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

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen ([1]), særlig artikel 16, stk. 8, og

ud fra følgende betragtninger:

(1) I henhold til direktiv (EU) 2016/1148 kan udbydere af digitale tjenester frit træffe de tekniske og organisatoriske foranstaltninger, som de finder passende og forholdsmæssige for at styre risiciene i forhold til sikkerheden i net- og informationssystemerne, for så vidt som disse foranstaltninger sikrer et passende sikkerhedsniveau under hensyntagen til de elementer, der kræves ifølge direktivet.

(2) Når udbydere af digitale tjenester fastlægger passende og forholdsmæssige tekniske og organisatoriske foranstaltninger, bør de gribe informationssikkerhed an på en systematisk måde ved hjælp af en risikobaseret tilgang.

(3) For at garantere systemers og faciliteters sikkerhed bør udbydere af digitale tjenester gennemføre vurderings- og analyseprocedurer. Disse aktiviteter bør omfatte systematisk forvaltning af net- og informationssystemer, fysisk og miljømæssig sikkerhed, forsyningssikkerhed og adgangskontrol.

(4) Når udbydere af digitale tjenester gennemfører en risikoanalyse som led i den systematiske forvaltning af net- og informationssystemer, bør de tilskyndes til at kortlægge de specifikke risici og kvantificere deres betydning, f.eks. ved at påpege trusler mod kritiske aktiver og fastslå, hvordan truslerne kan påvirke driften, og de bør afgøre, hvordan man bedst kan imødegå disse trusler i betragtning af den disponible kapacitet og ressourcebehovene.

(5) Personalepolitik kan f.eks. omfatte forvaltning af kvalifikationer, herunder aspekter vedrørende udvikling af sikkerhedsrelaterede kvalifikationer og bevidstgørelse. Når udbydere af digitale tjenester træffer beslutning om et passende sæt politikker for driftssikkerhed, bør de tilskyndes til at tage hensyn til aspekter som ændringsstyring, sårbarhedsstyring, formalisering af drifts- og administrationspraksis og systemkortlægning.

(6) Politikker for sikkerhedsarkitektur kan f.eks. omfatte adskillelse af net og systemer samt særlige sikkerhedsforanstaltninger for kritiske funktioner såsom administrative funktioner. Adskillelse af net og systemer kan gøre det muligt for en udbyder af digitale tjenester at skelne mellem elementer såsom datastrømme og IT-ressourcer, der tilhører henholdsvis en kunde, en gruppe af kunder, udbyderen af digitale tjenester eller en tredjepart.

(7) De foranstaltninger, der træffes vedrørende fysisk og miljømæssig sikkerhed, bør sikre en organisations net- og informationssystemer mod skader forårsaget af hændelser som f.eks. tyveri, brand, oversvømmelse eller andre ugunstige vejrforhold, telekommunikations- eller strømafbrydelser.

(8) Forsyningssikkerheden med hensyn til bl.a. elektricitet, brændstof eller køling kan f.eks. dække sikkerhed i forsyningskæden, der navnlig omfatter sikkerheden i forbindelse med tredjepartsleverandører og underkontrahenter samt disses forvaltning. Kritiske forsyningers sporbarhed vedrører tjenesteudbyderens evne til at udpege og dokumentere kilderne til disse forsyninger.

(9) Brugerne af digitale tjenester bør omfatte fysiske og juridiske personer, der er kunder eller abonnenter på en onlinemarkedsplads eller en cloud computing-tjeneste, eller som besøger en onlinesøgemaskines websted for at foretage søgninger på nøgleord.

([1]) EUT L 194 af 19.7.2016, s. 1.

(10) Ved bestemmelsen af, om en hændelses konsekvenser er betydelige, bør de tilfælde, der er fastsat i denne forordning, betragtes som en ikke-udtømmende liste over hændelser med betydelige konsekvenser. Der bør drages lære af gennemførelsen af denne forordning og af arbejdet i samarbejdsgruppen, for så vidt angår indsamlingen af oplysninger om bedste praksis i forbindelse med risici og hændelser og drøftelserne om metoder til rapportering af underretning om hændelser, jf. artikel 11, stk. 3, litra i) og m), i direktiv (EU) 2016/1148. Dette kan f.eks. udmunde i omfattende retningslinjer vedrørende kvantitative grænseværdier for underretningsparametre, der kan udløse underretningspligten for udbydere af digitale tjenester i henhold til artikel 16, stk. 3, i direktiv (EU) 2016/1148. Hvor det er relevant, kunne Kommissionen også overveje at tage de grænseværdier, der er fastsat i denne forordning, op til fornyet overvejelse.

(11) For at de kompetente myndigheder kan blive underrettet om potentielle nye risici, bør udbyderne af digitale tjenester tilskyndes til frivilligt at rapportere om enhver hændelse med kendetegn, der hidtil har været ukendte for dem, såsom nye angrebsværktøjer (»exploits«), angrebsvektorer eller trusselsaktører, sårbarheder og risici.

(12) Denne forordning bør anvendes fra og med dagen efter udløbet af fristen for gennemførelse af direktiv (EU) 2016/1148.

(13) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra Udvalget for Sikkerhed i Net- og Informationssystemer, jf. artikel 22 i direktiv (EU) 2016/1148 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

Ved denne forordning specificeres det, hvilke elementer udbydere af digitale tjenester skal tage i betragtning, når de fastlægger og træffer foranstaltninger for at garantere et niveau af sikkerhed i net- og informationssystemer, som de anvender i forbindelse med de typer af tjenester, der er opført i bilag III til direktiv (EU) 2016/1148, og det specificeres, hvilke kriterier der skal tages i betragtning ved bestemmelsen af, om en hændelse har betydelige konsekvenser for leveringen af disse tjenester.

Artikel 2

Sikkerhedselementer

1. Ved systemers og faciliteters sikkerhed som anført i artikel 16, stk. 1, litra a), i direktiv (EU) 2016/1148 forstås sikkerheden i net- og informationssystemer og deres fysiske omgivelser, hvilket omfatter følgende elementer:

a) systematisk forvaltning af net- og informationssystemer, hvilket indebærer en kortlægning af informationssystemerne og fastlæggelse af et sæt passende politikker til styring af informationssikkerhed, herunder risikoanalyse, personaleressourcer, driftssikkerhed, sikkerhedsarkitektur, sikre data og livscyklusstyring af systemer og, hvor det er relevant, kryptering og styring af en sådan kryptering

b) fysisk og miljømæssig sikkerhed, hvilket betyder, at der skal træffes en række foranstaltninger for at beskytte sikkerheden i de net- og informationssystemer, som udbydere af digitale tjenester anvender, mod skader gennem en risikobaseret tilgang, der dækker alle risici, herunder systemsvigt, menneskelige fejl, handlinger i ond hensigt og naturfænomener

c) forsyningssikkerhed, hvilket betyder, at der skal fastlægges og ajourføres passende politikker for at sikre adgang til kritiske forsyninger, der anvendes i forbindelse med levering af tjenesterne, og hvor det er relevant, sikre disse forsyningers sporbarhed

d) kontrol af adgangen til net- og informationssystemer, hvilket betyder, at der skal træffes en række foranstaltninger for at sikre, at fysisk og logisk adgang til net- og informationssystemer, herunder den administrative sikkerhed i net- og informationssystemer, tillades og begrænses på grundlag af forretnings- og sikkerhedsmæssige krav.

2. Med hensyn til håndtering af hændelser som anført i artikel 16, stk. 1, litra b), i direktiv (EU) 2016/1148 skal udbyderne af digitale tjenester træffe foranstaltninger, der omfatter:

a) opretholdelse og afprøvning af detekteringssprocesser og -procedurer, der sikrer rettidig og tilstrækkelig bevidsthed om unormale begivenheder

b) processer og politikker for rapportering af hændelser og konstatering af svagheder og sårbarheder i deres informationssystemer

c) reaktion på hændelser i overensstemmelse med fastlagte procedurer og rapportering om resultaterne af de trufne foranstaltninger

d) vurdering af hændelsernes alvor og redegørelse for den viden, der er opnået ved analyse af hændelserne, og indsamling af relevante oplysninger, som kan tjene som dokumentation og fremme en vedvarende forbedringsproces.

3. Ved styring af driftskontinuitet som anført i artikel 16, stk. 1, litra c), i direktiv (EU) 2016/1148 forstås en organisations evne til at opretholde eller, hvor det er relevant, genoprette leveringen af tjenester på et acceptabelt, forud fastsat niveau efter en forstyrrende hændelse; dette omfatter:

a) udarbejdelse og anvendelse af beredskabsplaner på grundlag af en konsekvensanalyse for at sikre kontinuiteten i de tjenester, der leveres af udbydere af digitale tjenester; planerne skal vurderes og afprøves regelmæssigt, f.eks. gennem øvelser

b) katastrofeberedskabskapacitet, der skal vurderes og afprøves regelmæssigt, f.eks. gennem øvelser.

4. Monitorering, audit og testning som anført i artikel 16, stk. 1, litra d), i direktiv (EU) 2016/1148 skal omfatte fastlæggelse og ajourføring af politikker for:

a) gennemførelse af en planlagt sekvens af observationer eller målinger med henblik på at vurdere, om net- og informationssystemerne fungerer efter hensigten

b) inspektion og verifikation med henblik på at kontrollere, om en standard eller et sæt retningslinjer følges, om registreringerne er nøjagtige, og om målene for effektivitet og virkningsfuldhed opfyldes

c) en proces med henblik på at afsløre mangler i et net- og informationssystems sikkerhedsmekanismer til beskyttelse af data og opretholdelse af den tilsigtede funktionalitet. En sådan proces skal omfatte de tekniske processer og det personale, der indgår i driften.

5. Ved internationale standarder som anført i artikel 16, stk. 1, litra e) i direktiv (EU) 2016/1148 forstås standarder, der er vedtaget af et internationalt standardiseringsorgan, som omhandlet i artikel 2, nr. 1), litra a), i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 ([1]). I henhold til artikel 19 i direktiv (EU) 2016/1148 kan der også anvendes europæiske eller internationalt anerkendte standarder og specifikationer, der er relevante for sikkerheden i net- og informationssystemer, herunder eksisterende nationale standarder.

6. Udbydere af digitale tjenester skal sikre, at de kan stille den dokumentation til rådighed, som den kompetente myndighed behøver for at kontrollere, om de sikkerhedselementer, der er beskrevet i stk. 1-5, er opfyldt.

Artikel 3

Kriterier for bestemmelse af, om en hændelses konsekvenser er betydelige

1. Hvad angår antallet af brugere, der berøres af en hændelse, navnlig brugere, som er afhængige af tjenesten med henblik på levering af deres egne tjenester, som anført i artikel 16, stk. 4, litra a), i direktiv (EU) 2016/1148 skal udbydere af digitale tjenester være i stand til at anslå enten:

a) antallet af berørte fysiske og juridiske personer, med hvem der er indgået kontrakt om levering af tjenesten eller

b) antallet af berørte brugere, der har benyttet tjenesten, navnlig baseret på tidligere trafikdata.

2. Ved hændelsens varighed som anført i artikel 16, stk. 4, litra b), forstås tidsrummet fra afbrydelsen af den normale levering af tjenesten, for så vidt angår tilgængelighed, autenticitet, integritet eller fortrolighed, indtil det tidspunkt, hvor tjenesten blev genoprettet.

3. Hvad angår den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen, som anført i artikel 16, stk. 4, litra c), i direktiv (EU) 2016/1148 skal udbydere af digitale tjenester være i stand til at fastslå, om hændelsen påvirker leveringen af deres tjenester i bestemte medlemsstater.

4. Omfanget af afbrydelsen af tjenestens funktion som anført i artikel 16, stk. 4, litra d), i direktiv (EU) 2016/1148 skal måles for så vidt angår en eller flere af følgende egenskaber, der svækkes som følge af en hændelse: datas eller dermed forbundne tjenesters tilgængelighed, autenticitet, integritet eller fortrolighed.

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

5. Hvad angår omfanget af konsekvenserne for økonomiske og samfundsmæssige aktiviteter som anført i artikel 16, stk. 4, litra e), i direktiv (EU) 2016/1148 skal udbydere af digitale tjenester på baggrund af f.eks. arten af deres kontraktforhold med kunderne, eller, hvor det er relevant, antallet af potentielt berørte brugere, kunne konkludere, om hændelsen har medført betydelige materielle eller ikke-materielle tab for brugerne, f.eks. med hensyn til sundhed, sikkerhed eller skade på ejendom.

6. Med henblik på anvendelsen af stk. 1-5 er udbydere af digitale tjenester ikke forpligtet til at indsamle yderligere oplysninger, som de ikke har adgang til.

Artikel 4

Betydelige konsekvenser af en hændelse

1. En hændelse anses for at have betydelige konsekvenser, hvis den har medført mindst én af følgende situationer:

a) tjenesten, der leveres af en udbyder af digitale tjenester, var ikke tilgængelig i over 5 000 000 brugertimer, idet udtrykket »brugertime« henviser til antallet af berørte brugere i Unionen i en periode på 60 minutter

b) hændelsen har ført til tab af integritet, autenticitet eller fortrolighed i forbindelse med arkiverede, overførte eller behandlede data eller dermed forbundne tjenester, der tilbydes af udbyderen eller er tilgængelige via udbyderens net- og informationssystem, og dette tab berører mere end 100 000 brugere i Unionen

c) hændelsen har medført risiko for den offentlige sikkerhed eller tab af menneskeliv

d) hændelsen har forårsaget materiel skade på over 1 000 000 EUR for mindst én bruger i Unionen.

2. På grundlag af de oplysninger om bedste praksis, som samarbejdsgruppen har indsamlet under udøvelsen af sine opgaver i henhold til artikel 11, stk. 3, i direktiv (EU) 2016/1148, og drøftelserne i henhold til samme direktivs artikel 11, stk. 3, litra m), kan Kommissionen revidere de grænseværdier, der er fastsat i stk. 1.

Artikel 5

Ikrafttræden

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

2. Den anvendes fra den 10. maj 2018.

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

Udfærdiget i Bruxelles, den 30. januar 2018.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand