 2016/943 exfiltreras från den berörda entiteten.

(c) Incidenten har orsakat eller kan orsaka en fysisk persons dödsfall.

(d) Incidenten har orsakat eller kan orsaka betydande skador på en fysisk persons hälsa.

(e) En framgångsrik, misstänkt skadlig och obehörig åtkomst till nätverks- och informationssystem har inträffat och kan orsaka allvarliga driftsstörningar.

(f) Incidenten uppfyller de kriterier som anges i artikel 4.

(g) Incidenten uppfyller ett eller flera av de kriterier som anges i artiklarna 5–14.

(2) Planerade avbrott av tjänsten och planerade konsekvenser av planerat underhåll som utförs av de berörda entiteterna eller på deras vägnar ska inte anses som betydande incidenter.

(3) När de berörda entiteterna beräknar antalet användare som påverkas av en incident vid tillämpningen av artiklarna 7 och 9–14 ska de beakta samtliga följande aspekter:

(a) Antalet kunder som har ett avtal med den berörda entiteten som ger dem tillgång till den berörda entitetens nätverks- och informationssystem eller tjänster som erbjuds av, eller är tillgängliga via, dessa nätverks- och informationssystem.

(b) Antalet fysiska och juridiska personer kopplade till företagskunder som använder entiteternas nätverks- och informationssystem eller tjänster som erbjuds av, eller är tillgängliga via, dessa nätverks- och informationssystem.

Artikel 4

Återkommande incidenter

Incidenter som var för sig inte anses som en betydande incident i den mening som avses i artikel 3 ska kollektivt anses som en betydande incident om samtliga följande kriterier är uppfyllda:

(a) De har inträffat minst två gånger inom sex månader.

(b) De verkar ha samma grundorsak.

(c) De uppfyller kollektivt kriterierna i artikel 3.1 a.

Artikel 5

Betydande incidenter när det gäller leverantörer av molntjänster

När det gäller leverantörer av DNS-tjänster ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En rekursiv eller auktoritativ tjänst för att lösa domännamnsfrågor är helt otillgänglig i över 30 minuter.

(b) Under en tidsperiod som överstiger en timme är den genomsnittliga svarstiden hos en rekursiv eller auktoritativ tjänst för att lösa domännamnsfrågor över tio sekunder när det gäller en DNS-begäran.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av den auktoritativa tjänsten för att lösa domännamnsfrågor har komprometterats, förutom om uppgifter som rör färre än 1 000 domännamn som förvaltas av leverantören av DNS-tjänster, motsvarande högst 1 % av de domännamn som den leverantören av DNS-tjänster förvaltar, är felaktiga till följd av felkonfigurering.

Artikel 6

Betydande incidenter när det gäller registreringsenheter för toppdomäner

När det gäller registreringsenheter för toppdomäner ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En auktoritativ tjänst för att lösa domännamnsfrågor är helt otillgänglig.

(b) Under en tidsperiod som överstiger en timme är den genomsnittliga svarstiden hos en auktoritativ tjänst för att lösa domännamnsfrågor över tio sekunder när det gäller en DNS-begäran.

(c) integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med den tekniska driften av registreringsenheten för toppdomäner har komprometterats.

Artikel 7

Betydande incidenter när det gäller leverantörer av molntjänster

När det gäller leverantörer av molntjänster ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En molntjänst som tillhandahålls är helt otillgänglig i över 30 minuter.

(b) Tillgången till en leverantörs molntjänst är begränsad för mer än 5 % av molntjänstens användare i unionen, eller för mer än en miljon användare av molntjänsten i unionen, beroende på vilket antal som är lägst, under en period av mer än en timme.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en molntjänst har komprometterats till följd av en misstänkt skadlig handling.

(d) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en molntjänst har komprometterats och det påverkar mer än 5 % av användarna av molntjänsten i unionen, eller mer än en miljon av molntjänstens användare i unionen, beroende på vilket antal som är lägst.

Artikel 8

Betydande incidenter när det gäller leverantörer av datacentraltjänster

När det gäller leverantörer av datacentraler ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En datacentraltjänst hos en datacentral som drivs av leverantören är helt otillgänglig.

(b) Tillgången till en datacentraltjänst hos en datacentral som drivs av leverantören är begränsad under en period av mer än en timme.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en datacentraltjänst har komprometterats till följd av en misstänkt skadlig handling.

(d) Den fysiska tillgången till en datacentral som drivs av leverantören har komprometterats.

Artikel 9

Betydande incidenter när det gäller leverantörer av nätverk för leverans av innehåll

När det gäller leverantörer av nätverk för leverans av innehåll, ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) Ett nätverk för leverans av innehåll är helt otillgängligt i över 30 minuter.

(b) Tillgången till ett nätverk för leverans av innehåll är begränsad för mer än 5 % av användarna av nätverket för leverans av innehåll i unionen, eller för mer än en miljon användare av nätverket för leverans av innehåll i unionen, beroende på vilket antal som är lägst, under en period av mer än en timme.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av ett nätverk för leverans av innehåll har komprometterats till följd av en misstänkt skadlig handling.

(d) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av ett nätverk för leverans av innehåll har komprometterats och det påverkar mer än 5 % av användarna av nätverket för leverans av innehåll i unionen, eller mer än 1 miljon av användarna av nätverket för leverans av innehåll i unionen, beroende på vilket antal som är lägst.

Artikel 10

Betydande incidenter när det gäller leverantörer av utlokaliserade driftstjänster och leverantörer av utlokaliserade säkerhetstjänster

När det gäller leverantörer av utlokaliserade driftstjänster och leverantörer av utlokaliserade säkerhetstjänster ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En utlokaliserad driftstjänst eller en utlokaliserad säkerhetstjänst är helt otillgänglig i över 30 minuter.

(b) Tillgången till en utlokaliserad driftstjänst eller en utlokaliserad säkerhetstjänst är begränsad för mer än 5 % av användarna av tjänsten i unionen, eller för mer än en miljon användare av tjänsten i unionen, beroende på vilket antal som är lägst, under en period av mer än en timme.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en utlokaliserad driftstjänst eller en utlokaliserad säkerhetstjänst har komprometterats till följd av en misstänkt skadlig handling.

(d) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en utlokaliserad driftstjänst eller en utlokaliserad säkerhetstjänst har komprometterats och det påverkar mer än 5 % av användarna av en utlokaliserad driftstjänst eller utlokaliserad säkerhetstjänst i unionen, eller mer än en miljon av användarna av tjänsten i unionen, beroende på vilket antal som är lägst.

Artikel 11

Betydande incidenter när det gäller leverantörer av marknadsplatser online

När det gäller leverantörer av marknadsplatser online ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) Marknadsplatsen online är helt otillgänglig för mer än 5 % av användarna av marknadsplatsen online i unionen, eller för mer än en miljon användare av marknadsplatsen online i unionen, beroende på vilket antal som är lägst.

(b) Mer än 5 % av användarna av en marknadsplats online i unionen, eller mer än en miljon användare av en marknadsplats online i unionen, beroende på vilket antal som är lägst, påverkas av den begränsade tillgången till marknadsplatsen online.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en marknadsplats online har komprometterats till följd av en misstänkt skadlig handling.

(d) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en marknadsplats online har komprometterats och det påverkar mer än 5 % av användarna av

marknadsplatsen online i unionen, eller mer än en miljon av användarna av marknadsplatsen online i unionen, beroende på vilket antal som är lägst.

Artikel 12

Betydande incidenter när det gäller leverantörer av sökmotorer

När det gäller leverantörer av sökmotorer ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En sökmotor är helt otillgänglig för mer än 5 % av användarna av sökmotorn i unionen, eller för mer än en miljon användare av sökmotorn i unionen, beroende på vilket antal som är lägst.

(b) Mer än 5 % av användarna av en sökmotor i unionen, eller mer än en miljon användare av sökmotorn i unionen, beroende på vilket antal som är lägst, påverkas av den begränsade tillgången till sökmotorn.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en sökmotor har komprometterats till följd av en misstänkt skadlig handling.

(d) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en sökmotor har komprometterats och det påverkar mer än 5 % av användarna av sökmotorn i unionen, eller mer än en miljon av användarna av sökmotorn i unionen, beroende på vilket antal som är lägst.

Artikel 13

Betydande incidenter när det gäller leverantörer av plattformar för sociala nätverkstjänster

När det gäller leverantörer av plattformar för sociala nätverkstjänster ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En plattform för sociala nätverkstjänster är helt otillgänglig för mer än 5 % av användarna av plattformen i unionen, eller för mer än en miljon användare av plattformen i unionen, beroende på vilket antal som är lägst.

(b) Mer än 5 % av användarna av en plattform för sociala nätverkstjänster i unionen, eller mer än en miljon användare av plattformen i unionen, beroende på vilket antal som är lägst, påverkas av den begränsade tillgången till plattformen.

(c) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en plattform för sociala nätverkstjänster har komprometterats till följd av en misstänkt skadlig handling.

(d) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en plattform för sociala nätverkstjänster har komprometterats och det påverkar mer än 5 % av användarna av plattformen i unionen, eller mer än en miljon av plattformens användare i unionen, beroende på vilket antal som är lägst.

Artikel 14

Betydande incidenter när det gäller tillhandahållare av betrodda tjänster

När det gäller tillhandahållare av betrodda tjänster ska en incident anses som betydande enligt artikel 3.1 g om den uppfyller ett eller flera av följande kriterier:

(a) En betrodd tjänst är helt otillgänglig i över 20 minuter.

(b) En betrodd tjänst är otillgänglig för användare eller förlitande parter i mer än en timme beräknat per kalendervecka.

(c) Mer än 1 % av användarna eller de förlitande parterna i unionen, eller fler än 200 000 användare eller förlitande parter i unionen, beroende på vilket antal som är lägst, påverkas av den begränsade tillgången till en betrodd tjänst.

(d) Den fysiska tillgången till ett område där nätverks- och informationssystem är lokaliserade och till vilket tillgången är begränsad till betrodd personal hos tillhandahållaren av betrodda tjänster, eller skyddet av sådan fysisk tillgång, har kompromitterats.

(e) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en betrodd tjänst har kompromitterats och det påverkar mer än 0,1 % av användarna eller de förlitande parterna, eller fler än 100 användare eller förlitande parter, beroende på vilket antal som är lägst, för den betrodda tjänsten i unionen.

Artikel 15

Upphävande

Kommissionens genomförandeförordning (EU) 2018/151[4] ska upphöra att gälla.

Artikel 16

Ikraftträdande och tillämpning

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

[4] Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 vad gäller närmare specificering av de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan (EUT L 26, 31.1.2018, s. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

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

Utfärdad i Bryssel den 17.10.2024

På kommissionens vägnar
Ordförande
Ursula VON DER LEYEN