Europeiska unionens
officiella tidning

SV
L-serien

2024/2690

18.10.2024

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2024/2690

av den 17 oktober 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 bilagan till denna förordning på europeiska och internationella standarder, såsom ISO/IEC 27001, ISO/IEC 27002 och Etsi EN 319401, 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.

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

(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 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.

([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).

(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 kompromitteras 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.

(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.

([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).

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 (EU) 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 euro 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 kompromitterats till följd av en misstänkt skadlig handling.

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

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 kompromitterats 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 kompromitterats 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 kompromitterats 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 kompromitterats 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 kompromitterats 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 kompromitterats 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 kompromitterats 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 kompromitterats 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 kompromitterats 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 kompromitterats 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 komprometterats.

e) Integriteten, konfidentialiteten eller autenticiteten hos lagrade, överförda eller behandlade uppgifter i samband med tillhandahållandet av en betrodd tjänst har komprometterats 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*.

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

Utfärdad i Bryssel den 17 oktober 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

([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).

BILAGA

Tekniska och metodologiska specifikationer som avses i artikel 2 i denna förordning

1. **Strategi för säkerhet i nätverks- och informationssystem (artikel 21.2 a i direktiv (EU) 2022/2555)**

1.1. *Strategi för säkerhet i nätverks- och informationssystem*

1.1.1. Vid tillämpning av artikel 21.2 a i direktiv (EU) 2022/2555 ska strategin för säkerhet i nätverks- och informationssystem

(a) fastställa de berörda entiteternas tillvägagångssätt för att hantera säkerheten i sina nätverks- och informationssystem,

(b) vara lämpliga för och komplettera de berörda entiteternas affärsstrategi och mål,

(c) fastställa nätverks- och informationssäkerhetsmål,

(d) omfatta ett åtagande om kontinuerlig förbättring av säkerheten i nätverks- och informationssystem,

(e) omfatta ett åtagande om att tillhandahålla tillräckliga resurser för genomförandet av denna strategi, inklusive nödvändig personal, ekonomiska resurser, processer, verktyg och teknik,

(f) kommuniceras till och erkännas av berörda anställda och berörda externa parter,

(g) fastställa roller och ansvarsområden i enlighet med punkt 1.2,

(h) förteckna den dokumentation som ska sparas och ange hur länge dokumentationen ska bevaras,

(i) förteckna de ämnesspecifika strategierna,

(j) omfatta indikatorer och åtgärder för att övervaka genomförandet och den aktuella mognadsnivån när det gäller nätverks- och informationssäkerhet hos de berörda entiteterna,

(k) ange det datum då den formellt godkändes av de berörda entiteternas ledningsorgan (*ledningsorganen*).

1.1.2. Säkerhetsstrategin för nätverks- och informationssystem ska ses över och när så är lämpligt uppdateras av ledningsorganen minst en gång om året samt när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar. Resultatet av översynerna ska dokumenteras,

1.2. *Roller, ansvarsområden och befogenheter*

1.2.1. Som ett led i sin strategi för säkerheten i nätverks- och informationssystem enligt punkt 1.1 ska de berörda entiteterna fastställa ansvarsområden och befogenheter för säkerheten i nätverks- och informationssystem, dela upp dem på roller och fördela dem i enlighet med de berörda entiteternas behov samt kommunicera dem till ledningsorganen.

1.2.2. De berörda entiteterna ska kräva att all personal och alla tredje parter tillämpar säkerheten i nätverks- och informationssystem i enlighet med den fastställda strategin för säkerhet i nätverks- och informationssystem samt med de berörda entiteternas ämnesspecifika strategier och förfaranden.

1.2.3. Åtminstone en person ska rapportera direkt till ledningsorganen om frågor som rör säkerheten i nätverks- och informationssystem.

1.2.4. Beroende på de berörda entiteternas storlek ska säkerheten i nätverks- och informationssystem täckas av särskilda roller eller uppgifter som utförs utöver de befintliga rollerna.

1.2.5. Uppgifter och ansvarsområden som står i strid med varandra ska separeras, om tillämpligt.

1.2.6. Roller, ansvarsområden och befogenheter ska ses över och vid behov uppdateras av ledningsorganen med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

2. **Strategi för riskhantering (artikel 21.2 a i direktiv (EU) 2022/2555)**

2.1. *Riskhanteringsram*

2.1.1. Vid tillämpning av artikel 21.2 a i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa och upprätthålla en ändamålsenlig riskhanteringsram för att identifiera och åtgärda risker för säkerheten i nätverks- och informationssystem. De berörda entiteterna ska utföra och dokumentera riskbedömningar och på grundval av resultaten fastställa, genomföra och övervaka en riskhanteringsplan. Riskbedömningens resultat och kvarstående risker ska godtas av ledningsorganen eller, om tillämpligt, av personer som är ansvariga och har befogenhet att hantera risker, förutsatt att de berörda entiteterna säkerställer lämplig rapportering till ledningsorganen.

2.1.2. Vid tillämningen av punkt 2.1.1 ska de berörda entiteterna fastställa förfaranden för identifiering, analys, bedömning och behandling av risker (*riskhanteringsprocess för cybersäkerhet*) Riskhanteringsprocessen för cybersäkerhet ska vara en integrerad del av de berörda entiteternas allmänna riskhanteringsprocess, om tillämpligt. Som ett led i riskhanteringsprocessen för cybersäkerhet ska de berörda entiteterna

(a) följa en riskhanteringsmetod,

(b) fastställa risktoleransnivån i enlighet med de berörda entiteternas riskbenägenhet,

(c) fastställa och upprätthålla relevanta riskkriterier,

(d) i enlighet med en allriskansats identifiera och dokumentera riskerna för säkerheten i nätverks- och informationssystem, i synnerhet i förhållande till tredje parter och när det gäller risker som kan leda till störningar vad gäller tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten för nätverks- och informationssystemen, inbegripet identifiering av felkritiska systemdelar (*SPOF*),

(e) analysera riskerna för säkerheten i nätverks- och informationssystem, inklusive hot, sannolikhet, konsekvenser och risknivå, med beaktande av underrättelser om cyberhot och sårbarheter,

(f) bedöma de identifierade riskerna baserat på riskkriterierna,

(g) identifiera och prioritera lämpliga riskhanteringsalternativ och -åtgärder,

(h) kontinuerligt övervaka genomförandet av riskhanteringsåtgärderna,

(i) identifiera vem som har ansvaret för riskhanteringsåtgärderna och när dessa bör genomföras,

(j) på ett begripligt sätt dokumentera de valda riskhanteringsåtgärderna i en riskhanteringsplan, liksom skälen till att kvarstående risker godtas.

2.1.3. När lämpliga riskhanteringsalternativ och -åtgärder identifieras och prioriteras ska de berörda entiteterna ta hänsyn till riskbedömningsresultaten, resultaten av förfarandet för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet, kostnaderna för genomförandet i förhållande till den förväntade nyttan, den klassificering av tillgångar som avses i punkt 12.1 samt den konsekvensanalys som avses i punkt 4.1.3.

2.1.4. De berörda entiteterna ska se över och när så är lämpligt uppdatera riskbedömningsresultaten och riskhanteringsplanen med planerade intervall och åtminstone varje år samt när betydande förändringar av driften eller riskerna eller betydande incidenter inträffar.

2.2. *Övervakning av efterlevnad*

2.2.1. De berörda entiteterna ska regelbundet granska efterlevnaden av sina strategier för säkerheten i nätverks- och informationssystem samt ämnesspecifika strategier, regler och standarder. Ledningsorganen ska genom regelbunden rapportering informeras om nivån av nätverks- och informationssäkerhet på grundval av granskningen av efterlevnaden.

2.2.2. De berörda entiteterna ska införa ett effektivt system för rapportering om efterlevnaden, vilket ska vara ändamålsenligt i förhållande till deras strukturer, driftsförhållanden och hotbilder. Rapporteringssystemet ska kunna ge ledningsorganen en väl underbyggd bild av det rådande läget i fråga om de berörda entiteternas riskhantering.

2.2.3. De berörda entiteterna ska genomföra övervakningen av efterlevnaden med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

2.3. *Oberoende granskning av nätverks- och informationssäkerheten*

2.3.1. De berörda entiteterna ska på ett oberoende sätt granska sitt tillvägagångssätt för att hantera säkerheten i nätverks- och informationssystem och sitt genomförande, inbegripet personer, processer och teknik.

2.3.2. De berörda entiteterna ska utveckla och upprätthålla processer för oberoende granskningar som ska utföras av personer med lämplig revisionskompetens. Om den oberoende granskningen utförs av anställda hos den berörda entiteten får de personer som utför granskningen inte ha en överordnad ställning i beslutshierarkin i förhållande till personalen på det område som granskas. Om den berörda entitetens storlek innebär att en sådan separation av beslutshierarkin inte är möjlig ska de berörda entiteterna vidta alternativa åtgärder för att garantera granskningarnas opartiskhet.

2.3.3. Resultaten av de oberoende granskningarna, inbegripet resultaten från övervakningen av efterlevnaden enligt punkt 2.2 och övervakningen och mätningen enligt punkt 7, ska rapporteras till ledningsorganen. Korrigerande åtgärder ska vidtas eller kvarstående risk godtas i enlighet med de berörda entiteternas kriterier för riskacceptans.

2.3.4. De oberoende granskningarna ska genomföras med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

3. **Incidenthantering (artikel 21.2 b i direktiv (EU) 2022/2555)**

3.1. *Incidenthanteringsstrategi*

3.1.1. Vid tillämpning av artikel 21.2 b i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa och genomföra en incidenthanteringsstrategi som omfattar roller, ansvarsområden och förfaranden för upptäckt, analys, begränsning, svarsåtgärder, återställande, dokumentation och rapportering i rätt tid när det gäller incidenter.

3.1.2. Den strategi som avses i punkt 3.1.1 ska överensstämma med den driftskontinuitets- och katastrofplan som avses i punkt 4.1. Strategin ska omfatta följande:

(a) Ett kategoriseringssystem för incidenter som är förenligt med den bedömning och klassificering av händelser som görs i enlighet med punkt 3.4.1.

(b) Effektiva kommunikationsplaner som innefattar eskalering och rapportering.

(c) Fördelning av roller på behöriga anställda när det gäller upptäckt och lämplig hantering av incidenter.

(d) Dokument att använda i samband med upptäckt och åtgärdande, såsom incidenthanteringsmanualer, eskaleringsscheman, kontaktlistor och mallar.

3.1.3. Roller, ansvarsområden och förfaranden som fastställs i strategin ska testas, ses över och när så är lämpligt uppdateras med planerade intervall och efter betydande incidenter eller betydande förändringar av driften eller riskerna.

3.2. *Övervakning och loggning*

3.2.1. De berörda entiteterna ska fastställa förfaranden och använda verktyg för att övervaka och logga aktiviteter på sina nätverks- och informationssystem för att upptäcka händelser som skulle kunna anses som incidenter och vidta åtgärder för att begränsa konsekvenserna.

3.2.2. I den mån det är genomförbart ska övervakningen automatiseras och utföras antingen kontinuerligt eller med jämna mellanrum, med förbehåll för verksamhetskapaciteten. De berörda entiteterna ska genomföra sin övervakningsverksamhet på ett sådant sätt att antalet falskt positiva och falskt negativa resultat minimeras.

3.2.3. Baserat på de förfaranden som avses i punkt 3.2.1 ska de berörda entiteterna upprätthålla, dokumentera och granska loggar. De berörda entiteterna ska upprätta en förteckning över tillgångar som ska vara föremål för loggning baserat på resultaten av den riskbedömning som utförts i enlighet med punkt 2.1. När så är lämpligt ska loggen inkludera följande:

(a) Relevant utgående och inkommande nätverkstrafik.

(b) Skapande, ändring eller radering av användare av de berörda entiteternas nätverks- och informationssystem och förlängning av tillstånd.

(c) Åtkomst till system och applikationer.

(d) Autentiseringsrelaterade händelser.

(e) All privilegierad åtkomst till system och applikationer samt aktiviteter som utförts av administratörskonton.

(f) Åtkomst eller ändringar av kritiska konfigurations- och säkerhetskopieringsfiler.

(g) Händelseloggar och loggar från säkerhetsverktyg, såsom antivirusprodukter, intrångsdetekteringssystem eller brandväggar.

(h) Användning av systemresurser samt deras prestanda.

(i) Fysiskt tillträde till anläggningar.

(j) Åtkomst till och användning av deras nätutrustning och enheter.

(k) Aktivering och stopp och paus för de olika loggarna.

(l) Miljöhändelser.

3.2.4. Loggarna ska regelbundet ses över med avseende på eventuella ovanliga eller oönskade trender. När så är lämpligt ska de berörda entiteterna fastställa lämpliga tröskelvärden för larm. Om de fastställda tröskelvärdena överskrids ska ett larm utlösas, när så är lämpligt automatiskt. Vid ett larm ska de berörda entiteterna säkerställa att en kvalificerad och ändamålsenlig svarsåtgärd snabbt inleds.

3.2.5. De berörda entiteterna ska bevara och säkerhetskopiera loggar under en på förhand fastställd tidsperiod och ska skydda dem från obehörig åtkomst eller obehöriga ändringar.

3.2.6. I den mån det är genomförbart ska de berörda entiteterna säkerställa att alla system har synkroniserade tidskällor så att det är möjligt att korrelera loggar mellan system för bedömning av händelser. De berörda entiteterna ska fastställa och bevara en förteckning över alla tillgångar som loggas och säkerställa att övervaknings- och loggningssystemen är redundanta. Tillgången till övervaknings- och loggningssystem ska övervakas oberoende av de system som de övervakar.

3.2.7. Förfarandena och förteckningen över tillgångar som loggas ska ses över och när så är lämpligt uppdateras regelbundet och efter betydande incidenter.

3.3. *Händelserapportering*

3.3.1. De berörda entiteterna ska införa en enkel mekanism som gör att deras anställda, leverantörer och kunder kan rapportera misstänkta händelser.

3.3.2. När så är lämpligt ska de berörda entiteterna förmedla händelserapporteringsmekanismen till sina leverantörer och kunder, och de ska regelbundet utbilda sina anställda om hur mekanismen ska användas.

3.4. *Bedömning och klassificering av händelser*

3.4.1. De berörda entiteterna ska bedöma misstänkta händelser för att fastställa om de utgör incidenter och i sådana fall fastställa deras art och allvarlighetsgrad.

3.4.2. Vid tillämpning av punkt 3.4.1 ska de berörda entiteterna agera på följande sätt:

(a) Utföra bedömningen baserat på fördefinierade kriterier som fastställts i förväg och på triage för att avgöra prioriteringsordningen för åtgärder för begränsning och eliminering.

(b) Varje kvartal bedöma förekomsten av sådana återkommande incidenter som avses i artikel 4 i denna förordning.

(c) Granska lämpliga loggar för bedömning och klassificering av händelser.

(d) Införa en process för korrelering och analys av loggar.

(e) Göra en förnyad bedömning och klassificera om händelser när ny information blir tillgänglig eller efter analys av tidigare tillgänglig information.

3.5. *Incidenthantering*

3.5.1. De berörda entiteterna ska hantera incidenterna i enlighet med dokumenterade förfaranden och i rätt tid.

3.5.2. Incidenthanteringsförfarandena ska omfatta följande stadier:

(a) Begränsning av incidenten, för att förhindra att dess konsekvenser sprids.

(b) Eliminering, för att förhindra att incidenten fortsätter eller återkommer.

(c) Återställande från incidenten, vid behov.

3.5.3. De berörda entiteterna ska fastställa kommunikationsplaner och kommunikationsförfaranden

(a) med CSIRT-enheter (enheter för hantering av it-säkerhetsincidenter) eller, om tillämpligt, de behöriga myndigheterna, när det gäller incidentrapportering,

(b) för kommunikation mellan den berörda entitetens anställda och för kommunikation med berörda aktörer utanför entiteten.

3.5.4. De berörda entiteterna ska logga incidenthanteringsåtgärder i enlighet med de förfaranden som avses i punkt 3.2.1 och registrera bevisningen.

3.5.5. De berörda entiteterna ska med planerade intervall testa sina incidenthanteringsförfaranden.

3.6. *Efterhandsgranskning efter incidenter*

3.6.1. När så är lämpligt ska de berörda entiteterna genomföra efterhandsgranskningar efter återställningen från incidenter. Efterhandsgranskningarna ska om möjligt identifiera grundorsaken till incidenten och mynna ut i dokumenterade lärdomar för att minska förekomsten och konsekvenserna av incidenter i framtiden.

3.6.2. De berörda entiteterna ska säkerställa att efterhandsgranskningarna bidrar till att förbättra deras tillvägagångssätt för nätverks- och informationssäkerhet och riskbehandling samt deras förfaranden för hantering, upptäckt och åtgärdande av incidenter.

3.6.3. De berörda entiteterna ske med planerade intervall granska om det skett någon efterhandsgranskning efter incidenter.

4. **Driftskontinuitet och krishantering (artikel 21.2 c i direktiv (EU) 2022/2555)**

4.1. *Driftskontinuitets- och katastrofplan*

4.1.1. Vid tillämpning av artikel 21.2 c i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa och upprätthålla en driftskontinuitets- och katastrofplan att använda vid incidenter.

4.1.2. De berörda entiteternas drift ska återställas i enlighet med driftskontinuitets- och katastrofplanen. Planen ska baseras på resultaten av den riskbedömning som utförts i enlighet med punkt 2.1 och ska, när så är lämpligt, innehålla följande:

(a) Ändamål, tillämpningsområde och målgrupp.

(b) Roller och ansvarsområden.

(c) Viktiga kontakter och (interna och externa) kommunikationskanaler.

(d) Villkor för aktivering och avaktivering av planen.

(e) Ordningsföljden för återställande av driften.

(f) Återställningsplaner för olika delar av driften, inklusive återställningsmål.

(g) Resurser som krävs, inklusive säkerhetskopior och redundans.

(h) Återläsning och återupptagande av verksamhet från tillfälliga åtgärder

4.1.3. De berörda entiteterna ska göra en konsekvensanalys för att bedöma de potentiella konsekvenser som allvarliga störningar har för deras verksamhet och, baserat på konsekvensanalysens resultat, fastställa kontinuitetskrav för sina nätverks- och informationssystem.

4.1.4. Driftskontinuitetsplanen och katastrofplanen ska testas, ses över och, när så är lämpligt, uppdateras med planerade intervall och efter betydande incidenter eller betydande ändringar av driften eller riskerna. De berörda entiteterna ska säkerställa att planerna införlivar lärdomarna från sådana tester.

4.2. *Hantering av säkerhetskopiering och redundans*

4.2.1. De berörda entiteterna ska bevara säkerhetskopior av data och tillhandahålla tillräckliga tillgängliga resurser, inklusive anläggningar, nätverks- och informationssystem och personal, för att säkerställa en lämplig nivå av redundans.

4.2.2. Baserat på resultaten av den riskbedömning som utförts i enlighet med punkt 2.1 och driftskontinuitetsplanen ska de berörda entiteterna fastställa säkerhetskopieringsplaner som omfattar följande:

(a) Återställningstid.

(b) Säkerställande av att säkerhetskopiorna är fullständiga och korrekta, inklusive konfigurationsdata och data som lagras i molntjänstmiljö.

(c) Lagring av säkerhetskopior (online eller offline) på en eller flera säkra platser, som inte ingår i samma nätverk som systemet och som är på tillräckligt avstånd för att klara sig från eventuella skador från en katastrof vid huvudanläggningen.

(d) Lämplig fysisk och logisk kontroll av åtkomst till säkerhetskopiorna, i enlighet med tillgångens klassificeringsnivå.

(e) Återläsning av data från säkerhetskopior.

(f) Lagringstiden baseras på verksamhetskrav och rättsliga krav.

4.2.3. De berörda entiteterna ska utföra regelbundna integritetskontroller av säkerhetskopiorna.

4.2.4. Baserat på resultaten av den riskbedömning som utförts i enlighet med punkt 2.1 och driftskontinuitetsplanen ska de berörda entiteterna säkerställa tillräckliga resurser genom åtminstone partiell redundans på följande områden:

(a) Nätverks- och informationssystem.

(b) Tillgångar, inklusive anläggningar, utrustning och materiel.

(c) Personal med det ansvar, de befogenheter och den kompetens som krävs.

(d) Ändamålsenliga kommunikationskanaler.

4.2.5. När så är lämpligt ska de berörda entiteterna säkerställa att övervakningen och anpassningen av resurser, inklusive anläggningar, system och personal, beaktar kraven i fråga om säkerhetskopiering och redundans.

4.2.6. De berörda entiteterna ska regelbundet testa återställningen av säkerhetskopior och redundanser för att säkerställa att de är tillförlitliga under återställningsförhållanden och att de omfattar de kopior, processer och kunskaper som krävs för en effektiv återställning. De berörda entiteterna ska dokumentera resultaten av testerna och vid behov vidta korrigerande åtgärder.

4.3. *Krishantering*

4.3.1. De berörda entiteterna ska införa en krishanteringsprocess.

4.3.2. De berörda entiteterna ska säkerställa att krishanteringsprocessen omfattar åtminstone följande aspekter:

(a) Roller och ansvarsområden för personal och, när så är lämpligt, leverantörer och tjänsteleverantörer, där rollfördelningen i krissituationer specificeras, inklusive specifika steg att följa.

(b) Ändamålsenliga kommunikationsmedel mellan de berörda entiteterna och de berörda behöriga myndigheterna.

(c) Tillämpning av ändamålsenliga åtgärder för att säkerställa att säkerheten i nätverks- och informationssystem upprätthålls i krissituationer.

Vid tillämpning av led b ska informationsflödet mellan de berörda entiteterna och de berörda behöriga myndigheterna innefatta både obligatorisk kommunikation, såsom incidentrapporter och tillhörande tidslinjer, och kommunikation som inte är obligatorisk.

4.3.3. De berörda entiteterna ska införa en process för hantering och utnyttjande av information som inkommer från CSIRT-enheter eller, om tillämpligt, de behöriga myndigheterna, om incidenter, sårbarheter, hot eller möjliga begränsningsåtgärder.

4.3.4. De berörda entiteterna ska testa, se över och när så är lämpligt uppdatera krishanteringsplanen regelbundet eller efter betydande incidenter eller betydande förändringar av driften eller riskerna.

5. **Säkerhet i leveranskedjan (artikel 21.2 d i direktiv (EU) 2022/2555)**

5.1. *Strategi för säkerhet i leveranskedjan*

5.1.1. Vid tillämpning av artikel 21.2 d i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa, genomföra och tillämpa en strategi för säkerhet i leveranskedjan som styr relationerna med deras direkta leverantörer och tjänsteleverantörer i syfte att minska de identifierade riskerna för säkerheten i nätverks- och informationssystem. I denna strategi ska de berörda entiteterna identifiera sin roll i leveranskedjan och förmedla den till sina direkta leverantörer och tjänsteleverantörer.

5.1.2. Som ett led i den strategi för säkerhet i leveranskedjan som avses i punkt 5.1.1 ska de berörda entiteterna fastställa kriterier för att välja ut och ingå avtal med leverantörer och tjänsteleverantörer. Kriterierna ska inbegripa följande:

(a) Leverantörernas och tjänsteleverantörernas cybersäkerhetsrutiner, inklusive deras säkra utvecklingsförfaranden.

(b) Leverantörernas och tjänsteleverantörernas förmåga att uppfylla de berörda entiteternas cybersäkerhetsspecifikationer.

(c) IKT-produkternas och IKT-tjänsternas allmänna kvalitet och resiliens samt de riskhanteringsåtgärder för cybersäkerhet som ingår i dem, inklusive IKT-produkternas och IKT-tjänsternas risknivå och klassificeringsnivå.

(d) De berörda entiteternas förmåga att diversifiera leveranskällor och förhindra inlåsningar till enskilda leverantörer, om tillämpligt.

5.1.3. När de berörda entiteterna fastställer sin strategi för säkerhet i leveranskedjan ska de, om tillämpligt, beakta resultaten av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som genomförts i enlighet med artikel 22.1 i direktiv (EU) 2022/2555.

5.1.4. Baserat på strategin för säkerhet i leveranskedjan och med beaktande av resultaten av den riskbedömning som genomförts i enlighet med punkt 2.1 i denna bilaga ska de berörda entiteterna säkerställa att följande specificeras i deras avtal med leverantörer och tjänsteleverantörer, i tillämpliga fall och när så är lämpligt genom servicenivåavtal:

(a) Cybersäkerhetskrav för leverantörerna eller tjänsteleverantörerna, inklusive krav som rör säkerheten vid förvärv av IKT-tjänster eller IKT-produkter enligt punkt 6.1.

(b) Krav som rör medvetenhet, kompetens och utbildning och, när så är lämpligt, certifiering, för leverantörens eller tjänsteleverantörens anställda.

(c) Krav som rör kontroll av bakgrunden för leverantörers och tjänsteleverantörers anställda.

(d) En skyldighet för leverantörer och tjänsteleverantörer att utan onödigt dröjsmål underrätta de berörda entiteterna om incidenter som utgör en risk för säkerheten i dessa entiteters nätverks- och informationssystem.

(e) Rätt att göra revisioner eller erhålla revisionsrapporter.

(f) En skyldighet för leverantörer och tjänsteleverantörer att hantera sårbarheter som utgör en risk för säkerheten i de berörda entiteternas nätverks- och informationssystem.

(g) Krav som rör underentreprenader och, om de berörda entiteterna tillåter underentreprenader, cybersäkerhetskrav för underleverantörer i enlighet med de cybersäkerhetskrav som avses i led a.

(h) Skyldigheter för leverantörer och tjänsteleverantörer vid uppsägning av avtalet, såsom insamling och bortskaffande av de uppgifter som leverantörerna och tjänsteleverantörerna erhållit i utövandet av sina uppgifter.

5.1.5. De berörda entiteterna ska ta hänsyn till de aspekter som avses i punkt 5.1.2 och 5.1.3 i sina urvalsförfaranden för nya leverantörer och tjänsteleverantörer samt som ett led i den upphandlingsprocess som avses i punkt 6.1.

5.1.6. De berörda entiteterna ska se över strategin för säkerhet i leveranskedjan och övervaka, utvärdera och, vid behov, agera vid ändringar av leverantörernas och tjänsteleverantörernas cybersäkerhetsrutiner, med planerade intervall och vid betydande förändringar av driften eller riskerna och vid betydande incidenter som är relaterade till tillhandahållandet av IKT-tjänster eller som påverkar säkerheten för IKT-produkterna från leverantören eller tjänsteleverantören.

5.1.7. Vid tillämpning av punkt 5.1.6 ska de berörda entiteterna

(a) regelbundet övervaka rapporteringen om genomförandet av servicenivåavtalen, i tillämpliga fall,

(b) granska incidenter som rör IKT-produkter och IKT-tjänster från leverantörer och tjänsteleverantörer,

(c) bedöma behovet av oplanerade granskningar och dokumentera resultaten på ett begripligt sätt,

(d) analysera riskerna förbundna med ändringar av IKT-produkter och IKT-tjänster från leverantörer och tjänsteleverantörer och, när så är lämpligt, snabbt vidta begränsningsåtgärder.

5.2. *Förteckning över leverantörer och tjänsteleverantörer*

De berörda entiteterna ska föra och uppdatera ett register över sina direkta leverantörer och tjänsteleverantörer vilket ska omfatta följande:

(a) Kontaktpunkter för varje direkt leverantör och tjänsteleverantör.

(b) En förteckning över IKT-produkter, IKT-tjänster och IKT-processer som den direkta leverantören eller tjänsteleverantören tillhandahåller den berörda entiteten.

6. **Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem (artikel 21.2 e i direktiv (EU) 2022/2555)**

6.1. *Säkerhet vid förvärv av IKT-tjänster och IKT-produkter*

6.1.1. Vid tillämpning av artikel 21.2 e i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa och genomföra processer för att hantera risker till följd av förvärv av IKT-tjänster eller IKT-produkter för komponenter som är kritiska för säkerheten i de berörda entiteternas nätverks- och informationssystem, baserat på den riskbedömning som utförts i enlighet med punkt 2.1, från leverantörer eller tjänsteleverantörer under hela deras livscykel.

6.1.2. Vid tillämpning av punkt 6.1.1 ska de processer som avses i punkt 6.1.1 omfatta följande:

(a) Säkerhetskrav som ska tillämpas på de IKT-tjänster eller IKT-produkter som förvärvas.

(b) Krav på säkerhetsuppdateringar under hela livslängden för IKT-tjänsterna eller IKT-produkterna eller krav på att de ska ersättas efter stödperiodens utgång.

(c) Information som beskriver de maskinvaru- och programvarukomponenter som används i IKT-tjänsterna eller IKT-produkterna.

(d) Information som beskriver de cybersäkerhetsfunktioner som IKT-tjänsterna eller IKT-produkterna omfattar och den konfiguration som krävs för en säker drift av dem.

(e) Garantier för att IKT-tjänsterna eller IKT-produkterna uppfyller säkerhetskraven enligt led a.

(f) Metoder för att validera att de levererade IKT-tjänsterna eller IKT-produkterna uppfyller de angivna säkerhetskraven samt dokumentation av valideringsresultaten.

6.1.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera processerna med planerade intervall och när betydande incidenter inträffar.

6.2. *Säker utvecklingslivscykel*

6.2.1. Innan de utvecklar ett nätverks- och informationssystem, inklusive programvara, ska de berörda entiteterna fastställa reglerna för en säker utveckling av nätverks- och informationssystem och tillämpa dessa regler när de själva utvecklar nätverks- och informationssystem och när utvecklingen läggs ut på entreprenad. Reglerna ska omfatta alla utvecklingsfaser och inbegripa specifikationer, utformning, utveckling, genomförande och testning.

6.2.2. Vid tillämpning av punkt 6.2.1 ska de berörda entiteterna göra följande:

(a) Göra en analys av säkerhetskraven i specifikations- och utformningsfaserna för alla utvecklings- eller inköpsprojekt som genomförs av de berörda entiteterna eller på dessa entiteters vägnar.

(b) Tillämpa principerna för konstruktion av säkra system och säker kodning på allt utvecklingsarbete som rör informationssystem, t.ex. främjande av inbyggd cybersäkerhet och nolltillitsarkitektur.

(c) Fastställa säkerhetskrav för utvecklingsmiljöer.

(d) Fastställa och genomföra processer för säkerhetstester under utvecklingscykeln.

(e) På lämpligt sätt välja ut, skydda och förvalta säkerhetstestdata.

(f) Sanera och anonymisera testdata enligt den riskbedömning som utförts i enlighet med punkt 2.1.

6.2.3. För utveckling av nätverks- och informationssystem som lagts ut på entreprenad ska de berörda entiteterna också tillämpa de strategier och förfaranden som avses i punkterna 5 och 6.1.

6.2.4. De berörda entiteterna ska se över och, vid behov, uppdatera sina regler för säker utveckling med planerade intervall.

6.3. *Konfigurationshantering*

6.3.1. De berörda entiteterna ska vidta ändamålsenliga åtgärder för att fastställa, dokumentera, genomföra och övervaka konfigurationer, inklusive säkerhetskonfigurationer av maskinvara, programvara, tjänster och nätverk.

6.3.2. Vid tillämpning av punkt 6.3.1 ska de berörda entiteterna göra följande:

(a) Fastställa och säkerställa säkerheten i konfigurationer för sin maskinvara och programvara och sina tjänster och nätverk.

(b) Fastställa och genomföra processer och verktyg för att verkställa de fastställda säkerhetskonfigurationerna för maskinvara, programvara, tjänster och nätverk, för nyinstallerade system och för system som är i drift under deras livslängd.

6.3.3. De berörda entiteterna ska se över och när så är lämpligt uppdatera konfigurationer med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

6.4. *Förändringshantering, reparationer och underhåll*

6.4.1. De berörda entiteterna ska tillämpa förändringshanteringsförfaranden för att kontrollera ändringar av nätverks- och informationssystem. Om tillämpligt ska förfarandena överensstämma med de berörda entiteternas allmänna strategier för förändringshantering.

6.4.2. De förfaranden som avses i punkt 6.4.1 ska tillämpas på versioner, ändringar och akutanpassningar av programvara och maskinvara som är i drift och på konfigurationsändringar. Förfarandena ska säkerställa att dessa ändringar är dokumenterade och, baserat på den riskbedömning som utförts i enlighet med punkt 2.1, testade och bedömda med avseende på de potentiella konsekvenserna innan de genomförs.

6.4.3. Om de vanliga förändringshanteringsförfarandena inte kan följas på grund av en akutsituation ska de berörda entiteterna dokumentera resultatet av ändringen och förklaringen till att förfarandena inte kunde följas.

6.4.4. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera förfarandena med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

6.5. *Säkerhetstestning*

6.5.1. De berörda entiteterna ska fastställa, införa och tillämpa en strategi och förfaranden för säkerhetstestning.

6.5.2. De berörda entiteterna ska

(a) baserat på den riskbedömning som utförts i enlighet med punkt 2.1 fastställa behov, tillämpningsområde, frekvens och typ när det gäller säkerhetstestning,

(b) genomföra säkerhetstester i enlighet med en dokumenterad testmetod, som omfattar de komponenter som i en riskanalys identifierats som relevanta för säker drift,

(c) dokumentera testernas typ, tillämpningsområde, tidsram och resultat, inklusive en bedömning av kritikalitet och begränsningsåtgärder för varje iakttagelse,

(d) tillämpa begränsningsåtgärder vid kritiska iakttagelser.

6.5.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera sina strategier för säkerhetstestning med planerade intervall.

6.6. *Hantering av programfix*

6.6.1. De berörda entiteterna ska specificera och tillämpa förfaranden som överensstämmer med de förändringshanteringsförfaranden som avses i punkt 6.4.1 och med sårbarhetshantering, riskhantering och andra relevanta hanteringsförfaranden för att säkerställa att

(a) programfixar tillämpas inom en rimlig tid från det att de blir tillgängliga,

(b) programfixar testas innan de tillämpas på produktionssystem,

(c) programfixar kommer från tillförlitliga källor och kontrolleras med avseende på integritet,

(d) kompletterande åtgärder vidtas och kvarstående risker godtas i de fall då en programfix inte är tillgänglig eller inte tillämpas i enlighet med punkt 6.6.2.

6.6.2. Genom undantag från punkt 6.6.1 a får de berörda entiteterna välja att inte tillämpa programfixar när nackdelarna med detta inte uppvägs av cybersäkerhetsfördelarna. De berörda entiteterna ska vederbörligen dokumentera och motivera varje sådant beslut.

6.7. *Nätverkssäkerhet*

6.7.1. De berörda entiteterna ska vidta ändamålsenliga åtgärder för att skydda sina nätverks- och informationssystem mot cyberhot.

6.7.2. Vid tillämpning av punkt 6.7.1 ska de berörda entiteterna

(a) dokumentera nätverkets arkitektur på ett begripligt och uppdaterat sätt,

(b) fastställa och tillämpa kontroller för att skydda de berörda entiteternas interna nätverksdomäner från obehörig åtkomst,

(c) konfigurera kontroller för att förhindra åtkomst och nätverkskommunikation som inte krävs för de berörda entiteternas drift,

(d) fastställa och tillämpa kontroller för fjärråtkomst till nätverks- och informationssystem, inbegripet tjänsteleverantörers åtkomst,

(e) inte använda system som används för att administrera genomförandet av säkerhetsstrategin för andra ändamål,

(f) uttryckligen förbjuda eller avaktivera anslutningar och tjänster som inte behövs,

(g) när så är lämpligt, uteslutande tillåta åtkomst till de berörda entiteternas nätverks- och informationssystem via utrustning med tillstånd från dessa entiteter,

(h) tillåta att tjänsteleverantörer ansluts först efter en begäran om behörighet och under en fastställd tidsperiod, såsom under den tid som en underhållsinsats tar,

(i) upprätta kommunikation mellan separata system endast via tillförlitliga kanaler som är isolerade med användning av logisk, kryptografisk eller fysisk separation från andra kommunikationskanaler och tillhandahålla säkrad identifiering av deras ändpunkter och skydd för kanaldata från ändring eller avslöjande,

(j) anta en genomförandeplan för en fullständig övergång till den senaste generationens kommunikationsprotokoll i nätverksskiktet på ett sätt som är säkert och ändamålsenligt och sker gradvis samt fastställa åtgärder för att påskynda en sådan övergång,

(k) anta en genomförandeplan för införande av internationellt överenskomna och interoperabla moderna standarder för e-postkommunikation för att säkra e-postkommunikationen i syfte att begränsa sårbarheter kopplade till e-postrelaterade hot och fastställa åtgärder för att påskynda ett sådant införande,

(l) tillämpa bästa praxis för DNS-säkerhet, dirigeringssäkerhet och dirigeringshygien för trafik från eller till nätverket.

6.7.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera dessa åtgärder med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

6.8. *Nätverkssegmentering*

6.8.1. De berörda entiteterna ska segmentera system i nätverk eller zoner i enlighet med resultaten från den riskbedömning som avses i punkt 2.1. De ska segmentera sina system och nätverk från tredje parters system och nätverk.

6.8.2. För detta ändamål ska de berörda entiteterna

(a) beakta det funktionella, logiska och fysiska förhållandet, inklusive lokalisering, mellan tillförlitliga system och tjänster,

(b) bevilja åtkomst till ett nätverk eller en zon baserat på en bedömning av dess säkerhetskrav,

(c) förvara system som är kritiska för den berörda entitetens drift eller säkerhet i säkrade zoner,

(d) införa en demilitariserad zon inom sina kommunikationsnät för att säkerställa säker kommunikation från eller till sina nätverk,

(e) begränsa åtkomst och kommunikation mellan och inom zoner till vad som är nödvändigt för de berörda entiteternas drift eller för säkerheten,

(f) separera det särskilda nätverket för administration av nätverks- och informationssystem från de berörda entiteternas nätverk för drift,

(g) segregera kanalerna för nätverksadministration från annan nätverkstrafik,

(h) separera produktionssystemen för den berörda entitetens tjänster från system som används för utveckling och testning, inklusive säkerhetskopior.

6.8.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera nätverkssegmenteringen med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

6.9. *Skydd mot sabotageprogram och otillåten programvara*

6.9.1. De berörda entiteterna ska skydda sina nätverks- och informationssystem mot sabotageprogram och otillåten programvara.

6.9.2. För detta ändamål ska de berörda entiteterna i synnerhet vidta åtgärder för upptäckt eller förhindrande av användning av sabotageprogram eller otillåten programvara. De berörda entiteterna ska, när så är lämpligt, säkerställa att deras nätverks- och informationssystem är utrustade med programvara för upptäckt och åtgärdande, som regelbundet uppdateras i enlighet med den riskbedömning som utförts i enlighet med punkt 2.1 och avtalen med leverantörerna.

6.10. *Sårbarhetshantering och sårbarhetsinformation*

6.10.1. De berörda entiteterna ska inhämta information om tekniska sårbarheter i deras nätverks- och informationssystem, bedöma sin exponering för sårbarheter och vidta ändamålsenliga åtgärder för att hantera sårbarheterna.

6.10.2. Vid tillämpning av punkt 6.10.1 ska de berörda entiteterna göra följande:

(a) Övervaka information om sårbarheter via lämpliga kanaler, såsom meddelanden från CSIRT-enheter eller behöriga myndigheter eller information som tillhandahålls av leverantörer eller tjänsteleverantörer.

(b) När så är lämpligt, genomföra sårbarhetsskanningar och registrera resultaten av skanningarna, med planerade intervall.

(c) Utan onödigt dröjsmål åtgärda sårbarheter som av de berörda entiteterna identifierats som kritiska för deras verksamhet.

(d) Säkerställa att deras sårbarhetshantering är förenlig med deras förfaranden för förändringshantering, hantering av programfix, riskhantering och incidenthantering.

(e) Fastställa ett förfarande för information om sårbarheter i enlighet med den tillämpliga nationella policyn för samordnad information om sårbarheter.

6.10.3. När det är motiverat på grund av sårbarhetens potentiella konsekvenser ska de berörda entiteterna upprätta och genomföra en plan för att begränsa sårbarheten. I andra fall ska de berörda entiteterna dokumentera och motivera varför sårbarheten inte behöver åtgärdas.

6.10.4. De berörda entiteterna ska med planerade intervall se över och, när så är lämpligt, uppdatera de kanaler som de använder för övervakning av sårbarhetsinformation.

7. **Strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärder för cybersäkerhet (artikel 21.2 f i direktiv (EU) 2022/2555)**

7.1. Vid tillämpning av artikel 21.2 f i direktiv (EU) 2022/2555) ska de berörda entiteterna fastställa, införa och tillämpa en strategi och förfaranden för att bedöma om de riskhanteringsåtgärder för cybersäkerhet som vidtagits av den berörda entiteten genomförs och upprätthålls på ett effektivt sätt.

7.2. De strategier och förfaranden som avses i punkt 7.1 ska beakta resultaten av riskbedömningen enligt punkt 2.1 och betydande incidenter i det förflutna. De berörda entiteterna ska fastställa

(a) vilka riskhanteringsåtgärder för cybersäkerhet som ska övervakas och mätas, inklusive processer och kontroller,

(b) metoderna för övervakning, mätning, analys och utvärdering, såsom tillämpligt, för att säkerställa giltiga resultat,

(c) när övervakning och mätning ska utföras,

(d) vem som har ansvaret för övervakning och mätning av effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,

(e) när resultaten från övervakning och mätning ska analyseras och utvärderas,

(f) vem som ska analysera och utvärdera dessa resultat.

7.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera strategierna och förfarandena med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

8. **Grundläggande praxis för cyberhygien och utbildning i cybersäkerhet (artikel 21.2 g i direktiv (EU) 2022/2555)**

8.1. *Medvetandehöjande och grundläggande praxis för cyberhygien*

8.1.1. Vid tillämpning av artikel 21.2 g i direktiv (EU) 2022/2555 ska de berörda entiteterna säkerställa att deras anställda, inbegripet personer i ledningsorganen, och direkta leverantörer och tjänsteleverantörer är medvetna om riskerna, har kunskap om betydelsen av cybersäkerhet och tillämpar praxis för cyberhygien.

8.1.2. Vid tillämpning av punkt 8.1.1 ska de berörda entiteterna erbjuda sina anställda, inbegripet personer i ledningsorganen, samt direkta leverantörer och tjänsteleverantörer när så är lämpligt i enlighet med punkt 5.1.4, ett program för att öka medvetenheten som ska

(a) schemaläggas över tid, så att aktiviteterna upprepas och täcker nya anställda,

(b) fastställas i enlighet med strategin för nätverks- och informationssäkerhet, ämnesspecifika strategier och relevanta förfaranden för nätverks- och informationssäkerhet,

(c) omfatta relevanta cyberhot, de riskhanteringsåtgärder för cybersäkerhet som införts, kontaktpunkter och resurser för ytterligare information och råd om cybersäkerhetsfrågor samt cyberhygienpraxis för användare.

8.1.3. Programmet för att öka medvetenheten ska, när så är lämpligt, testas med avseende på effektivitet. Programmet för att öka medvetenheten ska uppdateras och erbjudas med planerade intervall med beaktande av ändringar av praxis för cyberhygien och rådande hotbild och risker för de berörda entiteterna.

8.2. *Säkerhetsutbildning*

8.2.1. De berörda entiteterna ska identifiera anställda vars roller kräver säkerhetsrelevanta färdigheter och expertkunskaper och säkerställa att de regelbundet utbildas om säkerhet i nätverks- och informationssystem.

8.2.2. De berörda entiteterna ska fastställa, införa och tillämpa ett utbildningsprogram som är i linje med strategin för nätverks- och informationssäkerhet, ämnesspecifika strategier och andra relevanta förfaranden för nätverks- och informationssäkerhet som fastställer utbildningsbehoven för vissa roller och befattningar baserat på kriterier.

8.2.3. Den utbildning som avses i punkt 8.2.1 ska vara relevant för den anställdes arbetsuppgifter, och utbildningens effektivitet ska bedömas. Utbildningen ska ta hänsyn till befintliga säkerhetsåtgärder och omfatta följande:

(a) Anvisningar för säker konfiguration och drift av nätverks- och informationssystem, inbegripet mobil utrustning.

(b) Information om kända cyberhot.

(c) Utbildning om agerande vid säkerhetsrelevanta händelser.

8.2.4. De berörda entiteterna ska utbilda personal som övergår till nya befattningar och roller som kräver säkerhetsrelevanta färdigheter och expertkunskaper.

8.2.5. Programmet ska regelbundet uppdateras och genomföras med beaktande av tillämpliga strategier och regler, fördelningen av roller, ansvarsområden samt kända cyberhot och teknisk utveckling.

9. **Kryptografi (artikel 21.2 h i direktiv (EU) 2022/2555)**

9.1. Vid tillämpning av artikel 21.2 h i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa, införa och tillämpa en strategi och förfaranden för kryptografi, för att säkerställa en ändamålsenlig och effektiv användning av kryptografi för att skydda konfidentialiteten, autenticiteten och integriteten för data i enlighet med de berörda entiteternas klassificering av tillgångar och resultaten av den riskbedömning som utförts i enlighet med punkt 2.1.

9.2. Den strategi och de förfaranden som avses i punkt 9.1 ska fastställa följande:

(a) I enlighet med de berörda entiteternas klassificering av tillgångar – typ, styrka och kvalitet när det gäller de kryptografiska åtgärder som krävs för att skydda de berörda entiteternas tillgångar, inklusive data i vila och data vid transitering.

(b) Baserat på led a, de protokoll eller protokollfamiljer som ska antas, liksom kryptografiska algoritmer, krypteringsstyrka, kryptografiska lösningar och användningspraxis som ska godkännas och krävas för användning i entiteten, med kryptoföljsamhet när så är lämpligt.

(c) De berörda entiteternas nyckelhantering, inbegripet, när så är lämpligt, metoder för följande:

i) Generering av olika nycklar för kryptografiska system och applikationer.

ii) Utfärdande och erhållande av certifikat för öppen nyckel.

iii) Distribution av nycklar till avsedda entiteter, inklusive hur nycklarna ska aktiveras när de mottagits.

iv) Lagring av nycklar, inklusive hur behöriga användare får tillgång till nycklar.

v) Ändring eller uppdatering av nycklar, inklusive regler för när och hur nycklar ska ändras.

vi) Hantering av nycklar som komprometterats.

vii) Upphävande av nycklar, inklusive hur man drar in eller avaktiverar nycklar.

viii) Återställande av nycklar som förlorats eller korrumperats.

ix) Säkerhetskopiering eller arkivering av nycklar.

x) Förstörelse av nycklar.

xi) Loggning och revision av aktiviteter förbundna med nyckelhantering.

xii) Fastställande av aktiverings- och avaktiveringsdatum för nycklar för att säkerställa att nycklarna endast kan användas under den angivna tidsperioden i enlighet med organisationens regler om nyckelhantering.

9.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera sina strategier och förfaranden med planerade intervall, med beaktande av den senaste tekniken när det gäller kryptografi.

10. **Personalsäkerhet (artikel 21.2 i i direktiv (EU) 2022/2555)**

10.1. *Personalsäkerhet*

10.1.1. Vid tillämpning av artikel 21.2 i i direktiv (EU) 2022/2555 ska de berörda entiteterna säkerställa att deras anställda och direkta leverantörer och tjänsteleverantörer, om tillämpligt, förstår och åtar sig att uppfylla de säkerhetsuppgifter som de ansvarar för, på ett sätt som är lämpligt för de erbjudna tjänsterna och arbetet och i enlighet med de berörda entiteternas strategi för säkerheten i nätverks- och informationssystem.

10.1.2. De krav som avses i punkt 10.1.1 ska inbegripa följande:

(a) Mekanismer för att säkerställa att alla anställda, direkta leverantörer och tjänsteleverantörer, om tillämpligt, förstår och följer den standardpraxis för cyberhygien som de berörda entiteterna tillämpar i enlighet med punkt 8.1.

(b) Mekanismer för att säkerställa att alla användare med administrativ eller privilegierad åtkomst är medvetna om och agerar i enlighet med sina roller, ansvarsområden och befogenheter.

(c) Mekanismer för att säkerställa att personer i ledningsorganen förstår och agerar i enlighet med sina roller, ansvarsområden och befogenheter när det gäller säkerhet i nätverks- och informationssystem.

(d) Mekanismer för att anställa personal med rätt kvalifikationer för sina respektive roller, såsom referenskontroller, prövningsförfaranden, validering av certifieringar eller skriftliga prov.

10.1.3. De berörda entiteterna ska se över tilldelningen av personal till de specifika roller som avses i punkt 1.2 samt sina personalresurser i detta avseende, med planerade intervall och minst en gång per år. De ska uppdatera tilldelningen vid behov.

10.2. *Bakgrundskontroll*

10.2.1. De berörda entiteterna ska i den mån det är genomförbart säkerställa att bakgrunden kontrolleras för deras anställda och, om tillämpligt, för direkta leverantörer och tjänsteleverantörer i enlighet med punkt 5.1.4, om detta krävs för deras roller, ansvarsområden och befogenheter.

10.2.2. Vid tillämpning av punkt 10.2.1 ska de berörda entiteterna göra följande:

(a) Införa kriterier som anger vilka roller, ansvarsområden och befogenheter som endast får utövas av personer vars bakgrund har kontrollerats.

(b) Säkerställa att kontrollerna enligt punkt 10.2.1 av dessa personer utförs innan de börjar utöva dessa roller, ansvarsområden och befogenheter och att hänsyn därvid tas till tillämpliga lagar och andra författningar samt etik på ett sätt som står i proportion till verksamhetskraven, klassificeringen av tillgångar enligt punkt 12.1, de nätverks- och informationssystem som avses och de upplevda riskerna.

10.2.3. De berörda entiteterna ska, när så är lämpligt, se över strategin med planerade intervall och uppdatera den vid behov.

10.3. *Förfaranden vid avslutad eller ändrad anställning*

10.3.1. De berörda entiteterna ska säkerställa att ansvarsområden och uppgifter som rör säkerheten i nätverks- och informationssystem och som förblir giltiga efter avslutad eller ändrad anställning för deras anställda definieras i avtal och att efterlevnaden kontrolleras.

10.3.2. Vid tillämpning av punkt 10.3.1 ska de berörda entiteterna i personens arbets- och anställningsvillkor inkludera ett avtal eller en överenskommelse om vilka ansvarsområden och uppgifter som fortsätter att vara giltiga efter det att anställningen eller avtalet avslutats, t.ex. konfidentialitetsklausuler.

10.4. *Disciplinära förfaranden*

10.4.1. De berörda entiteterna ska fastställa, kommunicera och upprätthålla ett disciplinärt förfarande för hantering av överträdelser av strategin för säkerhet i nätverks- och informationssystem. Förfarandet ska beakta relevanta rättsliga och lagstadgade krav, avtalsbestämmelser och verksamhetskrav.

10.4.2. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera det disciplinära förfarandet med planerade intervall och när det är nödvändigt till följd av rättsliga ändringar eller betydande förändringar av driften eller riskerna.

11. Åtkomstkontroll (artikel 21.2 i och j i direktiv (EU) 2022/2555)

11.1. *Strategi för åtkomstkontroll*

11.1.1. Vid tillämpning av artikel 21.2 i i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa, dokumentera och genomföra strategier för fysisk och logisk åtkomstkontroll av åtkomsten till deras nätverks- och informationssystem, baserat på verksamhetskrav och nätverks- och informationssystemets säkerhetskrav.

11.1.2. De strategier som avses i punkt 11.1.1 ska

(a) behandla åtkomsten för personer, vilket inbegriper personal, besökare och externa entiteter såsom leverantörer och tjänsteleverantörer,

(b) behandla åtkomsten för nätverks- och informationssystem,

(c) säkerställa att åtkomst endast beviljas användare som har autentiserats på lämpligt sätt.

11.1.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera dessa strategier med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

11.2. *Hantering av åtkomsträttigheter*

11.2.1. De berörda entiteterna ska tillhandahålla, ändra, upphäva och dokumentera åtkomsträttigheter till nätverks- och informationssystem i enlighet med den strategi för åtkomstkontroll som avses i punkt 11.1.

11.2.2. De berörda entiteterna ska

(a) tilldela och återkalla åtkomsträttigheter baserat på principerna om behovsenlig behörighet, begränsad behörighet och åtskillnad mellan arbetsuppgifter,

(b) säkerställa att åtkomsträttigheterna ändras vid avslutad eller ändrad anställning,

(c) säkerställa att åtkomsten till nätverks- och informationssystem auktoriseras av rätt personer,

(d) säkerställa att åtkomsträttigheterna på lämpligt sätt beaktar åtkomsten för tredje part, t.ex. besökare, leverantörer och tjänsteleverantörer, i synnerhet genom att begränsa åtkomsträttigheternas omfattning och varaktighet,

(e) föra ett register över beviljade åtkomsträttigheter,

(f) använda loggning för hanteringen av åtkomsträttigheter.

11.2.3. De berörda entiteterna ska se över åtkomsträttigheterna med planerade intervall och ändra dem baserat på organisatoriska förändringar. De berörda entiteterna ska dokumentera resultaten av översynen, inbegripet de nödvändiga ändringarna av åtkomsträttigheter.

11.3. *Privilegierade konton och systemadministrationskonton*

11.3.1. De berörda entiteterna ska upprätthålla strategier för hanteringen av konton med särskild behörighet och systemadministrationskonton som ett led i den strategi för åtkomstkontroll som avses i punkt 11.1.

11.3.2. De strategier som avses i punkt 11.3.1 ska

(a) fastställa stark identifiering, autentisering som t.ex. flerfaktorsautentisering och auktorisationsförfaranden för konton med särskild behörighet och systemadministrationskonton,

(b) skapa särskilda konton som uteslutande används för systemadministration, såsom installation, konfiguration, hantering eller underhåll,

(c) individualisera och begränsa systemadministrationsprivilegierna i största möjliga utsträckning,

(d) föreskriva att systemadministrationskonton endast får användas för anslutning till system för systemadministration.

11.3.3. De berörda entiteterna ska se över de privilegierade kontonas och systemadministrationskontonas åtkomsträttigheter med planerade intervall och ändra dem i enlighet med organisatoriska förändringar och ska dokumentera resultaten av översynen, inklusive de nödvändiga ändringarna av åtkomsträttigheter.

11.4. *Systemadministration*

11.4.1. De berörda entiteterna ska begränsa och kontrollera användningen av system för systemadministration i enlighet med den strategi för åtkomstkontroll som avses i punkt 11.1.

11.4.2. För detta ändamål ska de berörda entiteterna

(a) endast använda system för systemadministration för systemadministrativa ändamål och inte för andra åtgärder,

(b) se till att sådana system är logiskt separerade från tillämpningsprogram som inte används för systemadministrativa ändamål,

(c) skydda åtkomsten till system för systemadministration genom autentisering och kryptering.

11.5. *Identifiering*

11.5.1. De berörda entiteterna ska hantera hela identitetslivscykeln för nätverks- och informationssystem och användarna av dessa.

11.5.2. För detta ändamål ska de berörda entiteterna

(a) fastställa unika identiteter för nätverks- och informationssystem och användarna av dessa,

(b) koppla användaridentiteten till en enda person,

(c) säkerställa tillsyn över identiteterna för nätverks- och, informationssystem,

(d) använda loggning för identitetshanteringen.

11.5.3. De berörda entiteterna får endast tillåta identiteter som tilldelats flera personer, såsom delade identiteter, om dessa är nödvändiga av verksamhetsskäl eller driftsskäl och är föremål för ett förfarande för uttryckligt godkännande och dokumentation. De berörda entiteterna ska beakta identiteter som tilldelats flera personer i den riskhanteringsram för cybersäkerhet som avses i punkt 2.1.

11.5.4. De berörda entiteterna ska regelbundet se över identiteterna för nätverks- och informationssystem och användarna av dessa och utan dröjsmål avaktivera dem om de inte längre behövs.

11.6. *Autentisering*

11.6.1. De berörda entiteterna ska genomföra säkra autentiseringsförfaranden och -tekniker som baseras på åtkomstbegränsningar och strategin för åtkomstkontroll.

11.6.2. För detta ändamål ska de berörda entiteterna

(a) säkerställa att autentiseringsstyrkan är anpassad till klassificeringen av den tillgång som åtkomsten avser,

(b) kontrollera tilldelningen av hemlig autentiseringsinformation till användare och ledning genom en process som säkerställer informationens konfidentialitet, vilket innefattar råd till personalen om lämplig hantering av autentiseringsinformation,

(c) kräva att autentiseringsuppgifterna ändras initialt, med på förhand fastställda intervall och vid misstanke om att uppgifterna har komprometterats,

(d) kräva att autentiseringsuppgifterna återställs och användare blockeras efter ett på förhand fastställt antal misslyckade inloggningsförsök,

(e) avsluta inaktiva sessioner efter en på förhand fastställd period av inaktivitet, och

(f) kräva separata uppgifter för åtkomst till privilegierade konton och administrativa konton.

11.6.3. De berörda entiteterna ska i den mån det är genomförbart använda de senaste autentiseringsmetoderna, i enlighet med de relaterade bedömda riskerna och klassificeringen av den tillgång som åtkomsten avser samt unik autentiseringsinformation.

11.6.4. De berörda entiteterna ska se över autentiseringsförfarandena och autentiseringsteknikerna med planerade intervall.

11.7. *Flerfaktorsautentisering*

11.7.1. De berörda entiteterna ska säkerställa att användarna autentiseras med hjälp av flera autentiseringsfaktorer eller kontinuerliga autentiseringsmekanismer för åtkomst till de berörda entiteternas nätverks- och informationssystem, när så är lämpligt i enlighet med klassificeringen av den tillgång som åtkomsten avser.

11.7.2. De berörda entiteterna ska säkerställa att autentiseringsstyrkan är anpassad till klassificeringen av den tillgång som åtkomsten avser.

12. **Tillgångsförvaltning (artikel 21.2 i i direktiv (EU) 2022/2555)**

12.1. *Klassificering av tillgångar*

12.1.1. Vid tillämpning av artikel 21.2 i i direktiv (EU) 2022/2555 ska de berörda entiteterna fastställa klassificeringsnivåerna för alla tillgångar, inbegripet information, som omfattas av deras nätverks- och informationssystem för den skyddsnivå som krävs.

12.1.2. Vid tillämpning av punkt 12.1.1 ska de berörda entiteterna göra följande:

(a) Fastställa ett system med klassificeringsnivåer för tillgångar.

(b) Tilldela alla tillgångar en klassificeringsnivå baserat på krav avseende konfidentialitet, riktighet, autenticitet och tillgänglighet, för att ange vilket skydd som krävs mot bakgrund av tillgångarnas känslighet, kritikalitet, risk och affärsvärde.

(c) Anpassa tillgänglighetskraven för tillgångarna till de leverans- och återställningsmål som fastställs i deras driftskontinuitets- och katastrofplaner.

12.1.3. De berörda entiteterna ska genomföra regelbundna översyner av klassificeringsnivåerna för tillgångar och uppdatera dem när så är lämpligt.

12.2. *Hantering av tillgångar*

12.2.1. De berörda entiteterna ska fastställa, införa och tillämpa en strategi för korrekt hantering av tillgångar, inbegripet information, i enlighet med deras strategi för säkerhet i nätverks- och informationssystem och ska kommunicera denna strategi till alla som använder eller hanterar tillgångar.

12.2.2. Strategin ska

(a) omfatta hela livscykeln för tillgångarna, inklusive förvärv, användning, lagring, transport och bortskaffande,

(b) omfatta regler för säker användning, säker lagring, säker transport och oåterkallelig radering och förstöring av tillgångarna,

(c) föreskriva att överföringen ska ske på ett säkert sätt, i enlighet med den typ av tillgång som ska överföras.

12.2.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera strategin med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

12.3. *Strategi för flyttbara medier*

12.3.1. De berörda entiteterna ska fastställa, införa och tillämpa en strategi för hantering av flyttbara lagringsmedier och kommunicera denna till sina anställda och tredje parter som hanterar flyttbara lagringsmedier i de berörda entiteternas lokaler eller på andra platser där de flyttbara medierna är anslutna till de berörda entiteternas nätverks- och informationssystem.

12.3.2. Strategin ska

(a) omfatta ett tekniskt förbud mot anslutning av flyttbara medier om inte det finns organisatoriska skäl till att de används,

(b) föreskriva att självexekvering ska avaktiveras från sådana medier och att skanning efter skadlig kod ska ske innan de används på de berörda entiteternas system,

(c) omfatta åtgärder för kontroll och skydd av bärbara lagringsenheter som innehåller data när de är i transitering och när de lagras,

(d) när så är lämpligt, omfatta åtgärder för användning av kryptografisk teknik för att skydda data på flyttbara lagringsmedier.

12.3.3. De berörda entiteterna ska se över och, när så är lämpligt, uppdatera strategin med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

12.4. *Inventering av tillgångar*

12.4.1. De berörda entiteterna ska utveckla och upprätthålla en fullständig, tillförlitlig, uppdaterad och konsekvent inventering av sina tillgångar. De ska registrera ändringar av poster i inventeringen på ett spårbart sätt.

12.4.2. Detaljnivån för inventeringen av tillgångar bör vara anpassad till de berörda entiteternas behov. Inventeringen ska omfatta följande:

(a) En förteckning över drift och tjänster och en beskrivning av dessa.

(b) En förteckning över nätverks- och informationssystem och andra tillhörande tillgångar som stöder de berörda entiteternas drift och tjänster.

12.4.3. De berörda entiteterna ska regelbundet se över och uppdatera inventeringen och sina tillgångar och dokumentera ändringshistoriken.

12.5. *Deponering, återlämning eller radering av tillgångar när anställning upphör*

De berörda entiteterna ska fastställa, införa och tillämpa förfaranden som säkerställer att deras tillgångar som förvaras hos personal deponeras, återlämnas eller raderas när anställningen upphör och ska dokumentera deponeringen, återlämnandet och raderingen av dessa tillgångar. När det inte är möjligt med deponering, återlämnande eller radering av tillgångar ska de berörda entiteterna säkerställa att tillgångarna inte längre kan få åtkomst till de berörda entiteternas nätverks- och informationssystem i enlighet med punkt 12.2.2.

13. **Miljömässig och fysisk säkerhet (artikel 21.2 c, e och i i direktiv (EU) 2022/2555)**

13.1. *Försörjningstjänster*

13.1.1. Vid tillämpning av artikel 21.2 c i direktiv (EU) 2022/2555 ska de berörda entiteterna förhindra förlust, skada eller kompromettering av nätverks- och informationssystem eller avbrott i driften av dem på grund av fel eller avbrott i försörjningstjänster.

13.1.2. För detta ändamål ska de berörda entiteterna när så är lämpligt

(a) skydda anläggningar från strömavbrott och andra störningar som orsakas av avbrott i försörjningstjänster såsom el, telekommunikation, vattenförsörjning, gas, avlopp, ventilation och luftkonditionering,

(b) överväga användning av redundans i försörjningstjänster,

(c) skydda försörjningstjänster för el och telekommunikation som transporterar data eller används för nätverks- och informationssystem mot avläsning och skada,

(d) övervaka de försörjningstjänster som avses i led c och till behörig intern eller extern personal rapportera händelser utanför de lägsta och högsta kontrolltrösklar som avses i punkt 13.2.2 b och som påverkar försörjningstjänsterna,

(e) ingå avtal om nödförsörjning med motsvarande tjänster när det gäller t.ex. bränsle för nödkraftförsörjning,

(f) säkerställa kontinuerlig effektivitet och övervaka, underhålla och testa den försörjning som nätverks- och informationssystemen behöver för driften av de tjänster som erbjuds – i synnerhet el, reglering av temperatur och luftfuktighet, telekommunikation och internetanslutning.

13.1.3. De berörda entiteterna ska testa, se över och, när så är lämpligt, uppdatera skyddsåtgärderna regelbundet eller efter betydande incidenter eller betydande förändringar av driften eller riskerna.

13.2. *Skydd mot fysiska och miljömässiga hot*

13.2.1. Vid tillämpning av artikel 21.2 e i direktiv (EU) 2022/2555 ska de berörda entiteterna förhindra eller begränsa konsekvenserna av händelser som härrör från fysiska och miljömässiga hot, såsom naturkatastrofer och andra avsiktliga eller oavsiktliga hot, baserat på resultaten av den riskbedömning som utförts i enlighet med punkt 2.1.

13.2.2. För detta ändamål ska de berörda entiteterna när så är lämpligt

(a) utforma och genomföra skyddsåtgärder mot de fysiska och miljömässiga hoten,

(b) fastställa lägsta och högsta kontrolltrösklar för fysiska och miljömässiga hot,

(c) övervaka miljöparametrarna och till behörig intern eller extern personal rapportera händelser utanför de lägsta och högsta kontrolltrösklar som avses i led b.

13.2.3. De berörda entiteterna ska testa, se över och, när så är lämpligt, uppdatera skyddsåtgärderna mot fysiska och miljömässiga hot regelbundet eller efter betydande incidenter eller betydande förändringar av driften eller riskerna.

13.3. *Perimeterkontroll och kontroll av fysiskt tillträde*

13.3.1. Vid tillämpning av artikel 21.2 i i direktiv (EU) 2022/2555 ska de berörda entiteterna förhindra och övervaka obehörig fysiskt tillträde, skada och interferens i deras nätverks- och informationssystem.

13.3.2. För detta ändamål ska de berörda entiteterna göra följande:

(a) På grundval av den riskbedömning som utförts i enlighet med punkt 2.1 fastställa och använda säkerhetsperimetrar för att skydda områden där nätverks- och informationssystemen och andra tillhörande tillgångar är lokaliserade.

(b) Skydda de områden som avses i led a genom lämpliga inträdeskontroller och tillträdespunkter.

(c) Utforma och genomföra fysisk säkerhet för kontor, rum och anläggningar.

(d) Kontinuerligt övervaka sina lokaler för obehörig fysisk åtkomst.

13.3.3. De berörda entiteterna ska testa, se över och, när så är lämpligt, uppdatera åtgärderna för kontroll av fysiskt tillträde regelbundet eller efter betydande incidenter eller betydande ändringar av driften eller riskerna.