2024/2690

18.10.2024

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2024/2690

af 17. oktober 2024

om regler for anvendelsen af direktiv (EU) 2022/2555 for så vidt angår tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici og yderligere præcisering af de tilfælde, hvor en hændelse anses for at være væsentlig, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) ([1]), særlig artikel 21, stk. 5, første afsnit, og artikel 23, stk. 11, andet afsnit, og

ud fra følgende betragtninger:

(1) For så vidt DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester som omfattet af artikel 3 i direktiv (EU) 2022/2555 (de relevante enheder) har denne forordning til formål at fastsætte de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i artikel 21, stk. 2, i direktiv (EU) 2022/2555, og yderligere at præcisere de tilfælde, hvor en hændelse skal anses for at være væsentlig, jf. artikel 23, stk. 3, i direktiv (EU) 2022/2555.

(2) For så vidt angår tillidstjenesteudbydere bør denne forordning under hensyntagen til den grænseoverskridende karakter af disse udbyderes aktiviteter og for at sikre en sammenhængende ramme yderligere præcisere de tilfælde, hvor en hændelse skal anses for at være væsentlig, og desuden fastsætte de tekniske og metodologiske krav til foranstaltningerne til styring af cybersikkerhedsrisici.

(3) I overensstemmelse med artikel 21, stk. 5, tredje afsnit, i direktiv (EU) 2022/2555 er de tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i bilaget til denne forordning, baseret på europæiske og internationale standarder, som f.eks. ISO/IEC 27001, ISO/IEC 27002 og ETSI EN 319401, og tekniske specifikationer, som f.eks. CEN/TS 18026:2024, der er relevante for sikkerheden i net- og informationssystemer.

(4) Med hensyn til gennemførelsen og anvendelsen af de tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i bilaget til denne forordning, bør der i forbindelse med overholdelsen af disse krav i overensstemmelse med proportionalitetsprincippet tages behørigt hensyn til de relevante enheders forskellige risikoeksponering, herunder hvorvidt den pågældende enhed er af kritisk betydning, de risici, som den er eksponeret for, enhedens størrelse og struktur samt sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

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

(5) I overensstemmelse med proportionalitetsprincippet bør de relevante enheder, hvis de ikke kan gennemføre nogle af de tekniske og metodologiske krav til foranstaltningerne til styring af cybersikkerhedsrisici på grund af deres størrelse, kunne træffe andre, kompenserende foranstaltninger, der kan opfylde formålet med kravene. Når der f.eks. fastlægges roller, ansvarsområder og bemyndigelser for net- og informationssystemernes sikkerhed inden for en relevant enhed, kan mikroenheder finde det vanskeligt at adskille modstridende forpligtelser og modstridende ansvarsområder. Sådanne enheder bør kunne overveje kompenserende foranstaltninger såsom målrettet tilsyn fra enhedens ledelses side eller øget overvågning og logning.

(6) Visse tekniske og metodologiske krav i bilaget til denne forordning bør anvendes af de relevante enheder, hvor det er relevant, hvis det er relevant, eller i det omfang, det er muligt. Hvis en relevant enhed finder, at det ikke er relevant eller muligt for den at anvende visse tekniske og metodologiske krav som fastsat i bilaget til denne forordning, bør den på en forståelig måde dokumentere sin begrundelse herfor. De nationale kompetente myndigheder kan, når de fører tilsyn, tage hensyn til den tid, der er nødvendig for, at de relevante enheder kan gennemføre de tekniske og metodologiske krav til foranstaltningerne til styring af cybersikkerhedsrisici.

(7) ENISA eller de nationale kompetente myndigheder i henhold til direktiv (EU) 2022/2555 kan give vejledning for at støtte de relevante enheder i deres afdækning, analyse og vurdering af risici med henblik på at gennemføre de tekniske og metodologiske krav vedrørende etablering og opretholdelse af en passende risikostyringsramme. Denne vejledning kan navnlig omfatte nationale og sektorspecifikke risikovurderinger samt risikovurderinger, der er specifikke for en bestemt type enhed. Vejledningen kan også omfatte værktøjer eller skabeloner til udvikling af risikostyringsrammer på enhedsniveau for de relevante enheder. Rammer, vejledning eller andre mekanismer i medlemsstaternes nationale lovgivning kan også støtte de relevante enheder med hensyn til at påvise, at de overholder denne forordning Desuden kan ENISA eller de nationale kompetente myndigheder i henhold til direktiv (EU) 2022/2555 bistå de relevante enheder med at finde frem til og gennemføre passende løsninger for at behandle risici, der er afdækket i risikovurderingerne. Denne vejledning bør ikke berøre de relevante enheders forpligtelse til at afdække og dokumentere risici, der påvirker sikkerheden i net- og informationssystemer, eller de relevante enheders forpligtelse til at gennemføre de tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i bilaget til denne forordning, i overensstemmelse med deres behov og ressourcer.

(8) Netsikkerhedsforanstaltninger i forbindelse med i) overgangen til den seneste generation af kommunikationsprotokoller i netværkslaget, ii) udbredelsen af internationalt aftalte og interoperable moderne e-mailkommunikationsstandarder og iii) anvendelsen af bedste praksis for DNS-sikkerhed og for internetroutingsikkerhed og routingshygiejne medfører særlige udfordringer med hensyn til udpegelse af de bedste tilgængelige standarder og implementeringsteknikker. For at opnå et højt fælles cybersikkerhedsniveau på tværs af net så hurtigt som muligt bør Kommissionen med bistand fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og i samarbejde med de kompetente myndigheder, erhvervslivet — herunder telekommunikationsbranchen — og andre interessenter støtte udviklingen af et multiinteressentforum med den opgave at udpege de bedste tilgængelige standarder og implementeringsteknikker. Denne multiinteressentvejledning bør ikke berøre de relevante enheders forpligtelse til at gennemføre de tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i bilaget til denne forordning.

(9) I henhold til artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555 skal væsentlige og vigtige enheder ud over politikker for risikoanalyse have politikker for informationssystemsikkerhed. Med henblik herpå bør de relevante enheder fastlægge en politik for sikkerheden i net- og informationssystemer samt emnespecifikke politikker, som f.eks. politikker for adgangskontrol, som bør være i overensstemmelse med politikken for sikkerheden i net- og informationssystemer. Politikken for sikkerheden i net- og informationssystemer bør være det dokument på højeste niveau, der fastlægger de relevante enheders overordnede tilgang til sikkerheden i net- og informationssystemer, og bør godkendes af de relevante enheders ledelsesorganer. De emnespecifikke politikker bør godkendes på et passende ledelsesniveau. I politikken bør der fastsættes indikatorer og foranstaltninger med henblik på overvågning af politikkens gennemførelse og den aktuelle status for de relevante enheders modenhedsniveau for net- og informationssikkerhed, navnlig for at lette tilsynet med gennemførelsen af foranstaltningerne til styring af cybersikkerhedsrisici gennem ledelsesorganerne.

(10) Med henblik på de tekniske og metodologiske krav, der er fastsat i bilaget til denne forordning, bør begrebet »bruger« omfatte alle juridiske og fysiske personer, der har adgang til enhedens net- og informationssystemer.

(11) Med henblik på at afdække og håndtere risici, der påvirker sikkerheden i net- og informationssystemer, bør de relevante enheder etablere og opretholde en passende risikostyringsramme. Som led i risikostyringsrammen bør de relevante enheder udarbejde, gennemføre og overvåge en risikobehandlingsplan. De relevante enheder kan benytte risikobehandlingsplanen til at afdække og prioritere forskellige valgmuligheder og foranstaltninger for at behandle risici. Valgmulighederne for risikobehandling omfatter navnlig at undgå, mindske eller i exceptionelle tilfælde acceptere en risiko. Valget af en bestemt risikobehandlingsløsning bør ske under hensyntagen til resultaterne af den risikovurdering, som den relevante enhed har foretaget, og i overensstemmelse med den relevante enheds politik for sikkerheden i net- og informationssystemer. For at gennemføre de valgte risikobehandlingsløsninger bør de relevante enheder træffe passende risikobehandlingsforanstaltninger.

(12) For at opdage begivenheder, nærvedhændelser og hændelser bør de relevante enheder overvåge deres net- og informationssystemer og træffe foranstaltninger til at evaluere begivenheder, nærvedhændelser og hændelser. Disse foranstaltninger bør gøre det muligt rettidigt at opdage netbaserede angreb på grundlag af unormale indgående og udgående trafikmønstre og denial of service-angreb.

(13) Når de relevante enheder foretager en forretningskonsekvensanalyse, opfordres de til at foretage en omfattende analyse, der fastlægger, i det omfang det er relevant, den maksimale acceptable nedetid, mål for genopretningstid, mål for genopretningspunkter og mål for tjenestelevering.

(14) For at afbøde risici, der hidrører fra en relevant enheds forsyningskæde og dens forbindelser med leverandørerne, bør de relevante enheder fastlægge en politik for sikkerheden i forsyningskæden, der regulerer deres forbindelser med direkte leverandører og tjenesteudbydere. Disse enheder bør i kontrakterne med deres direkte leverandører eller tjenesteudbydere anføre passende sikkerhedsklausuler, f.eks. ved at kræve foranstaltninger til styring af cybersikkerhedsrisici i henhold til artikel 21, stk. 2, i direktiv (EU) 2022/2555 eller andre lignende retlige krav, hvor det er relevant.

(15) De relevante enheder bør regelmæssigt udføre sikkerhedstest på grundlag af en særlig politik og særlige procedurer for at kontrollere, om foranstaltningerne til styring af cybersikkerhedsrisici er gennemført og fungerer korrekt. Der kan udføres sikkerhedstest af specifikke net- og informationssystemer eller af den relevante enhed som helhed, og testene kan omfatte automatiserede eller manuelle test, penetrationstest, sårbarhedsscanning, statiske og dynamiske applikationssikkerhedstest, konfigurationstest eller sikkerhedsaudits. De relevante enheder kan udføre sikkerhedstest af deres net- og informationssystemer ved etableringen, efter opgraderinger af infrastruktur eller applikationer eller ændringer, som de anser for væsentlige, eller efter vedligeholdelse. Resultaterne af sikkerhedstestene bør danne grundlag for de relevante enheders politik for og procedurer til at vurdere, hvor effektive foranstaltningerne til styring af cybersikkerhedsrisici er, samt for uafhængige gennemgange af enhedernes net- og informationssikkerhedspolitik.

(16) For at undgå væsentlige forstyrrelser og skader forårsaget af udnyttelse af uafhjulpne sårbarheder i net- og informationssystemer bør de relevante enheder fastlægge og anvende passende procedurer for sikkerhedspatchstyring, som er i overensstemmelse med de relevante enheders ændringsstyring, sårbarhedsstyring, risikostyring og andre relevante procedurer. De relevante enheder bør træffe foranstaltninger, der står i et rimeligt forhold til deres ressourcer, for at sikre, at sikkerhedspatches ikke medfører yderligere sårbarheder eller ustabilitet. I tilfælde af planlagt utilgængelighed af en tjeneste som følge af anvendelse af sikkerhedspatches opfordres de relevante enheder til at informere kunderne behørigt på forhånd.

(17) De relevante enheder bør styre de risici, der hidrører fra erhvervelse af IKT-produkter eller -tjenester fra leverandører eller tjenesteudbydere, og bør opnå sikkerhed for, at de IKT-produkter eller -tjenester, der skal erhverves, opfylder visse cybersikkerhedsbeskyttelsesniveauer, f.eks. ved hjælp af europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer for IKT-produkter og -tjenester, der er udstedt i henhold til en europæisk cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([2]). Hvis de relevante enheder fastsætter sikkerhedskrav, der skal gælde for de IKT-produkter, der skal erhverves, bør de tage hensyn til de væsentlige cybersikkerhedskrav, der er fastsat i en EU-forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer.

(18) For at beskytte mod cybertrusler og støtte forebyggelse og inddæmning af brud på datasikkerheden bør de relevante enheder gennemføre netsikkerhedsløsninger. Typiske netsikkerhedsløsninger omfatter anvendelse af firewalls til at beskytte de relevante enheders interne net, begrænsning af tilslutninger og adgang til tjenester til tilfælde, hvor tilslutning og adgang er absolut nødvendigt, og anvendelse af virtuelle private net til fjernadgang og for kun at tillade, at tjenesteudbydere tilslutter sig efter at have anmodet herom og i en bestemt periode, f.eks. den tid, en vedligeholdelsesaktivitet varer.

(19) De relevante enheder bør for at beskytte deres net og deres informationssystemer mod skadelig og uautoriseret software indføre kontroller, der forhindrer eller opdager brugen af uautoriseret software, og bør, i det omfang det er relevant, anvende detection and response-software. De relevante enheder bør også overveje at gennemføre foranstaltninger til at minimere angrebsfladen, mindske sårbarheder, der kan udnyttes af angribere, kontrollere eksekveringen af applikationer i endepunkter og indføre e-mail- og webapplikationsfiltre for at mindske eksponeringen for skadeligt indhold.

(20) I henhold til artikel 21, stk. 2, litra g), i direktiv (EU) 2022/2555 skal medlemsstaterne sikre, at væsentlige og vigtige enheder anvender grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse. Grundlæggende cyberhygiejnepraksisser kan omfatte zero trust-principper, softwareopdateringer, enhedskonfiguration, netværkssegmentering, identitets- og adgangsstyring eller brugerbevidsthed, personalekurser og oplysning om cybertrusler, phishing og social engineering-teknikker. Cyberhygiejnepraksisser er en del af forskellige tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i bilaget til denne forordning. Med hensyn til grundlæggende cyberhygiejnepraksisser for brugere bør de relevante enheder overveje praksisser såsom en politik om et ryddet skrivebord og en ryddet skærm, anvendelse af multifaktor- og andre godkendelsesmetoder, sikker brug af e-mail og webbrowsing, beskyttelse mod phishing og social engineering og sikre fjernarbejdspraksisser.

(21) De relevante enheder bør fastlægge og indføre en emnespecifik politik vedrørende adgang for personer og net- og informationssystemer, som f.eks. applikationer, for at forhindre uautoriseret adgang til deres aktiver.

(22) For at undgå, at ansatte kan misbruge f.eks. deres adgangsrettigheder i en relevant enhed til at forårsage skade, bør de relevante enheder overveje passende foranstaltninger til personalesikkerhedsstyring og højne de ansattes bevidsthed om sådanne risici. De relevante enheder bør indføre, oplyse om og vedligeholde en disciplinærprocedure for at håndtere overtrædelser af deres sikkerhedspolitik for net- og informationssystemer, som kan indgå i andre disciplinærprocedurer, som de relevante enheder har indført. Baggrundskontrol af de relevante enheders ansatte og, hvor det er relevant, direkte leverandører og tjenesteudbydere, bør bidrage til målet om personalesikkerhed i de relevante enheder og kan omfatte foranstaltninger som f.eks. kontrol af en persons straffeattest eller tidligere arbejdsopgaver, alt efter hvad der er relevant for vedkommendes opgaver i den relevante enhed og i overensstemmelse med den relevante enheds politik for sikkerheden i net- og informationssystemer.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) Multifaktorgodkendelse kan forbedre enhedernes cybersikkerhed og bør tages i betragtning af enhederne, navnlig når brugerne tilgår net- og informationssystemer fra fjerntliggende lokationer, eller når de tilgår følsomme oplysninger eller privilegerede konti og systemadministrationskonti. Multifaktorgodkendelse kan kombineres med andre teknikker for at kræve flere faktorer under særlige omstændigheder på grundlag af foruddefinerede regler og mønstre, som f.eks. adgang fra en usædvanlig lokation, fra en usædvanlig enhed eller på et usædvanligt tidspunkt.

(24) De relevante enheder bør forvalte og beskytte de aktiver, der har værdi for dem, gennem en forsvarlig forvaltning af aktiver, som også bør danne grundlag for risikoanalysen og styringen af driftskontinuiteten. De relevante enheder bør forvalte både materielle og immaterielle aktiver og bør oprette en fortegnelse over aktiverne, tildele aktiverne en defineret klassifikationsgrad, håndtere og spore aktiverne og tage skridt til at beskytte aktiverne i hele deres livscyklus.

(25) Forvaltningen af aktiver bør omfatte at klassificere aktiver efter type, følsomhed, risikoniveau og sikkerhedskrav og at anvende passende foranstaltninger og kontroller for at sikre deres tilgængelighed, integritet, fortrolighed og autenticitet. Ved at klassificere aktiver efter risikoniveau bør de relevante enheder kunne anvende passende sikkerhedsforanstaltninger og -kontroller for at beskytte aktiverne, som f.eks. kryptering, adgangskontrol, herunder perimeterkontrol og fysisk og logisk adgangskontrol, sikkerhedskopier, logning og overvågning, lagring og bortskaffelse. Når de relevante enheder foretager en forretningskonsekvensanalyse, kan de bestemme klassifikationsgraden på grundlag af konsekvenserne for enheden, hvis aktiverne forstyrres. Alle ansatte, der håndterer aktiver, i enhederne bør være bekendt med politikkerne for og instrukserne om håndtering af aktiver.

(26) Detaljeringsgraden af fortegnelsen over aktiver bør modsvare de relevante enheders behov. En omfattende fortegnelse over aktiver kan for hvert aktiv som minimum omfatte en entydig identifikator, aktivets ejer, en beskrivelse af aktivet, aktivets lokation, aktivets type, typen og klassificeringen af de oplysninger, der behandles i aktivet, datoen for den seneste opdatering af eller patch til aktivet, klassificeringen af aktivet i risikovurderingen, og hvornår aktivets livscyklus ender. Når et aktivs ejer identificeres, bør de relevante enheder også identificere den person, der er ansvarlig for at beskytte det pågældende aktiv.

(27) Tildelingen og tilrettelæggelsen af cybersikkerhedsmæssige roller, ansvarsområder og bemyndigelser bør etablere en konsekvent struktur for styring og gennemførelse af cybersikkerhed i de relevante enheder og sikre effektiv kommunikation i tilfælde af hændelser. Ved fastlæggelsen og tildelingen af ansvarsområder for bestemte roller bør de relevante enheder tage roller såsom chef for informationssikkerhed, informationssikkerhedsansvarlig, ansvarlig for håndtering af hændelser, revisor eller tilsvarende i betragtning. De relevante enheder kan tildele roller og ansvarsområder til eksterne parter, som f.eks. tredjepartsudbydere af IKT-tjenester.

(28) I henhold til artikel 21, stk. 2, i direktiv (EU) 2022/2555 skal foranstaltninger til styring af cybersikkerhedsrisici baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser såsom tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt, eller uautoriseret fysisk adgang til, beskadigelse af eller indgreb i en væsentlig eller vigtig enheds informations- og informationsbehandlingsfaciliteter, som kan kompromittere tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer. De tekniske og metodologiske krav til foranstaltningerne til styring af cybersikkerhedsrisici bør derfor også omhandle net- og informationssystemernes fysiske og miljømæssige sikkerhed ved også at omfatte foranstaltninger til at beskytte sådanne systemer mod systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener. Andre eksempler på fysiske og miljømæssige trusler kan omfatte jordskælv, eksplosioner, sabotage, insidertrusler, civil uro, giftigt affald og miljøemissioner. Forebyggelse af tab, beskadigelse eller kompromittering af net- og informationssystemer eller afbrydelse af deres drift som følge af svigt og afbrydelse af den understøttende forsyning bør bidrage til målet om driftskontinuitet i de relevante enheder. Desuden bør beskyttelse mod fysiske og miljømæssige trusler bidrage til sikkerheden i forbindelse med vedligeholdelse af net- og informationssystemer i de relevante enheder.

(29) De relevante enheder bør udforme og gennemføre beskyttelsesforanstaltninger mod fysiske og miljømæssige trusler og fastsætte minimums- og maksimumskontroltærskler for fysiske og miljømæssige trusler og overvåge miljøparametre. De bør f.eks. overveje at installere systemer til på et tidligt tidspunkt at opdage oversvømmelser i områder, hvor net- og informationssystemer er placeret. Med hensyn til brandfare bør de relevante enheder overveje at oprette en separat brandcelle til datacentret, anvende brandhæmmende materialer og sensorer til overvågning af temperatur og fugtighed, tilslutte bygningen til et brandalarmsystem med automatisk underretning af det lokale brandvæsen samt anvende anlæg til tidlig brandopdagelse og -slukning. De relevante enheder bør også foretage regelmæssige brandøvelser og brandinspektioner. For at sikre strømforsyningen bør de relevante enheder desuden overveje overspændingsbeskyttelse og tilsvarende nødstrømforsyning i overensstemmelse med de relevante standarder. Da overophedning udgør en risiko med hensyn til tilgængeligheden af net- og informationssystemer, kan de relevante enheder, navnlig udbydere af datacentertjenester, desuden overveje tilstrækkelige og kontinuerlige klimaanlæg med redundans.

(30) Denne forordning skal yderligere præcisere de tilfælde, hvor en hændelse skal anses for at være væsentlig med henblik på artikel 23, stk. 3, i direktiv (EU) 2022/2555. Kriterierne bør være af en sådan art, at de relevante enheder er i stand til at vurdere, om en hændelse er væsentlig, med henblik på at underrette om hændelsen i overensstemmelse med direktiv (EU) 2022/2555. Kriterierne i denne forordning bør desuden betragtes som udtømmende, jf. dog artikel 5 i direktiv (EU) 2022/2555. I denne forordning præciseres de tilfælde, hvor en hændelse skal anses for at være væsentlig, idet der fastlægges horisontale og enhedstypespecifikke tilfælde.

(31) I henhold til artikel 23, stk. 4, i direktiv (EU) 2022/2555 skal relevante enheder være forpligtede til at underrette om væsentlige hændelser inden for de frister, der er fastsat i nævnte bestemmelse. Disse underretningsfrister løber fra det tidspunkt, hvor enheden får kendskab til den væsentlige hændelse. Den relevante enhed er derfor forpligtet til at indberette hændelser, der ud fra den pågældende enheds indledende vurdering kan forårsage alvorlige driftsmæssige forstyrrelser af enhedens tjenester eller forårsage økonomiske tab for enheden eller påvirke andre fysiske eller juridiske personer ved at forvolde dem betydelig materiel eller immateriel skade. Når en relevant enhed har opdaget en mistænkelig begivenhed, eller er blevet gjort opmærksom på en potentiel hændelse af en tredjepart, som f.eks. en enkeltperson, en kunde, en enhed, en myndighed, en medieorganisation eller en anden kilde, bør den relevante enhed derfor rettidigt vurdere den mistænkelige begivenhed for at vurdere, om der er tale om en hændelse, og i så fald fastslå dens art og alvor. Den relevante enhed skal derfor anses for at have fået »kendskab« til den væsentlige hændelse, når den efter en sådan indledende vurdering har en rimelig grad af sikkerhed for, at der er indtruffet en væsentlig hændelse.

(32) Med henblik på at fastslå, om en hændelse er væsentlig, bør de relevante enheder, hvis det er relevant, tælle antallet af brugere, der er påvirket af hændelsen, under hensyntagen til de erhvervs- og slutkunder, som de relevante enheder har et kontraktforhold med, samt fysiske og juridiske personer med tilknytning til erhvervskunder. Hvis en relevant enhed ikke er i stand til at beregne antallet af berørte brugere, bør den relevante enheds skøn over det mulige maksimale antal berørte brugere tages i betragtning i beregningen af det samlede antal brugere, der er påvirket af hændelsen. Betydningen af en hændelse, der involverer en tillidstjeneste, bør ikke kun bestemmes af antallet af brugere, men også af antallet af tilknyttede parter, da disse også kan blive berørt af en væsentlig hændelse, der involverer en tillidstjeneste, for så vidt angår driftsforstyrrelser og materiel eller immateriel skade. Tillidstjeneste-udbydere bør derfor, hvis det er relevant, også tage antallet af tilknyttede parter i betragtning, når de vurderer, om en hændelse er væsentlig. Med henblik herpå bør tilknyttede parter forstås som fysiske eller juridiske personer, der er afhængige af en tillidstjeneste.

(33) Vedligeholdelsesarbejde, der resulterer i en begrænset tilgængelighed af tjenesterne, eller at tjenesterne er utilgængelige, bør ikke betragtes som væsentlige hændelser, hvis den begrænsede tilgængelighed eller utilgængeligheden af tjenesten sker i overensstemmelse med planlagt vedligeholdelsesarbejde. Desuden bør det ikke betragtes som en væsentlig hændelse, at en tjeneste er utilgængelig på grund af planlagte afbrydelser, som f.eks. afbrydelser eller utilgængelighed som følge af en forudindgået kontraktlig aftale.

(34) Varigheden af en hændelse, der påvirker en tjenestes tilgængelighed, bør måles fra forstyrrelsen af den korrekte levering af tjenesten til genopretningstidspunktet. Hvis en relevant enhed ikke er i stand til at fastslå, hvornår forstyrrelsen indtraf, bør hændelsens varighed måles fra det tidspunkt, hvor hændelsen blev opdaget, eller fra det tidspunkt, hvor hændelsen blev registreret i net- eller systemlogfiler eller andre datakilder, alt efter hvad der indtraf først.

(35) Fuldstændig utilgængelighed af en tjeneste bør måles fra det tidspunkt, hvor tjenesten er helt utilgængelig for brugerne, til det tidspunkt, hvor regelmæssige aktiviteter eller regelmæssig drift genoprettes til det serviceniveau, der blev leveret forud for hændelsen. Hvis en relevant enhed ikke er i stand til at fastslå, hvornår den fuldstændige utilgængelighed af en tjeneste indtraf, bør utilgængeligheden måles fra det tidspunkt, hvor den pågældende enhed opdagede den.

(36) Med henblik på at fastslå de direkte økonomiske tab som følge af en hændelse bør de relevante enheder tage hensyn til alle de finansielle tab, som de har lidt som følge af hændelsen, som f.eks. omkostninger til udskiftning eller flytning af software, hardware eller infrastruktur, personaleomkostninger, herunder omkostninger i forbindelse med udskiftning eller flytning af personale, ansættelse af ekstra personale, aflønning af overarbejde og genopretning af mistede eller forringede færdigheder, gebyrer som følge af manglende overholdelse af kontraktlige forpligtelser, omkostninger i forbindelse med klager og kompensation til kunder, tab som følge af mistede indtægter, omkostninger i forbindelse med intern og ekstern kommunikation, rådgivningsomkostninger, herunder omkostninger i forbindelse med juridisk rådgivning, kriminaltekniske tjenester, oprydningstjenester og andre omkostninger i forbindelse med hændelsen. Administrative bøder samt omkostninger, der er nødvendige for virksomhedens daglige drift, bør imidlertid ikke betragtes som økonomiske tab som følge af en hændelse, herunder omkostninger til almindelig vedligeholdelse af infrastruktur, udstyr, hardware og software, ajourføring af personalets færdigheder, interne og eksterne omkostninger i forbindelse med forbedring af virksomheden efter hændelsen, herunder opgraderinger, forbedringer og risikovurderingsinitiativer, og forsikringspræmier. De relevante enheder bør beregne størrelsen af de økonomiske tab på grundlag af de tilgængelige data, og hvis de faktiske økonomiske tab ikke kan fastslås, bør enhederne anslå beløbene.

(37) De relevante enheder bør også være forpligtede til at indberette hændelser, der har forårsaget eller er i stand til at forårsage fysiske personers død eller betydelig skade på fysiske personers helbred, da sådanne hændelser udgør særlig alvorlige tilfælde af materiel eller immateriel skadeforvoldelse. F.eks. kan en hændelse, der påvirker en relevant enhed, forårsage, at sundhedsydelser eller beredskabstjenester er utilgængelige, eller forårsage tab af datafortrolighed eller -integritet, der har indvirkning på fysiske personers helbred. For at fastslå, om en hændelse har forårsaget eller kan forårsage betydelig skade på en fysisk persons helbred, bør de relevante enheder tage i betragtning, om hændelsen har forårsaget eller kan forårsage alvorlige skader og dårligt helbred. Med henblik herpå bør de relevante enheder ikke være forpligtede til at indsamle yderligere oplysninger, som de ikke har adgang til.

(38) Det bør navnlig betragtes som begrænset tilgængelighed, når en tjeneste, der leveres af en relevant enhed, er betydeligt langsommere end den gennemsnitlige svartid, eller hvis ikke alle en tjenestes funktionaliteter er tilgængelige. Hvis det er muligt, bør der til at vurdere forsinkelser i svartiden anvendes objektive kriterier baseret på de gennemsnitlige svartider for de tjenester, der leveres af de relevante enheder. En funktionalitet hos en tjeneste kan f.eks. være en chatfunktion eller en billedsøgefunktion.

(39) Hvis der opnås formodet ondsindet og uautoriseret adgang til en relevant enheds net- og informationssystemer, bør det betragtes som en væsentlig hændelse, hvis denne adgang kan forårsage alvorlige driftsforstyrrelser. Hvis en cybertrusselsaktør f.eks. forlods placerer sig i en relevant enheds net- og informationssystemer med den hensigt at forårsage forstyrrelser af tjenester i fremtiden, bør hændelsen anses for at være væsentlig.

(40) Tilbagevendende hændelser, der er forbundet via den samme åbenlyse grundlæggende årsag, og som ikke hver for sig opfylder kriterierne for en væsentlig hændelse, bør samlet anses for at være en væsentlig hændelse, forudsat at de tilsammen opfylder kriteriet for økonomisk tab, og hvis de er indtruffet mindst to gange inden for seks måneder. Sådanne tilbagevendende hændelser kan indikere væsentlige mangler og svagheder i den relevante enheds procedurer for styring af cybersikkerhedsrisici og modenhedsniveau for cybersikkerhed. Desuden er sådanne tilbagevendende hændelser i stand til at forårsage betydelige økonomiske tab for den relevante enhed.

(41) Kommissionen har udvekslet rådgivning og samarbejdet med samarbejdsgruppen og ENISA om udkastene til gennemførelsesretsakter i overensstemmelse med artikel 21, stk. 5, og artikel 23, stk. 11, i direktiv (EU) 2022/2555.

(42) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([3]) og afgav udtalelse den 1. september 2024.

(43) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 39 i direktiv (EU) 2022/2555 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

For så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester (de relevante enheder) fastsættes ved denne forordning de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i artikel 21, stk. 2, i direktiv (EU) 2022/2555, og de tilfælde, hvor en hændelse skal anses for at være væsentlig, jf. artikel 23, stk. 3, i direktiv (EU) 2022/2555, præciseres yderligere.

Artikel 2

Tekniske og metodologiske krav

1. For de relevante enheder er de tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici som omhandlet i artikel 21, stk. 2, litra a)-j), i direktiv (EU) 2022/2555 fastsat i bilaget til denne forordning.

2. De relevante enheder sikrer et i forhold til risiciene passende niveau af sikkerhed i net- og informationssystemer, når de gennemfører og anvender de tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i bilaget til denne forordning. Med henblik herpå tager de relevante enheder behørigt hensyn til graden af deres eksponering for risici, deres størrelse samt sandsynligheden for hændelser og disses alvor, herunder deres samfundsmæssige og økonomiske indvirkning, i forbindelse med overholdelsen af de tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici, der er fastsat i bilaget til denne forordning.

([3]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Hvis det i bilaget til denne forordning fastsættes, at et teknisk eller metodologisk krav til en foranstaltning til styring af cybersikkerhedsrisici skal anvendes »hvor det er relevant«, »hvis det er relevant« eller »i det omfang, det er muligt«, og hvis en relevant enhed finder, at det ikke er relevant eller muligt for den relevante enhed at anvende visse af disse tekniske og metodologiske krav, dokumenterer den relevante enhed på en forståelig måde sin begrundelse herfor.

Artikel 3

Væsentlige hændelser

1. En hændelse anses for at være væsentlig i henhold til artikel 23, stk. 3, i direktiv (EU) 2022/2555 for så vidt angår de relevante enheder, hvis et eller flere af følgende kriterier er opfyldt:

a) hændelsen har forårsaget eller er i stand til at forårsage direkte økonomiske tab for den relevante enhed, som overstiger 500 000 EUR eller 5 % af den relevante enheds samlede årsomsætning i det foregående regnskabsår, alt efter hvad der er lavest

b) hændelsen har forårsaget eller er i stand til at forårsage afsløring af den relevante enheds forretningshemmeligheder som defineret i artikel 2, nr. 1), i direktiv (EU) 2016/943

c) hændelsen har forårsaget eller er i stand til at forårsage en fysisk persons død

d) hændelsen har forårsaget eller er i stand til at forårsage betydelig skade på en fysisk persons helbred

e) der er opnået formodet ondsindet og uautoriseret adgang til net- og informationssystemer, hvilket kan forårsage alvorlige driftsforstyrrelser

f) hændelsen opfylder kriterierne i artikel 4

g) hændelsen opfylder et eller flere af kriterierne i artikel 5-14.

2. Planlagte driftsafbrydelser og forventede konsekvenser af planlagt vedligeholdelsesarbejde, der udføres af eller på vegne af de relevante enheder, anses ikke for at være væsentlige hændelser.

3. Ved beregningen af, hvor mange brugere der er påvirket af en hændelse, med henblik på artikel 7 og 9-14, tager de relevante enheder hensyn til følgende:

a) antallet af kunder, der har en kontrakt med den relevante enhed, som giver dem adgang til den relevante enheds net- og informationssystemer eller tjenester, der tilbydes eller er tilgængelige gennem disse net- og informationssystemer

b) antallet af fysiske og juridiske personer med tilknytning til erhvervskunder, der anvender enhedernes net- og informationssystemer eller tjenester, der tilbydes eller er tilgængelige gennem disse net- og informationssystemer.

Artikel 4

Tilbagevendende hændelser

Hændelser, der hver for sig ikke anses for at være væsentlige hændelser, jf. artikel 3, anses samlet for at være én væsentlig hændelse, hvis de opfylder alle følgende kriterier:

a) de er indtruffet mindst to gange inden for seks måneder

b) de har samme åbenlyse grundlæggende årsag

c) de opfylder samlet set kriterierne i artikel 3, stk. 1, litra a).

Artikel 5

Væsentlige hændelser for så vidt angår DNS-tjenesteudbydere

For så vidt angår DNS-tjenesteudbydere anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en rekursiv eller autoritativ domænenavnsoversættelsestjeneste er fuldstændig utilgængelig i mere end 30 minutter

b) i en periode på mindst en time er en rekursiv eller autoritativ domænenavnsoversættelsestjenestes gennemsnitlige svartid for DNS-anmodninger mere end 10 sekunder

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende leveringen af den autoritative domænenavnsoversættelsestjeneste er bragt i fare, undtagen i tilfælde, hvor data om mindre end 1 000 domænenavne, der forvaltes af DNS-tjenesteudbyderen, hvilket højst må udgøre 1 % af de domænenavne, der forvaltes af DNS-tjenesteudbyderen, er ukorrekte på grund af fejlkonfiguration.

Artikel 6

Væsentlige hændelser for så vidt angår topdomænenavneadministratorer

For så vidt angår topdomænenavneadministratorer anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en autoritativ domænenavnsoversættelsestjeneste er fuldstændig utilgængelig

b) i en periode på mindst en time er en autoritativ domænenavnsoversættelsestjenestes gennemsnitlige svartid for DNS-anmodninger mere end 10 sekunder

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende den tekniske drift af topdomænet er bragt i fare.

Artikel 7

Væsentlige hændelser for så vidt angår udbydere af cloudcomputingtjenester

For så vidt angår udbydere af cloudcomputingtjenester anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en leveret cloudcomputingtjeneste er fuldstændig utilgængelig i mere end 30 minutter

b) tilgængeligheden af en udbyders cloudcomputingtjeneste er begrænset for mere end 5 % af brugerne af cloudcomputingtjenesten i Unionen eller for mere end 1 mio. brugere af cloudcomputingtjenesten i Unionen, alt efter hvilket tal der er lavest, i en periode på mindst en time

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende leveringen af en cloudcomputingtjeneste er bragt i fare som følge af en formodet ondsindet handling

d) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende leveringen af en cloudcomputingtjeneste er bragt i fare i et omfang, der påvirker mere end 5 % af brugerne af cloudcomputingtjenesten i Unionen eller mere end 1 mio. brugere af cloudcomputingtjenesten i Unionen, alt efter hvilket tal der er lavest.

Artikel 8

Væsentlige hændelser for så vidt angår udbydere af datacentertjenester

For så vidt angår udbydere af datacentertjenester anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en datacentertjeneste fra et datacenter, der drives af udbyderen, er fuldstændig utilgængelig

b) tilgængeligheden af en datacentertjeneste fra et datacenter, der drives af udbyderen, er begrænset i en periode på mindst en time

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende leveringen af en datacentertjeneste er bragt i fare som følge af en formodet ondsindet handling

d) den fysiske adgang til et datacenter, der drives af udbyderen, er bragt i fare.

Artikel 9

Væsentlige hændelser for så vidt angår udbydere af indholdsleveringsnetværk

For så vidt angår udbydere af indholdsleveringsnetværk anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) et indholdsleveringsnetværk er fuldstændig utilgængeligt i mere end 30 minutter

b) tilgængeligheden af et indholdsleveringsnetværk er begrænset for mere end 5 % af brugerne af indholdsleveringsnetværket i Unionen eller for mere end 1 mio. brugere af indholdsleveringsnetværket i Unionen, alt efter hvilket tal der er lavest, i en periode på mindst en time

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende et indholdsleveringsnetværks levering er bragt i fare som følge af en formodet ondsindet handling

d) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende et indholdsleveringsnetværks levering er bragt i fare i et omfang, der påvirker mere end 5 % af brugerne af indholdsleveringsnetværket i Unionen eller mere end 1 mio. brugere af indholdsleveringsnetværket i Unionen, alt efter hvilket tal der er lavest.

Artikel 10

Væsentlige hændelser for så vidt angår udbydere af administrerede tjenester og udbydere af administrerede sikkerhedstjenester

For så vidt angår udbydere af administrerede tjenester og udbydere af administrerede sikkerhedstjenester anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en administreret tjeneste eller administreret sikkerhedstjeneste er fuldstændig utilgængelig i mere end 30 minutter

b) tilgængeligheden af en administreret tjeneste eller administreret sikkerhedstjeneste er begrænset for mere end 5 % af brugerne af tjenesten i Unionen eller for mere end 1 mio. brugere af tjenesten i Unionen, alt efter hvilket tal der er lavest, i en periode på mindst en time

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende leveringen af en administreret tjeneste eller administreret sikkerhedstjeneste er bragt i fare som følge af en formodet ondsindet handling

d) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende leveringen af en administreret tjeneste eller en administreret sikkerhedstjeneste er bragt i fare i et omfang, der påvirker mere end 5 % af brugerne af den administrerede tjeneste eller den administrerede sikkerhedstjeneste i Unionen eller mere end 1 mio. brugere af tjenesten i Unionen, alt efter hvilket tal der er lavest.

Artikel 11

Væsentlige hændelser for så vidt angår udbydere af onlinemarkedspladser

For så vidt angår udbydere af onlinemarkedspladser anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en onlinemarkedsplads er fuldstændig utilgængelig for mere end 5 % af brugerne af onlinemarkedspladsen i Unionen eller for mere end 1 mio. brugere af onlinemarkedspladsen i Unionen, alt efter hvilket tal der er lavest

b) mere end 5 % af brugerne af en onlinemarkedsplads i Unionen eller mere end 1 mio. brugere af en onlinemarkedsplads i Unionen, alt efter hvilket tal der er lavest, er påvirket af en begrænset tilgængelighed af onlinemarkedspladsen

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende en onlinemarkedsplads' levering er bragt i fare som følge af en formodet ondsindet handling

d) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende en onlinemarkedsplads' levering er bragt i fare i et omfang, der påvirker mere end 5 % af brugerne af onlinemarkedspladsen i Unionen eller mere end 1 mio. brugere af onlinemarkedspladsen i Unionen, alt efter hvilket tal der er lavest.

Artikel 12

Væsentlige hændelser for så vidt angår udbydere af onlinesøgemaskiner

For så vidt angår udbydere af onlinesøgemaskiner anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en onlinesøgemaskine er fuldstændig utilgængelig for mere end 5 % af brugerne af onlinesøgemaskinen i Unionen eller for mere end 1 mio. brugere af onlinesøgemaskinen i Unionen, alt efter hvilket tal der er lavest

b) mere end 5 % af brugerne af en onlinesøgemaskine i Unionen eller mere end 1 mio. brugere af en onlinesøgemaskine i Unionen, alt efter hvilket tal der er lavest, er påvirket af en begrænset tilgængelighed af onlinesøgemaskinen

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende en onlinesøgemaskines levering er bragt i fare som følge af en formodet ondsindet handling

d) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende en onlinesøgemaskines levering er bragt i fare i et omfang, der påvirker mere end 5 % af brugerne af onlinesøgemaskinen i Unionen eller mere end 1 mio. brugere af onlinesøgemaskinen i Unionen, alt efter hvilket tal der er lavest.

Artikel 13

Væsentlige hændelser for så vidt angår udbydere af platforme for sociale netværkstjenester

For så vidt angår udbydere af platforme for sociale netværkstjenester anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en platform for sociale netværkstjenester er fuldstændig utilgængelig for mere end 5 % af brugerne af platformen for sociale netværkstjenester i Unionen eller for mere end 1 mio. brugere af platformen for sociale netværkstjenester i Unionen, alt efter hvilket tal der er lavest

b) mere end 5 % af brugerne af en platform for sociale netværkstjenester i Unionen eller mere end 1 mio. brugere af en platform for sociale netværkstjenester i Unionen, alt efter hvilket tal der er lavest, er påvirket af en begrænset tilgængelighed af platformen for sociale netværkstjenester

c) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende en platform for sociale netværkstjenesters levering er bragt i fare som følge af en formodet ondsindet handling

d) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende en platform for sociale netværkstjenesters levering er bragt i fare i et omfang, der påvirker mere end 5 % af brugerne af platformen for sociale netværkstjenester i Unionen eller mere end 1 mio. brugere af platformen for sociale netværkstjenester i Unionen, alt efter hvilket tal der er lavest.

Artikel 14

Væsentlige hændelser for så vidt angår tillidstjenesteudbydere

For så vidt angår tillidstjenesteudbydere anses en hændelse for at være væsentlig i henhold til artikel 3, stk. 1, litra g), når den opfylder et eller flere af følgende kriterier:

a) en tillidstjeneste er fuldstændig utilgængelig i mere end 20 minutter

b) en tillidstjeneste er utilgængelig for brugere eller tilknyttede parter i mere end en time beregnet på kalenderugebasis

c) mere end 1 % af brugerne eller de tilknyttede parter i Unionen eller mere end 200 000 brugere eller tilknyttede parter i Unionen, alt efter hvilket tal der er lavest, er påvirket af en begrænset tilgængelighed af en tillidstjeneste

d) den fysiske adgang til et område, hvor net- og informationssystemer er placeret, og hvortil adgangen er begrænset til tillidstjenesteudbyderens betroede personale, eller beskyttelsen af denne fysiske adgang, er bragt i fare

e) integriteten, fortroligheden eller autenticiteten af lagrede, overførte eller behandlede data vedrørende leveringen af en tillidstjeneste er bragt i fare i et omfang, der påvirker mere end 0,1 % af brugerne af tillidstjenesten eller de tilknyttede parter i Unionen eller mere end 100 brugere af tillidstjenesten eller tilknyttede parter i Unionen, alt efter hvilket tal der er lavest.

Artikel 15

Ophævelse

Kommissionens gennemførelsesforordning (EU) 2018/151 ([4]) ophæves.

Artikel 16

Ikrafttræden og anvendelse

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 17. oktober 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([4]) Kommissionens gennemførelsesforordning (EU) 2018/151 af 30. januar 2018 om regler for anvendelsen af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 for så vidt angår yderligere specifikation af de elementer, som udbydere af digitale tjenester skal tage i betragtning for at styre risiciene i forhold til sikkerheden i net- og informationssystemer, og af kriterierne for bestemmelse af, om en hændelses konsekvenser er betydelige (EUT L 26 af 31.1.2018, s. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

BILAG

Tekniske og metodologiske krav, jf. denne forordnings artikel 2

1. **Politik for sikkerheden i net- og informationssystemer (artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555)**

1.1. *Politik for sikkerheden i net- og informationssystemer*

1.1.1. Med henblik på artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555 skal politikken for sikkerhed i net- og informationssystemer:

(a) fastsætte de relevante enheders tilgang til styring af sikkerheden i deres net- og informationssystemer

(b) være passende i forhold til og supplere de relevante enheders forretningsstrategi og -mål

(c) fastsætte net- og informationssikkerhedsmål

(d) omfatte en forpligtelse til løbende at forbedre sikkerheden i net- og informationssystemer

(e) omfatte en forpligtelse til at stille de nødvendige ressourcer til rådighed til dens gennemførelse, herunder det nødvendige personale, de nødvendige finansielle ressourcer, samt de nødvendige processer, værktøjer og teknologier

(f) meddeles til og anerkendes af relevante medarbejdere og relevante interesserede eksterne parter

(g) fastsætte roller og ansvarsområder i henhold til punkt 1.2

(h) omfatte en liste over den dokumentation, der skal opbevares, og en angivelse af, hvor længe denne dokumentation skal opbevares

(i) omfatte en liste over emnespecifikke politikker

(j) fastsætte indikatorer og foranstaltninger til overvågning af politikkens gennemførelse og den aktuelle status for modenheden af de relevante enheders net- og informationssikkerhed

(k) omfatte en angivelse af datoen for ledelsesorganernes formelle godkendelse af de relevante enheder ("ledelsesorganerne").

1.1.2. Ledelsesorganerne gennemgår og, hvis det er relevant, ajourfører politikken for sikkerheden i net- og informationssystemer mindst én gang om året, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici. Resultatet af hver gennemgang skal dokumenteres.

1.2. *Roller, ansvarsområder og bemyndigelser*

1.2.1. De relevante enheder fastlægger som led i deres sikkerhedspolitik for net- og informationssystemer, jf. punkt 1.1, ansvarsområder og bemyndigelser i forbindelse med sikkerheden i net- og informationssystemer, indordner dem pr. rolle, fordeler dem i overensstemmelse med de relevante enheders behov og meddeler dem til ledelsesorganerne.

1.2.2. De relevante enheder skal kræve, at alt personale og alle tredjeparter anvender et sikkerhedsniveau i deres net- og informationssystemer i overensstemmelse med de relevante enheders etablerede politik for net- og informationssikkerhed, emnespecifikke politikker og procedurer.

1.2.3. Mindst én person skal rapportere direkte til ledelsesorganerne om spørgsmål vedrørende sikkerheden i net- og informationssystemer.

1.2.4. Afhængigt af de relevante enheders størrelse skal sikkerheden i net- og informationssystemer være omfattet af særlige roller eller opgaver, der udføres, ud over de eksisterende roller.

1.2.5. Modstridende forpligtelser og modstridende ansvarsområder adskilles, hvor det er relevant.

1.2.6. Ledelsesorganerne gennemgår og, hvis det er relevant, ajourfører rollerne, ansvarsområderne og bemyndigelserne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

2. **Politik for risikostyring (artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555)**

2.1. *Ramme for risikostyring*

2.1.1. Med henblik på artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555 etablerer og opretholder de relevante enheder en passende ramme for risikostyring for at afdække og håndtere de risici, der er forbundet med sikkerheden i net- og informationssystemer. De relevante enheder skal udføre og dokumentere risikovurderinger og på grundlag af resultaterne udarbejde, gennemføre og overvåge en risikobehandlingsplan. Resultaterne af risikovurderingen og de resterende risici accepteres af ledelsesorganerne eller, hvor det er relevant, af personer, der er ansvarlige og bemyndigede til at styre risici, forudsat at de relevante enheder sikrer passende rapportering til ledelsesorganerne.

2.1.2. Med henblik på punkt 2.1.1 fastlægger de relevante enheder procedurer for afdækning, analyse, vurdering og behandling af risici ("risikostyringsprocessen for cybersikkerhed"). Risikostyringsprocessen for cybersikkerhed skal være en integreret del af de relevante enheders overordnede proces for risikostyring, hvor det er relevant. Som led i risikostyringsprocessen for cybersikkerhed skal de relevante enheder:

(a) følge en risikostyringsmetode

(b) fastsætte risikotolerancetærsklen i overensstemmelse med de relevante enheders risikovillighed

(c) fastlægge og opretholde relevante risikokriterier

(d) i overensstemmelse med en tilgang, der omfatter alle farer, afdække og dokumentere risici, der påvirker sikkerheden i net- og informationssystemer, navnlig i forbindelse med tredjeparter, og risici, der kan føre til forstyrrelser i net- og informationssystemernes tilgængelighed, integritet, autenticitet og fortrolighed, herunder afdækning af enkelte fejlpunkter

(e) analysere de risici, der påvirker sikkerheden i net- og informationssystemer, herunder trussels-, sandsynligheds-, indvirknings- og risikoniveauet, under hensyntagen til efterretninger om cybertrusler og sårbarheder

(f) evaluere de afdækkede risici på grundlag af risikokriterierne

(g) udpege og prioritere egnede risikobehandlingsmuligheder og -foranstaltninger

(h) løbende overvåge gennemførelsen af risikobehandlingsforanstaltningerne

(i) identificere, hvem der er ansvarlig for at gennemføre risikobehandlingsforanstaltningerne, og hvornår de bør gennemføres

(j) dokumentere de valgte risikobehandlingsforanstaltninger i en risikobehandlingsplan og begrunde accepten af de resterende risici på en forståelig måde.

2.1.3. Når de relevante enheder udpeger og prioriterer passende risikobehandlingsmuligheder og -foranstaltninger, tager de hensyn til risikovurderingsresultaterne, resultaterne af proceduren til vurdering af effektiviteten af foranstaltningerne til styring af cybersikkerhedsrisici, gennemførelsesomkostningerne i forhold til den forventede fordel, den klassifikation af aktiver, der er omhandlet i punkt 12.1, og den forretningskonsekvensanalyse, der er omhandlet i punkt 4.1.3.

2.1.4. De relevante enheder gennemgår og, hvis det er relevant, ajourfører både resultaterne af risikovurderingen og risikostyringsplanen med planlagte mellemrum og mindst én gang om året, samt når der sker væsentlige ændringer med hensyn til drift eller risici eller væsentlige hændelser.

2.2. *Overvågning af overholdelse*

2.2.1. De relevante enheder gennemgår regelmæssigt overholdelsen af deres politikker for sikkerheden i net- og informationssystemer, emnespecifikke politikker, regler og standarder. Ledelsesorganerne underrettes gennem regelmæssig rapportering på grundlag af evalueringer af overholdelsen om status for net- og informationssikkerheden.

2.2.2. De relevante enheder indfører et effektivt system til rapportering om overholdelse, som skal være passende for deres strukturer, driftsmiljøer og trusselsbilleder. Systemet til rapportering om overholdelse skal kunne give ledelsesorganerne et informeret overblik over den aktuelle situation med hensyn til de relevante enheders risikostyring.

2.2.3. De relevante enheder udfører overvågningen af overholdelsen med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

2.3. *Uafhængig gennemgang af informations- og netsikkerhed*

2.3.1. De relevante enheder gennemgår uafhængigt deres tilgang til styring af sikkerheden i deres net- og informationssystemer og gennemførelsen heraf, herunder mennesker, processer og teknologier.

2.3.2. De relevante enheder udvikler og opretholder processer til gennemførelse af uafhængige gennemgange, som skal udføres af personer med passende auditkompetence. Hvis den uafhængige gennemgang foretages af medarbejdere i den relevante enhed, må de personer, der foretager gennemgangen, ikke være underordnet eller overordnet personalet på det område, der er genstand for gennemgangen. Hvis enhedernes størrelse ikke tillader en sådan adskillelse af autoritetsmæssige forhold, træffer de relevante enheder alternative foranstaltninger for at sikre, at gennemgangen er upartisk.

2.3.3. Resultaterne af de uafhængige gennemgange, herunder resultaterne af overvågningen af overholdelsen i henhold til punkt 2.2 samt overvågningen og målingen i henhold til punkt 7, rapporteres til ledelsesorganerne. Der træffes korrigerende foranstaltninger, eller den resterende risiko accepteres i henhold til de relevante enheders kriterier for risikoaccept.

2.3.4. De uafhængige gennemgange skal foretages med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

3. **Håndtering af hændelser (artikel 21, stk. 2, litra b), i direktiv (EU) 2022/2555)**

3.1. *Politik for håndtering af hændelser*

3.1.1. Med henblik på artikel 21, stk. 2, litra b), i direktiv (EU) 2022/2555 fastlægger og gennemfører de relevante enheder en politik for håndtering af hændelser, hvori der fastsættes roller, ansvarsområder og procedurer for rettidigt at opdage, analysere, inddæmme eller reagere på, afhjælpe virkningerne af, dokumentere og rapportere hændelser.

3.1.2. Den politik, der er omhandlet i punkt 3.1.1, skal være i overensstemmelse med den driftskontinuitets- og katastrofeberedskabsplan, der er omhandlet i punkt 4.1. Politikken skal omfatte:

(a) et kategoriseringssystem for hændelser, der er i overensstemmelse med den vurdering og klassifikation af begivenheder, der foretages i henhold til punkt 3.4.1

(b) planer for effektiv kommunikation, herunder med hensyn til eskalering og rapportering

(c) tildeling af roller til kompetente medarbejdere med henblik på at opdage og reagere hensigtsmæssigt på hændelser

(d) dokumenter, der skal anvendes i forbindelse med opdagelse af og reaktion på hændelser, såsom håndbøger om håndtering af hændelser, eskaleringsdiagrammer, kontaktlister og skabeloner.

3.1.3. De roller, ansvarsområder og procedurer, der fastlægges i politikken, skal testes og gennemgås og, hvis det er relevant, ajourføres med planlagte mellemrum, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

3.2. *Overvågning og logning*

3.2.1. De relevante enheder fastlægger procedurer og anvender værktøjer til at overvåge og logge aktiviteter på deres net- og informationssystemer for at opdage begivenheder, der kan betragtes som hændelser, og reagere i overensstemmelse hermed for at afbøde virkningerne.

3.2.2. I det omfang, det er muligt, skal overvågningen automatiseres og udføres enten kontinuerligt eller med regelmæssige mellemrum, afhængigt af driftskapaciteten. De relevante enheder gennemfører deres overvågningsaktiviteter på en måde, der minimerer falske positive og falske negative resultater.

3.2.3. På grundlag af de procedurer, der er omhandlet i punkt 3.2.1, opbevares, dokumenteres og gennemgås logfiler af de relevante enheder. De relevante enheder opstiller en liste over aktiver, der skal være omfattet af logning, på grundlag af resultaterne af den risikovurdering, der foretages i henhold til punkt 2.1. Hvor det er relevant, skal logfilerne omfatte:

(a) relevant udgående og indgående nettrafik

(b) oprettelse, ændring eller sletning af brugere af de relevante enheders net- og informationssystemer og udvidelse af tilladelserne

(c) adgang til systemer og applikationer

(d) begivenheder i forbindelse med autentificering

(e) al privilegeret adgang til systemer og applikationer og aktiviteter, der udføres af administrative konti

(f) adgang til eller ændringer af kritiske konfigurations- og backupfiler

(g) logfiler over begivenheder og logfiler fra sikkerhedsværktøjer såsom antivirus, systemer til opdagelse af indtrængen eller firewalls

(h) anvendelse af systemressourcer samt deres ydeevne

(i) fysisk adgang til faciliteter

(j) adgang til og anvendelse af deres netudstyr og -anordninger

(k) aktivering, standsning og pause af de forskellige logningsprocesser

(l) miljøbegivenheder.

3.2.4. Logfilerne gennemgås regelmæssigt for usædvanlige eller uønskede tendenser. Hvor det er relevant, fastsætter de relevante enheder passende værdier for alarmtærskler. Hvis de fastsatte værdier for alarmtærsklerne overskrides, udløses der, hvor det er relevant, automatisk en alarm. De relevante enheder sikrer, at der i tilfælde af en alarm rettidigt iværksættes en kvalificeret og passende reaktion.

3.2.5. De relevante enheder opbevarer logfiler og backups heraf i en på forhånd fastsat periode og beskytter dem mod uautoriseret adgang eller ændringer.

3.2.6. I det omfang, det er muligt, sikrer de relevante enheder, at alle systemer har synkroniserede tidskilder for at kunne sammenholde logfiler mellem systemer til vurdering af begivenheder. De relevante enheder udarbejder og fører en liste over alle aktiver, der logges, og sikrer, at der er reservesystemer til overvågning og logning. Tilgængeligheden af overvågnings- og logningssystemerne skal overvåges uafhængigt af de systemer, de overvåger.

3.2.7. Procedurerne og listen over aktiver, der logges, skal gennemgås og, hvis det er relevant, ajourføres regelmæssigt samt efter væsentlige hændelser.

3.3. *Indberetning af begivenheder*

3.3.1. De relevante enheder indfører en enkel mekanisme, der gør det muligt for deres ansatte, leverandører og kunder at indberette mistænkelige begivenheder.

3.3.2. De relevante enheder skal, hvor det er relevant, underrette deres leverandører og kunder om mekanismen til indberetning af begivenheder og regelmæssigt uddanne deres ansatte i, hvordan de anvender mekanismen.

3.4. *Vurdering og klassifikation af begivenheder*

3.4.1. De relevante enheder vurderer mistænkelige begivenheder for at fastslå, om de udgør hændelser, og i bekræftende fald fastslå deres art og alvor.

3.4.2. Med henblik på punkt 3.4.1 handler de relevante enheder på følgende måde:

(a) Vurderingen foretages på grundlag af foruddefinerede kriterier og med prioritering af hændelser med henblik på inddæmning og afhjælpning

(b) Hvert kvartal vurderes forekomsten af tilbagevendende hændelser som omhandlet i denne forordnings artikel 4

(c) De relevante logfiler gennemgås med henblik på vurdering og klassifikation af begivenheder

(d) Der indføres en procedure for korrelation og analyse af logfiler

(e) Begivenheder revurderes og omklassificeres, hvis nye oplysninger bliver tilgængelige, eller efter analyser af tidligere tilgængelige oplysninger.

3.5. *Reaktion på hændelser*

3.5.1. De relevante enheder skal reagere rettidigt på hændelser i overensstemmelse med dokumenterede procedurer.

3.5.2. Procedurerne for reaktion på hændelser skal omfatte følgende faser:

(a) inddæmning af hændelser for at forhindre, at konsekvenserne af hændelsen spredes

(b) afhjælpning for at forhindre, at hændelsen fortsætter eller dukker op igen

(c) genopretning efter hændelsen, hvor det er nødvendigt.

3.5.3. De relevante enheder udarbejder kommunikationsplaner og -procedurer:

(a) med enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er) eller, hvor det er relevant, de kompetente myndigheder i forbindelse med underretning om hændelser

(b) til kommunikation mellem medarbejdere i den relevante enhed og til kommunikation med relevante interessenter uden for den relevante enhed.

3.5.4. De relevante enheder opfører i loggen aktiviteter vedrørende reaktion på hændelser i overensstemmelse med de procedurer, der er omhandlet i punkt 3.2.1, og dokumenterer forløbet.

3.5.5. De relevante enheder tester med planlagte mellemrum deres procedurer for reaktion på hændelser.

3.6. *Gennemgang efter hændelsen*

3.6.1. Hvor det er relevant, foretager de relevante enheder gennemgange efter hændelser, efter en given hændelse er blevet afhjulpet. Disse gennemgange efter hændelser skal, hvor det er muligt, afdække den grundlæggende årsag til hændelsen og resultere i dokumenterede erfaringer for at reducere forekomsten og konsekvenserne af fremtidige hændelser.

3.6.2. De relevante enheder sikrer, at gennemgange efter hændelser bidrager til at forbedre deres tilgang til net- og informationssikkerhed, til risikobehandlingsforanstaltninger og til procedurer for håndtering, opdagelse og reaktion på hændelser.

3.6.3. De relevante enheder gennemgår med planlagte mellemrum, hvorvidt hændelser afstedkom gennemgange efter hændelsen.

4. **Driftskontinuitet og krisestyring (artikel 21, stk. 2, litra c), i direktiv (EU) 2022/2555)**

4.1. *Driftskontinuitets- og katastrofeberedskabsplan*

4.1.1. Med henblik på artikel 21, stk. 2, litra c), i direktiv (EU) 2022/2555 fastlægger og opretholder de relevante enheder en driftskontinuitets- og katastrofeberedskabsplan, der finder anvendelse i tilfælde af hændelser.

4.1.2. De relevante enheders drift genoprettes i overensstemmelse med driftskontinuitets- og katastrofeberedskabsplanen. Planen skal bygge på resultaterne af den risikovurdering, der foretages i henhold til punkt 2.1, og skal, hvis det er relevant, omfatte følgende:

(a) formål, omfang og målgruppe

(b) roller og ansvarsområder

(c) vigtige kontakter og (interne og eksterne) kommunikationskanaler

(d) betingelser for aktivering og deaktivering af planen

(e) rækkefølge for genopretning af driften

(f) genopretningsplaner for specifikke aktiviteter, herunder genopretningsmål

(g) nødvendige ressourcer, herunder backup og reserver

(h) genopretning og genoptagelse af aktiviteter efter afslutningen af midlertidige foranstaltninger.

4.1.3. De relevante enheder foretager en forretningskonsekvensanalyse for at vurdere de potentielle konsekvenser af alvorlige forstyrrelser af deres forretningsaktiviteter og fastsætter på grundlag af forretningskonsekvensanalysens resultater kontinuitetskrav for net- og informationssystemerne.

4.1.4. driftskontinuitetsplanen og katastrofeberedskabsplanen skal testes, gennemgås og, hvis det er relevant, ajourføres med planlagte mellemrum, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici. De relevante enheder sikrer, at erfaringerne fra sådanne test indarbejdes i planerne.

4.2. *Styring af backups og reserver*

4.2.1. De relevante enheder opretholder backupkopier af data og stiller tilstrækkelige ressourcer til rådighed, herunder faciliteter, net- og informationssystemer og personale, for at sikre et passende niveau af reservekapacitet.

4.2.2. På grundlag af resultaterne af den risikovurdering, der foretages i henhold til punkt 2.1, og driftskontinuitetsplanen fastlægger de relevante enheder backupplaner, der skal omfatte følgende:

(a) genopretningstider

(b) sikring af, at backupkopier er fuldstændige og nøjagtige, herunder med hensyn til konfigurationsdata og data, der er lagret i cloudcomputing-tjenestemiljøet

(c) lagring af backupkopier (online eller offline) på et eller flere sikre steder, som ikke befinder sig i samme netværk som systemet, og som befinder sig i tilstrækkelig afstand til at undgå enhver skade fra en katastrofe på hovedstedet

(d) passende fysisk og logisk kontrol med adgang til backupkopier i overensstemmelse med aktivets klassifikationsgrad

(e) gendannelse af data fra sikkerhedskopier

(f) opbevaringsperioder baseret på forretningsmæssige og lovgivningsmæssige krav.

4.2.3. De relevante enheder foretager regelmæssig integritetskontrol af backupkopierne.

4.2.4. På grundlag af resultaterne af den risikovurdering, der foretages i henhold til punkt 2.1, og driftskontinuitetsplanen sikrer de relevante enheder, at der er tilstrækkelige ressourcer til rådighed ved at indføre i det mindste delvis reservekapacitet for følgende:

(a) net- og informationssystemer

(b) aktiver, herunder faciliteter, udstyr og forsyninger

(c) personale med det påkrævede ansvar, de nødvendige bemyndigelser og den nødvendige kompetence

(d) passende kommunikationskanaler.

4.2.5. Hvor det er relevant, sikrer de relevante enheder, at der tages hensyn til kravene om backup og reservekapacitet i forbindelse med overvågningen og tilpasningen af ressourcer, herunder faciliteter, systemer og personale.

4.2.6. De relevante enheder foretager regelmæssige test af forløbet med genopretning ud fra backupkopier og af reservekapaciteten for at sikre, at de både kan anvendes i en reel genopretningssituation og omfatter kopier, processer og viden til at foretage en effektiv genopretning. De relevante enheder dokumenterer testresultaterne og træffer om nødvendigt korrigerende foranstaltninger.

4.3. *Krisestyring*

4.3.1. De relevante enheder indfører en proces til krisestyring.

4.3.2. De relevante enheder sikrer, at krisestyringsprocessen som minimum omfatter følgende elementer:

(a) roller og ansvarsområder for personale og, hvor det er relevant, leverandører og tjenesteudbydere med angivelse af rollefordelingen i krisesituationer, herunder specifikke skridt, der skal følges

(b) passende kommunikationsmidler mellem de relevante enheder og relevante kompetente myndigheder

(c) anvendelse af passende foranstaltninger til at sikre vedligeholdelsen af sikkerheden i net- og informationssystemer i krisesituationer.

Med henblik på litra b) skal informationsstrømmen mellem de relevante enheder og de relevante kompetente myndigheder omfatte både obligatorisk kommunikation såsom hændelsesrapporter og dertil knyttede tidsfrister samt ikkeobligatorisk kommunikation.

4.3.3. De relevante enheder gennemfører en proces for forvaltning og anvendelse af oplysninger, der modtages fra CSIRT'erne eller de kompetente myndigheder, hvor det er relevant, vedrørende hændelser, sårbarheder, trusler eller mulige afbødende foranstaltninger.

4.3.4. De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører krisestyringsplanen regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

5. **Forsyningskædesikkerhed (artikel 21, stk. 2, litra d), i direktiv (EU) 2022/2555)**

5.1. *Politik for forsyningskædesikkerhed*

5.1.1. Med henblik på artikel 21, stk. 2, litra d), i direktiv (EU) 2022/2555 udarbejder, gennemfører og anvender de relevante enheder en politik for forsyningskædesikkerhed, som indeholder bestemmelser om forbindelserne med deres direkte leverandører og tjenesteudbydere med henblik på at afbøde de afdækkede risici for sikkerheden i net- og informationssystemer. I politikken for forsyningskædesikkerhed udpeger de relevante enheder deres rolle i forsyningskæden og kommunikerer den til deres direkte leverandører og tjenesteudbydere.

5.1.2. Som led i den i punkt 5.1.1 omhandlede sikkerhedspolitik for forsyningskæden fastsætter de relevante enheder kriterier for udvælgelse af og indgåelse af kontrakter med leverandører og tjenesteudbydere. Disse kriterier omfatter følgende:

(a) leverandørernes og tjenesteudbydernes cybersikkerhedspraksis, herunder deres procedurer for sikker udvikling

(b) leverandørernes og tjenesteudbydernes evne til at opfylde de cybersikkerhedsspecifikationer, der er fastsat af de relevante enheder

(c) IKT-produkternes og IKT-tjenesternes generelle kvalitet og modstandsdygtighed samt de indbyggede foranstaltninger til styring af cybersikkerhedsrisici, herunder IKT-produkternes og IKT-tjenesternes risici og klassifikationsgrad

(d) de relevante enheders evne til at diversificere forsyningskilderne og begrænse leverandørfastlåsning, hvor det er relevant.

5.1.3. Ved fastsættelsen af deres politik for forsyningskædesikkerhed tager de relevante enheder hensyn til resultaterne af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der foretages i henhold til artikel 22, stk. 1, i direktiv (EU) 2022/2555, hvor det er relevant.

5.1.4. På grundlag af politikken for forsyningskædesikkerhed og under hensyntagen til resultaterne af den risikovurdering, der foretages i overensstemmelse med dette bilags punkt 2.1, sikrer de relevante enheder, at der i deres kontrakter med leverandører og tjenesteudbydere, hvor det er relevant gennem serviceleveranceaftaler, angives følgende, hvor det er relevant:

(a) cybersikkerhedskrav til leverandører eller tjenesteudbydere, herunder krav vedrørende sikkerhed i forbindelse med erhvervelse af IKT-tjenester eller -produkter, jf. punkt 6.1

(b) krav til oplysning, færdigheder og uddannelse samt, hvor det er relevant, påkrævede certificeringer af leverandørernes eller tjenesteudbydernes ansatte

(c) krav til baggrundskontrol af leverandørers og tjenesteudbyderes ansatte

(d) en forpligtelse for leverandører og tjenesteudbydere til uden unødig forsinkelse at underrette de relevante enheder om hændelser, der udgør en risiko for sikkerheden i disse enheders net- og informationssystemer

(e) retten til audit eller retten til at modtage auditrapporter

(f) en forpligtelse for leverandører og tjenesteudbydere til at håndtere sårbarheder, der udgør en risiko for sikkerheden i de relevante enheders net- og informationssystemer

(g) krav vedrørende underentreprise og, såfremt de relevante enheder tillader underentreprise, cybersikkerhedskrav til underleverandører i overensstemmelse med de cybersikkerhedskrav, der er omhandlet i litra a)

(h) leverandørernes og tjenesteudbydernes forpligtelser ved kontraktens ophør, såsom indhentning og sletning af oplysninger, som leverandørerne og tjenesteyderne har erhvervet i forbindelse med udførelsen af deres opgaver.

5.1.5. De relevante enheder tager hensyn til de elementer, der er omhandlet i punkt 5.1.2 og 5.1.3, som led i udvælgelsesprocessen for nye leverandører og tjenesteudbydere samt som led i den udbudsproces, der er omhandlet i punkt 6.1.

5.1.6. De relevante enheder gennemgår politikken for forsyningskædesikkerhed og overvåger, evaluerer og, hvor det er nødvendigt, reagerer på ændringer i leverandørernes og tjenesteudbyderenes cybersikkerhedspraksis med planlagte mellemrum, samt når der sker væsentlige ændringer med hensyn til drift eller risici eller opstår væsentlige hændelser i forbindelse med leveringen af IKT-tjenester, eller når disse har indvirkning på sikkerheden i IKT-produkter fra leverandørerne og tjenesteudbyderne.

5.1.7. Med henblik på punkt 5.1.6 skal de relevante enheder:

(a) regelmæssigt overvåge rapporter om gennemførelsen af serviceleveranceaftalerne, hvor det er relevant

(b) gennemgå hændelser i forbindelse med IKT-produkter og IKT-tjenester fra leverandører og tjenesteudbydere

(c) vurdere behovet for spontane gennemgange og dokumentere resultaterne på en forståelig måde

(d) analysere de risici, der følger af ændringer i forbindelse med IKT-produkter og IKT-tjenester fra leverandører og tjenesteudbydere, og, hvis det er relevant, træffe afbødende foranstaltninger rettidigt.

5.2. *Fortegnelse over leverandører og tjenesteydere*

De relevante enheder fører og ajourfører et register over deres direkte leverandører og tjenesteudbydere, herunder:

(a) kontaktpunkter for hver direkte leverandør og tjenesteudbyder

(b) en liste over IKT-produkter, IKT-tjenester og IKT-processer, som den direkte leverandør eller tjenesteudbyder leverer til de relevante enheder.

6. **Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer (artikel 21, stk. 2, litra e), i direktiv (EU) 2022/2555)**

6.1. *Sikkerhed i forbindelse med erhvervelse af IKT-tjenester eller IKT-produkter*

6.1.1. Med henblik på artikel 21, stk. 2, litra e), i direktiv (EU) 2022/2555 fastsætter og gennemfører de relevante enheder på grundlag af den risikovurdering, der foretages i henhold til punkt 2.1, processer til styring af risici, der følger af erhvervelsen af IKT-tjenester eller IKT-produkter til komponenter, der er kritiske for de relevante enheders sikkerhed i net- og informationssystemer, fra leverandører eller tjenesteudbydere i hele deres livscyklus.

6.1.2. Med henblik på punkt 6.1.1 skal de i punkt 6.1.1 omhandlede processer omfatte:

(a) sikkerhedskrav til de IKT-tjenester eller IKT-produkter, der skal erhverves

(b) krav vedrørende sikkerhedsopdateringer i hele IKT-tjenesternes eller IKT-produkternes levetid eller udskiftning, når de pågældende tjenester eller produkter ikke længere understøttes

(c) oplysninger, der beskriver de hardware- og softwarekomponenter, der anvendes i IKT-tjenesterne eller IKT-produkterne

(d) oplysninger, der beskriver IKT-tjenesternes eller IKT-produkternes aktuelle cybersikkerhedsfunktioner og den konfiguration, der er nødvendig for en sikker drift heraf

(e) sikkerhed for, at IKT-tjenesterne eller IKT-produkterne opfylder sikkerhedskravene i henhold til litra a)

(f) metoder til validering af, at de leverede IKT-tjenester eller IKT-produkter opfylder de anførte sikkerhedskrav, samt dokumentation for resultaterne af valideringen.

6.1.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører processerne med planlagte mellemrum, samt når der opstår væsentlige hændelser.

6.2. *Sikker udviklingsproces*

6.2.1. Inden der udvikles et net- og informationssystem, herunder software, fastsætter de relevante enheder regler for sikker udvikling af net- og informationssystemer og anvender dem, når de udvikler net- og informationssystemer internt eller outsourcer udviklingen af net- og informationssystemer. Reglerne skal dække alle udviklingsfaser, herunder specifikation, udformning, udvikling, indførelse og test.

6.2.2. Med henblik på punkt 6.2.1 skal de relevante enheder:

(a) foretage en analyse af sikkerhedskravene i specifikations- og udformningsfasen af ethvert udviklings- eller erhvervelsesprojekt, der igangsættes af de relevante enheder eller på vegne af disse enheder

(b) anvende principper for udformning af sikre systemer og principper for sikker kodning på alle aktiviteter i forbindelse med udvikling af informationssystemer såsom fremme af indbygget cybersikkerhed og zero trust-arkitektur

(c) fastsætte sikkerhedskrav vedrørende udviklingsmiljøer

(d) etablere og gennemføre processer til sikkerhedstest i hele udviklingsprocessen

(e) på en passende måde udvælge, beskytte og forvalte data i forbindelse med sikkerhedstest

(f) rense og anonymisere testdata i henhold til den risikovurdering, der foretages i henhold til punkt 2.1.

6.2.3. I forbindelse med outsourcet udvikling af net- og informationssystemer anvender de relevante enheder også de politikker og procedurer, der er omhandlet i punkt 5 og 6.1.

6.2.4. De relevante enheder gennemgår og, hvis det er relevant, ajourfører med planlagte mellemrum deres regler for sikker udvikling.

6.3. *Konfigurationsstyring*

6.3.1. De relevante enheder træffer passende foranstaltninger til at etablere, dokumentere, gennemføre og overvåge konfigurationer, herunder sikkerhedskonfigurationer af hardware, software, tjenester og net.

6.3.2. Med henblik på punkt 6.3.1 skal de relevante enheder:

(a) fastlægge og sikre sikkerheden i konfigurationerne af deres hardware, software, tjenester og net

(b) fastlægge og gennemføre processer og værktøjer til håndhævelse af de fastlagte sikre konfigurationer af hardware, software, tjenester og net for både nyinstallerede systemer og systemer, der er i drift i hele deres levetid.

6.3.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører konfigurationerne med planlagte mellemrum, eller når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

6.4. *Ændringsstyring, reparation og vedligeholdelse*

6.4.1. De relevante enheder anvender ændringsstyringsprocedurer til at kontrollere ændringer af net- og informationssystemer. Hvor det er relevant, skal procedurerne være i overensstemmelse med de relevante enheders generelle politikker vedrørende ændringsstyring.

6.4.2. De procedurer, der er omhandlet i punkt 6.4.1, finder anvendelse på udgivelser, ændringer og nødændringer af enhver software og hardware, der er i drift, og på ændringer af konfigurationen. Procedurerne skal sikre, at disse ændringer dokumenteres og på grundlag af den risikovurdering, der foretages i henhold til punkt 2.1, testes og vurderes i betragtning af de potentielle virkninger, inden de gennemføres.

6.4.3. I tilfælde, hvor de regelmæssige ændringsstyringsprocedurer ikke kunne følges på grund af en nødsituation, skal de relevante enheder dokumentere resultatet af ændringen og begrundelsen for, hvorfor procedurerne ikke kunne følges.

6.4.4. De relevante enheder gennemgår og, hvis det er relevant, ajourfører procedurerne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer i forbindelse med drift eller risici.

6.5. *Sikkerhedstest*

6.5.1. De relevante enheder fastlægger, gennemfører og anvender en politik og procedurer for sikkerhedstest.

6.5.2. De relevante enheder:

(a) fastlægger på grundlag af den risikovurdering, der foretages i henhold til punkt 2.1, behovet for, omfanget af, hyppigheden af og typen af sikkerhedstest

(b) udfører sikkerhedstest i henhold til en dokumenteret testmetode, der omfatter de komponenter, der i en risikoanalyse er udpeget som relevante for sikker drift

(c) dokumenterer testenes type, omfang, tid og resultater, herunder med en vurdering af den kritiske betydning og en vurdering af afbødende foranstaltninger for hver konstatering

(d) anvender afbødende foranstaltninger i tilfælde af alvorlige konstateringer.

6.5.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører deres sikkerhedstestningspolitikker med planlagte mellemrum.

6.6. *Sikkerhedspatchstyring*

6.6.1. De relevante enheder specificerer og anvender procedurer, der er i overensstemmelse med de procedurer for ændringsstyring, der er omhandlet i punkt 6.4.1, samt med sårbarhedsstyrings-, risikostyrings- og andre relevante styringsprocedurer, med henblik på at sikre, at:

(a) sikkerhedspatches anvendes inden for en rimelig periode, efter at de er blevet tilgængelige

(b) sikkerhedspatches testes, inden de anvendes i systemer i produktionsmiljøet

(c) sikkerhedspatches stammer fra pålidelige kilder, og deres integritet kontrolleres

(d) der gennemføres yderligere foranstaltninger, og resterende risici accepteres i tilfælde, hvor en patch ikke er tilgængelig eller i henhold til punkt 6.6.2 ikke anvendes.

6.6.2. Uanset punkt 6.6.1, litra a), kan de relevante enheder vælge ikke at anvende en given sikkerhedspatch, hvis ulemperne ved at anvende sikkerhedspatchen er større end cybersikkerhedsfordelene. De relevante enheder skal behørigt dokumentere og begrunde en sådan afgørelse.

6.7. *Netsikkerhed*

6.7.1. De relevante enheder træffer passende foranstaltninger til at beskytte deres net- og informationssystemer mod cybertrusler.

6.7.2. Med henblik på punkt 6.7.1 skal de relevante enheder:

(a) dokumentere nettets arkitektur på en forståelig og ajourført måde

(b) fastlægge og anvende kontrolforanstaltninger til at beskytte de relevante enheders interne netdomæner mod uautoriseret adgang

(c) konfigurere kontrolforanstaltninger til at forhindre adgang og netværkskommunikation, der ikke er nødvendig for driften af de relevante enheder

(d) fastlægge og anvende kontrolforanstaltninger for fjernadgang til net- og informationssystemer, herunder tjenesteudbyderes adgang

(e) undlade at anvende systemer, der anvendes til administration af gennemførelsen af sikkerhedspolitikken, til andre formål

(f) udtrykkeligt forbyde eller deaktivere unødvendige forbindelser og tjenester

(g) hvis det er relevant, udelukkende tillade adgang til de relevante enheders net- og informationssystemer fra udstyr, der er godkendt af disse enheder

(h) kun tillade forbindelser mellem tjenesteudbydere og de relevante enheders systemer efter en anmodning om autorisering og i en bestemt periode, f.eks. varigheden af en vedligeholdelsesaktivitet

(i) kun etablere kommunikation mellem særskilte systemer gennem pålidelige kanaler, der isoleres ved hjælp af logisk, kryptografisk eller fysisk adskillelse fra andre kommunikationskanaler og på sikker vis kan identificere deres slutpunkter og beskytte data i kanalen mod ændring eller videregivelse

(j) vedtage en gennemførelsesplan for den fulde overgang til den seneste generation af kommunikationsprotokoller i netværkslaget på en sikker, hensigtsmæssig og gradvis måde og fastlægge foranstaltninger til at fremskynde en sådan overgang

(k) vedtage en gennemførelsesplan for indførelse af internationalt aftalte og interoperable moderne e-mailkommunikationsstandarder for at sikre e-mailkommunikation og derved afbøde sårbarheder i forbindelse med e-mailrelaterede trusler og fastlægge foranstaltninger til at fremskynde en sådan indførelse

(l) anvende bedste praksis for DNS-sikkerhed, internetroutingsikkerhed og routinghygiejne i forbindelse med trafik fra og til nettet.

6.7.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører disse foranstaltninger med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

6.8. *Netsegmentering*

6.8.1. De relevante enheder segmenterer systemer i net eller zoner i overensstemmelse med resultaterne af den risikovurdering, der er omhandlet i punkt 2.1. De opdeler deres systemer og net, så de er adskilt fra tredjeparters systemer og net.

6.8.2. Med henblik herpå skal de relevante enheder:

(a) overveje de funktionelle, logiske og fysiske forhold, herunder placering, mellem pålidelige systemer og tjenester

(b) give adgang til et net eller en zone på grundlag af en vurdering af nettets eller zonens sikkerhedskrav

(c) placere systemer, der er kritiske for de relevante enheders drift eller for sikkerheden, i sikrede zoner

(d) etablere en demilitariseret zone i deres kommunikationsnet for at sikre, at kommunikationen fra eller til deres netværk er sikker

(e) begrænse adgangen og kommunikationen mellem og inden for zoner til det, der er nødvendigt for de relevante enheders drift eller for sikkerheden

(f) adskille det dedikerede net til administration af net- og informationssystemerne fra de relevante enheders driftsnet

(g) adskille netadministrationskanalerne fra anden nettrafik

(h) adskille systemerne i produktionsmiljøet for de relevante enheders tjenester fra systemer, der anvendes til udvikling og test, herunder sikkerhedskopier.

6.8.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører netopdelingen med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer i forbindelse med drift eller risici.

6.9. *Beskyttelse mod skadelig og uautoriseret software*

6.9.1. De relevante enheder beskytter deres net- og informationssystemer mod skadelig og uautoriseret software.

6.9.2. Med henblik herpå gennemfører de relevante enheder navnlig foranstaltninger, der detekterer eller forhindrer brugen af skadelig eller uautoriseret software. De relevante enheder sikrer, hvis det er relevant, at deres net- og informationssystemer er udstyret med software til detektion og afhjælpning, og at det ajourføres regelmæssigt i overensstemmelse med den risikovurdering, der foretages i henhold til punkt 2.1, og de kontraktlige aftaler med udbyderne.

6.10. *Håndtering og offentliggørelse af sårbarheder*

6.10.1. De relevante enheder indhenter oplysninger om tekniske sårbarheder i deres net- og informationssystemer, evaluerer deres eksponering for sådanne sårbarheder og træffer passende foranstaltninger til at håndtere sårbarhederne.

6.10.2. Med henblik på punkt 6.10.1 skal de relevante enheder:

(a) overvåge oplysninger om sårbarheder gennem passende kanaler såsom meddelelser fra CSIRT'er, kompetente myndigheder eller oplysninger fra leverandører eller tjenesteudbydere

(b) med planlagte intervaller foretage sårbarhedsscanninger, hvor det er relevant, og dokumentere resultaterne af scanningerne

(c) uden unødig forsinkelse afhjælpe sårbarheder, som de relevante enheder har konstateret som værende af kritisk betydning for deres drift

(d) sikre, at deres sårbarhedshåndtering er forenelig med deres procedurer for ændringsstyring, sikkerheds-patchstyring, risikostyring og hændelsesstyring

(e) fastlægge en procedure for offentliggørelse af sårbarheder i overensstemmelse med den gældende nationale koordinerede politik for offentliggørelse af sårbarheder.

6.10.3. De relevante enheder udarbejder og gennemfører en plan for at afhjælpe sårbarheden i tilfælde, hvor sårbarhedens potentielle indvirkning berettiger dette. I andre tilfælde dokumenterer og begrunder de relevante enheder årsagen til, at sårbarheden ikke kræver afhjælpning.

6.10.4. De relevante enheder gennemgår og, hvis det er relevant, ajourfører med planlagte mellemrum de kanaler, de anvender til overvågning af sårbarhedsoplysninger.

7. **Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici (artikel 21, stk. 2, litra f), i direktiv (EU) 2022/2555)**

7.1. Med henblik på artikel 21, stk. 2, litra f), i direktiv (EU) 2022/2555 fastlægger, gennemfører og anvender de relevante enheder en politik og procedurer til vurdering af, om de foranstaltninger til styring af cybersikkerhedsrisici, som den relevante enhed har truffet, gennemføres og opretholdes effektivt.

7.2. Der skal i den politik og de procedurer, der er omhandlet i punkt 7.1, tages hensyn til resultaterne af risikovurderingen i henhold til punkt 2.1 og tidligere væsentlige hændelser. De relevante enheder fastlægger:

(a) hvilke foranstaltninger til styring af cybersikkerhedsrisici der skal overvåges og måles, herunder processer og kontrolforanstaltninger

(b) hvilke metoder der skal anvendes til passende overvågning, måling, analyse og evaluering for at sikre gyldige resultater

(c) hvornår overvågningen og målingen skal udføres

(d) hvem der er ansvarlig for at overvåge og måle effektiviteten af foranstaltningerne til styring af cybersikkerhedsrisici

(e) hvornår resultaterne fra overvågningen og målingen skal analyseres og evalueres

(f) hvem der skal analysere og evaluere disse resultater.

7.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken og procedurerne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer i forbindelse med drift eller risici.

8. **Grundlæggende cyberhygiejnepraksisser og sikkerhedsuddannelse (artikel 21, stk. 2, litra g), i direktiv (EU) 2022/2555)**

8.1. *Bevidstgørelse og grundlæggende cyberhygiejnepraksisser*

8.1.1. Med henblik på artikel 21, stk. 2, litra g), i direktiv (EU) 2022/2555 sikrer de relevante enheder, at deres ansatte, herunder medlemmer af ledelsesorganer, samt direkte leverandører og tjenesteudbydere er opmærksomme på risici, underrettes om betydningen af cybersikkerhed og anvender cyberhygiejnepraksisser.

8.1.2. Med henblik på punkt 8.1.1 skal de relevante enheder tilbyde deres ansatte, herunder medlemmer af ledelsesorganer samt direkte leverandører og tjenesteydere, hvis det er relevant i overensstemmelse med punkt 5.1.4, et bevidstgørelsesprogram, som:

(a) planlægges over en periode, således at aktiviteterne gentages, og nye medarbejdere inddrages i dem

(b) fastlægges i overensstemmelse med politikken for net- og informationssikkerhed, emnespecifikke politikker og relevante procedurer for net- og informationssikkerhed

(c) omfatter relevante cybertrusler, de eksisterende foranstaltninger til styring af cybersikkerhedsrisici, kontaktpunkter og ressourcer til yderligere oplysning og rådgivning af brugere om cybersikkerhedsspørgsmål samt cyberhygiejnepraksis.

8.1.3. Bevidstgørelsesprogrammet testes med hensyn til effektivitet, hvor det er relevant. Bevidstgørelsesprogrammet ajourføres og tilbydes med planlagte mellemrum under hensyntagen til ændringer i cyberhygiejnepraksis, det nuværende trusselsbillede og risici for de relevante enheder.

8.2. *Sikkerhedsuddannelse*

8.2.1. De relevante enheder udpeger medarbejdere, hvis roller kræver sikkerhedsrelevante færdigheder og ekspertise, og sikrer, at de modtager regelmæssig uddannelse i net- og informationssystemers sikkerhed.

8.2.2. De relevante enheder udarbejder, gennemfører og anvender et uddannelsesprogram i overensstemmelse med politikken for net- og informationssikkerhed, de emnespecifikke politikker og andre relevante procedurer for net- og informationssikkerhed, hvori uddannelsesbehovene for visse roller og stillinger fastlægges på grundlag af kriterier.

8.2.3. Den uddannelse, der er omhandlet i punkt 8.2.1, skal være relevant for medarbejderens jobfunktion, og dens effektivitet skal vurderes. Uddannelsen skal tage hensyn til eksisterende sikkerhedsforanstaltninger og omfatte følgende:

(a) instruktioner vedrørende sikker konfiguration og drift af net- og informationssystemer, herunder mobile enheder

(b) orientering om kendte cybertrusler

(c) uddannelse i hvad, der skal gøres, når der indtræffer sikkerhedsrelevante begivenheder.

8.2.4. De relevante enheder skal uddanne medarbejdere, der overgår til nye stillinger eller roller, som kræver sikkerheds-relevante færdigheder og ekspertise.

8.2.5. Programmet ajourføres og gennemføres regelmæssigt under hensyntagen til gældende politikker og regler, tildelte roller, ansvarsområder, kendte cybertrusler og den teknologiske udvikling.

9. **Kryptografi (artikel 21, stk. 2, litra h), i direktiv (EU) 2022/2555)**

9.1. Med henblik på artikel 21, stk. 2, litra h), i direktiv (EU) 2022/2555 fastlægger, gennemfører og anvender de relevante enheder en politik og procedurer vedrørende kryptografi for at sikre en passende og effektiv anvendelse af kryptografi til at beskytte fortroligheden, autenticiteten og integriteten af data i overensstemmelse med de relevante enheders klassifikation af aktiver og resultaterne af den risikovurdering, der foretages i henhold til punkt 2.1.

9.2. Med den politik og de procedurer, der er omhandlet i punkt 9.1, fastlægges:

(a) typen, styrken og kvaliteten af de kryptografiske foranstaltninger, der er nødvendige for at beskytte de relevante enheders aktiver, herunder data i hvile og data under overførsel, i overensstemmelse med de relevante enheders klassifikation af aktiver

(b) de protokoller eller typer af protokoller med udgangspunkt i litra a), der skal vedtages, samt de kryptografiske algoritmer, krypteringens styrke, de kryptografiske løsninger og den brugspraksis, der skal godkendes og kræves anvendt i enhederne efter en kryptografisk fleksibel tilgang, hvor dette er relevant

(c) de relevante enheders tilgang til nøgleforvaltning, herunder, hvor det er relevant, metoder til følgende:

i) generering af forskellige nøgler til kryptografiske systemer og applikationer

ii) udstedelse og erhvervelse af offentlige nøglecertifikater

iii) distribution af nøgler til de tilsigtede enheder, herunder hvordan nøgler aktiveres, når de modtages

iv) opbevaring af nøgler, herunder hvordan autoriserede brugere får adgang til nøgler

v) ændring eller ajourføring af nøgler, herunder regler om, hvornår og hvordan nøgler skal ændres

vi) håndtering af kompromitterede nøgler

vii) tilbagekaldelse af nøgler, herunder hvordan nøgler kaldes tilbage eller deaktiveres

viii) genoprettelse af tabte eller beskadigede nøgler

ix) backup eller arkivering af nøgler

x) destruktion af nøgler

xi) logning og revision af centrale ledelsesrelaterede aktiviteter

xii) fastsættelse af aktiverings- og deaktiveringsdatoer for nøgler for at sikre, at nøglerne kun kan anvendes i den angivne periode i henhold til organisationens regler om nøgleforvaltning.

9.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører deres politik og procedurer med planlagte mellemrum under hensyntagen til det aktuelle tekniske niveau inden for kryptografi.

10. **Personalesikkerhed (artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555)**

10.1. *Personalesikkerhed*

10.1.1. Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 sikrer de relevante enheder, at deres ansatte og direkte leverandører og tjenesteydere, hvor det er relevant, forstår og forpligter sig til deres sikkerhedsansvar, alt efter hvad der er relevant for de udbudte tjenester og jobbet, og i overensstemmelse med de relevante enheders politik for sikkerhed i net- og informationssystemer.

10.1.2. Det i punkt 10.1.1 omhandlede krav skal omfatte følgende:

(a) mekanismer til at sikre, at alle ansatte, direkte leverandører og tjenesteudbydere, hvor det er relevant, forstår og følger den standardpraksis for cyberhygiejne, som enhederne anvender i henhold til punkt 8.1

(b) mekanismer til at sikre, at alle brugere med administrativ eller privilegeret adgang er bekendt med og handler i overensstemmelse med deres roller, ansvarsområder og bemyndigelser

(c) mekanismer til at sikre, at medlemmer af ledelsesorganer forstår og handler i overensstemmelse med deres rolle, ansvarsområder og bemyndigelser med hensyn til sikkerheden i net- og informationssystemer

(d) mekanismer til ansættelse af personale, der er kvalificeret til de respektive roller, såsom kontrol af jobreferencer, undersøgelsesprocedurer, validering af certificeringer eller skriftlige prøver.

10.1.3. De relevante enheder gennemgår med planlagte mellemrum og mindst én gang om året tildelingen af personale til specifikke roller som omhandlet i punkt 1.2 samt deres dertil afsatte menneskelige ressourcer. De ajourfører om nødvendigt tildelingen.

10.2. *Baggrundskontrol*

10.2.1. De relevante enheder sikrer i det omfang, det er muligt, at der foretages baggrundskontrol af deres ansatte og, hvor det er relevant, af direkte leverandører og tjenesteydere i overensstemmelse med punkt 5.1.4, hvis det er nødvendigt i forbindelse med deres rolle, ansvarsområder og autoriseringer.

10.2.2. Med henblik på punkt 10.2.1 skal de relevante enheder:

(a) indføre kriterier for de roller, ansvarsområder og bemyndigelser, der kun må udøves eller indehaves af personer, hvis baggrund er blevet kontrolleret

(b) sikre, at der foretages den i punkt 10.2.1 omhandlede baggrundskontrol af disse personer, inden de begynder at udøve disse roller og myndigheder eller tildeles disse ansvarsområder, under hensyntagen til gældende love, forskrifter og etiske regler i forhold til de forretningsmæssige krav, klassifikationen af aktiver, jf. punkt 12.1, og de net- og informationssystemer, der skal tilgås, samt de opfattede risici.

10.2.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken med planlagte mellemrum og ajourfører den, hvor det er nødvendigt.

10.3. *Procedurer ved ophør eller ændring af ansættelsesforhold*

10.3.1. De relevante enheder sikrer, at ansvarsområder og opgaver i forbindelse med sikkerheden i net- og informationssystemer, der forbliver gyldige efter ophør eller ændring af deres ansattes ansættelsesforhold, defineres og håndhæves kontraktligt.

10.3.2. Med henblik på punkt 10.3.1 medtager de relevante enheder i den enkeltes arbejds- og ansættelsesvilkår, kontrakt eller aftale de ansvarsområder og forpligtelser, der stadig er gældende efter ansættelsesforholdets eller kontraktens ophør, såsom fortrolighedsklausuler.

10.4. *Disciplinærprocedure*

10.4.1. De relevante enheder etablerer, formidler og opretholder en disciplinærprocedure til håndtering af overtrædelser af politikker for sikkerheden i net- og informationssystemer. Der skal i proceduren tages hensyn til relevante retlige, vedtægtsmæssige, kontraktmæssige og forretningsmæssige krav.

10.4.2. De relevante enheder gennemgår og, hvis det er relevant, ajourfører disciplinærproceduren med planlagte mellemrum, samt når det er nødvendigt på grund af juridiske ændringer eller væsentlige ændringer i forbindelse med drift eller risici.

11. **Adgangskontrol (artikel 21, stk. 2, litra i) og j), i direktiv (EU) 2022/2555)**

11.1. *Politik for adgangskontrol*

11.1.1. Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 fastlægger, dokumenterer og gennemfører de relevante enheder politikker for logisk og fysisk kontrol af adgangen til deres net- og informationssystemer på grundlag af forretningsmæssige krav samt krav til sikkerheden i net- og informationssystemer.

11.1.2. De i punkt 11.1.1 omhandlede politikker skal:

(a) omhandle adgang for personer, herunder personale, besøgende og eksterne enheder såsom leverandører og tjenesteydere

(b) omhandle for net- og informationssystemer

(c) sikre, at der kun gives adgang til brugere, der er blevet behørigt autentificeret.

11.1.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikkerne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

11.2. *Forvaltning af adgangsrettigheder*

11.2.1. De relevante enheder skal give, ændre, fjerne og dokumentere adgangsrettigheder til net- og informationssystemer i overensstemmelse med den politik for adgangskontrol, der er omhandlet i punkt 11.1.

11.2.2. De relevante enheder:

(a) tildeler og tilbagekalder adgangsrettigheder på grundlag af "need to know"-princippet, "least privilege"-princippet og princippet om adskillelse af opgaver

(b) sikrer, at adgangsrettighederne ændres derefter ved ophør eller ændring af ansættelsesforhold

(c) sikrer, at adgangen til net- og informationssystemer autoriseres af de relevante personer

(d) sikre, at adgangsrettighederne på passende vis tager højde for tredjeparters adgang, såsom besøgende, leverandører og tjenesteudbydere, navnlig ved at begrænse adgangsrettigheder i omfang og varighed

(e) føre et register over tildelte adgangsrettigheder

(f) logge forvaltningen af adgangsrettigheder.

11.2.3. De relevante enheder gennemgår adgangsrettighederne med planlagte mellemrum og ændrer dem på grundlag af organisatoriske ændringer. De relevante enheder dokumenterer resultaterne af deres gennemgang, herunder de nødvendige ændringer af adgangsrettighederne.

11.3. *Privilegerede konti og systemadministrationskonti*

11.3.1. De relevante enheder fører politikker for forvaltning af privilegerede konti og systemadministrationskonti som led i den politik for adgangskontrol, der er omhandlet i punkt 11.1.

11.3.2. De i punkt 11.3.1 omhandlede politikker skal:

(a) indføres stærke identifikations-, autentificerings- (såsom multifaktor-autentificering) og autoriserings-procedurer for privilegerede konti og systemadministrationskonti

(b) oprettes særlige konti, der udelukkende skal anvendes til systemadministrationsaktiviteter, såsom installation, konfiguration, forvaltning eller vedligeholdelse

(c) individualisere og begrænse systemadministrationsbeføjelserne i videst muligt omfang

(d) fastsætte, at systemadministrationskonti kun anvendes til ved forbindelse til systemadministrationssystemer.

11.3.3. De relevante enheder gennemgår adgangsrettighederne til privilegerede konti og systemadministrationskonti med planlagte mellemrum, ændrer dem efter organisatoriske ændringer og dokumenterer resultaterne af gennemgangen, herunder nødvendige ændringer af adgangsrettighederne.

11.4. *Administrationssystemer*

11.4.1. De relevante enheder skal begrænse og kontrollere anvendelsen af systemadministrationssystemer i overensstemmelse med den politik for adgangskontrol, der er omhandlet i punkt 11.1.

11.4.2. Med henblik herpå skal de relevante enheder:

(a) kun anvende systemadministrationssystemer til systemadministrationsformål og ikke til andre aktiviteter

(b) logisk adskille disse systemer fra applikationssoftware, der ikke anvendes til systemadministrationsformål

(c) beskytte adgangen til systemadministrationssystemer gennem autentificering og kryptering.

11.5. *Identifikation*

11.5.1. De relevante enheder forvalter hele livscyklussen for net- og informationssystemer og deres brugere.

11.5.2. Med henblik herpå skal de relevante enheder:

(a) oprette unikke identiteter for net- og informationssystemer og deres brugere

(b) forbinde en given brugeridentitet med en enkelt person

(c) sikre tilsyn med identiteter i net- og informationssystemer

(d) logge forvaltningen af identiteter.

11.5.3. De relevante enheder må kun tillade identiteter, der er tildelt flere personer, såsom fælles identiteter, hvis dette er nødvendigt af forretningsmæssige eller driftsmæssige årsager og er underlagt en udtrykkelig godkendelsesproces og dokumenteres. De relevante enheder tager hensyn til identiteter, der er tildelt flere personer, i den ramme for styring af cybersikkerhedsrisici, der er omhandlet i punkt 2.1.

11.5.4. De relevante enheder gennemgår regelmæssigt identiteterne for net- og informationssystemer og deres brugere og deaktiverer dem straks, hvis der ikke længere er behov for dem.

11.6. *Autentificering*

11.6.1. De relevante enheder indfører sikre autentificeringsprocedurer og -teknologier baseret på adgangsbegrænsninger og politikken for adgangskontrol.

11.6.2. Med henblik herpå skal de relevante enheder:

(a) sikre, at autentificeringsstyrken er hensigtsmæssig i forhold til klassifikationen af det aktiv, der tilgås

(b) kontrollere tildelingen til brugerne og forvaltningen af hemmelige autentificeringsoplysninger ved hjælp af en proces, der sikrer oplysningernes fortrolighed, herunder via rådgivning af personalet om passende håndtering af autentificeringsoplysninger

(c) kræve ændring af autentificeringsoplysninger ved den indledende tildeling, med planlagte mellemrum og ved mistanke om, at oplysningerne er blevet kompromitteret

(d) kræve nulstilling af autentificeringsoplysninger og blokering af brugere efter et på forhånd fastsat antal mislykkede loginforsøg

(e) afslutte inaktive sessioner efter en på forhånd fastsat periode med inaktivitet og

(f) kræve særskilte autentificeringsoplysninger for adgang til privilegerede konti eller administrationskonti.

11.6.3. De relevante enheder anvender i det omfang, det er muligt, de nyeste autentificeringsmetoder i overensstemmelse med den tilknyttede vurderede risiko og klassifikationen af det aktiv, der tilgås, samt unikke autentificeringsoplysninger.

11.6.4. De relevante enheder gennemgår autentificeringsprocedurerne og -teknologierne med planlagte mellemrum.

11.7. *Multifaktor-autentificering*

11.7.1. De relevante enheder sikrer, at brugerne autentificeres ved hjælp af flere autentificeringsfaktorer eller mekanismer til kontinuerlig autentificering, når de forsøger at tilgå enhedernes net- og informationssystemer, hvor det er relevant, i overensstemmelse med klassifikationen af det aktiv, der tilgås.

11.7.2. De relevante enheder sikrer, at autentificeringsstyrken er hensigtsmæssig i forhold til klassifikationen af det aktiv, der tilgås.

12. **Forvaltning af aktiver (artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555)**

12.1. *Klassifikation af aktiver*

12.1.1. Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 fastsætter de relevante enheder klassifikationsgrader med henblik på det krævede beskyttelsesniveau for alle aktiver, herunder oplysninger, der er omfattet af deres net- og informationssystemer.

12.1.2. Med henblik på punkt 12.1.1 skal de relevante enheder:

(a) fastlægge et system med klassifikationsgrader for aktiver

(b) knytte alle oplysninger og aktiver til en klassifikationsgrad på grundlag af krav om fortrolighed, integritet, autenticitet og tilgængelighed for at angive det påkrævede beskyttelsesniveau i forhold til deres følsomhed, kritiske betydning, risiko og forretningsværdi

(c) tilpasse tilgængelighedskravene til aktiverne til de leverings- og genopretningsmål, der er fastsat i deres driftskontinuitets- og katastrofeberedskabsplaner.

12.1.3. De relevante enheder foretager regelmæssige gennemgange af klassifikationsniveauerne for aktiver og ajourfører dem, hvor det er relevant.

12.2. *Håndtering af aktiver*

12.2.1. De relevante enheder fastlægger, gennemfører og anvender en politik for korrekt håndtering af aktiver, herunder oplysninger, i overensstemmelse med deres politik for net- og informationssikkerhed og formidler politikken for korrekt håndtering af aktiver til enhver, der anvender eller håndterer aktiver.

12.2.2. Politikken skal:

(a) dække aktivernes fuldstændige livscyklus, herunder erhvervelse, anvendelse, opbevaring, transport og bortskaffelse

(b) indeholde regler om sikker anvendelse, sikker opbevaring, sikker transport og uigenkaldelig sletning og destruktion af aktiverne

(c) indeholde bestemmelser om, at overførsler skal finde sted på en sikker måde i overensstemmelse med den type aktiv, der overføres.

12.2.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

12.3. *Politik om mobile medier*

12.3.1. De relevante enheder fastlægger, gennemfører og anvender en politik for forvaltning af mobile lagringsmedier og formidler den til deres ansatte og de tredjeparter, der håndterer mobile lagringsmedier i de relevante enheders lokaler eller andre steder, hvor de mobile medier tilsluttes de relevante enheders net- og informationssystemer.

12.3.2. Politikken skal:

(a) fastsætte et teknisk forbud mod tilslutning af mobile medier, medmindre der er en organisatorisk begrundelse for deres anvendelse

(b) indeholde bestemmelser om deaktivering af autoeksekvering fra sådanne medier og scanning af medierne for skadelig kode, inden de anvendes i enhedernes systemer

(c) indeholde foranstaltninger til kontrol og beskyttelse af bærbare lagringsenheder, der indeholder data, mens de er i transit eller under opbevaring

(d) hvor det er relevant, indeholde foranstaltninger om anvendelse af kryptografiske teknikker for at beskytte oplysninger på mobile lagringsmedier.

12.3.3. De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

12.4. *Fortegnelse over aktiver*

12.4.1. De relevante enheder udarbejder og vedligeholder en fuldstændig, nøjagtig, ajourført og konsekvent fortegnelse over deres aktiver. De registrerer ændringer i fortegnelsen på en sporbar måde.

12.4.2. Detaljeringsgraden af fortegnelsen over aktiver skal modsvare de relevante enheders behov. Fortegnelsen skal omfatte følgende:

(a) en liste over aktiviteter og tjenesteydelser og beskrivelser heraf

(b) en liste over net- og informationssystemer og andre tilknyttede aktiver, der understøtter enhedernes drift og tjenester.

12.4.3. De relevante enheder reviderer og ajourfører regelmæssigt fortegnelsen og deres aktiver og dokumenterer ændringernes historik.

12.5. *Deponering, tilbagelevering eller sletning af aktiver ved ophør af ansættelsesforhold*

De relevante enheder indfører, gennemfører og anvender procedurer, der sikrer, at de af deres aktiver, som er i personalets varetægt, deponeres, tilbageleveres eller slettes ved ansættelsesforholdets ophør, og dokumenterer deponering, tilbagelevering og sletning af disse aktiver. I tilfælde, hvor deponering, tilbagelevering eller sletning af aktiver ikke er mulig, sikrer de relevante enheder, at aktiverne ikke længere kan anvendes til at tilgå de relevante enheders net- og informationssystemer i overensstemmelse med punkt 12.2.2.

13. **Miljømæssig og fysisk sikkerhed (artikel 21, stk. 2, litra c), e) og i), i direktiv (EU) 2022/2555)**

13.1. *Understøttende forsyningstjenester*

13.1.1. Med henblik på artikel 21, stk. 2, litra c), i direktiv (EU) 2022/2555 forebygger de relevante enheder tab, beskadigelse eller kompromittering af net- og informationssystemer samt afbrydelse af deres drift som følge af svigt eller forstyrrelse af de understøttende forsyningstjenester.

13.1.2. Med henblik herpå skal de relevante enheder, hvor det er relevant:

(a) beskytte anlæg mod strømsvigt og andre forstyrrelser som følge af mangler i de understøttende forsyningstjenester såsom elektricitet, telekommunikation, vandforsyning, gas, spildevand, ventilation og klimaanlæg

(b) overveje anvendelsen af reservekapacitet i forbindelse med forsyningstjenester

(c) beskytte forsyningstjenesterne for elektricitet og telekommunikation, som transporterer data eller forsyner net- og informationssystemerne, mod aflytning og beskadigelse

(d) overvåge de forsyningstjenester, der er omhandlet i litra c), og rapportere begivenheder uden for de minimums- og maksimumskontroltærskler, der er omhandlet i punkt 13.2.2, litra b), og som påvirker forsyningstjenesterne, til det kompetente interne eller eksterne personale

(e) indgå kontrakter om nødforsyning med tilsvarende tjenester, f.eks. brændstof til nødstrømforsyning

(f) overvåge, vedligeholde og teste forsyningen til de net- og informationssystemer, der er nødvendige for driften af den tjeneste, der tilbydes, navnlig el-, temperatur- og fugtighedskontrol, telekommunikation og internetforbindelse, samt sikre, at de nævnte systemer fungerer kontinuerligt.

13.1.3. De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører beskyttelsesforanstaltningerne regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

13.2. *Beskyttelse mod fysiske og miljømæssige trusler*

13.2.1. Med henblik på artikel 21, stk. 2, litra e), i direktiv (EU) 2022/2555 skal de relevante enheder på grundlag af resultaterne af den risikovurdering, der foretages i henhold til punkt 2.1, forebygge eller mindske konsekvenserne af begivenheder, der skyldes fysiske og miljømæssige trusler, såsom naturkatastrofer og andre forsætlige eller uforsætlige trusler.

13.2.2. Med henblik herpå skal de relevante enheder, hvor det er relevant:

(a) udforme og gennemføre foranstaltninger til beskyttelse mod fysiske og miljømæssige trusler

(b) fastsætte minimums- og maksimumskontroltærskler for fysiske og miljømæssige trusler

(c) overvåge miljømæssige parametre og rapportere begivenheder uden for de i litra b) omhandlede minimums- og maksimumskontroltærskler til det kompetente interne eller eksterne personale

13.2.3. De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører foranstaltningerne til beskyttelse mod fysiske og miljømæssige trusler regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.

13.3. *Perimeterkontrol og fysisk adgangskontrol*

13.3.1. Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 skal de relevante enheder forebygge og overvåge uautoriseret fysisk adgang til, beskadigelse af og indgreb i deres net- og informationssystemer.

13.3.2. Med henblik herpå skal de relevante enheder:

(a) på grundlag af den risikovurdering, der foretages i henhold til punkt 2.1, fastlægge og anvende sikkerhedsperimetre til at beskytte områder, hvor net- og informationssystemer og andre tilknyttede aktiver befinder sig

(b) beskytte de områder, der er omhandlet i litra a), ved hjælp af passende adgangskontrol og adgangspunkter

(c) udforme og gennemføre foranstaltninger til fysisk sikkerhed i kontorer, lokaler og faciliteter

(d) løbende overvåge deres lokaler for uautoriseret fysisk adgang.

13.3.3. De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører foranstaltningerne til fysisk adgangskontrol regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici.