KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2018/151

av den 30 januari 2018

om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen vad gäller närmare specificering av de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen [1], särskilt artikel 16.8, och

av följande skäl:

(1) Enligt direktiv (EU) 2016/1148 bör leverantörer av digitala tjänster fritt kunna vidta de tekniska och organisatoriska åtgärder som de anser lämpliga för att hantera risker för säkerheten i deras nät- och informationssystem, om dessa åtgärder säkerställer en lämplig säkerhetsnivå och tar hänsyn till de aspekter som föreskrivs i direktivet.

(2) När leverantörer av digitala tjänster fastställer vilka tekniska och organisatoriska åtgärder som är ändamålsenliga och proportionella bör de ta ett systematiskt grepp på informationssäkerheten och tillämpa ett riskbaserat tillvägagångssätt.

(3) För att garantera säkerheten för system och anläggningar bör leverantörer av digitala tjänster genomföra bedömnings- och analysförfaranden. Förfarandena bör omfatta en systematisk förvaltning av nät- och informationssystem, fysisk säkerhet och miljösäkerhet, försörjningstrygghet och åtkomstkontroll.

(4) När leverantörer av digitala tjänster utför en riskanalys inom ramen för en systematisk förvaltning av nät- och informationssystem bör de uppmuntras att identifiera särskilda risker och kvantifiera deras betydelse, t.ex. genom att identifiera hot mot kritiska tillgångar och hur dessa hot påverkar driften och fastställa hur de bäst kan begränsas baserat på befintlig kapacitet och befintliga resurskrav.

(5) Policyn för mänskliga resurser kan avse förvaltningen av kompetens, inklusive aspekter förbundna med utvecklingen av säkerhetsrelaterad kompetens och åtgärder för att öka medvetenheten. Vid fastställandet av ett antal ändamålsenliga policyer för driftssäkerhet bör leverantören av digitala tjänster uppmuntras att ta hänsyn till aspekter rörande förändringshantering, sårbarhetshantering, formaliserade drifts- och förvaltningsmetoder och systemmappning.

(6) Policyerna för säkerhetsarkitektur kan i synnerhet omfatta segregering av nätverk och system liksom specifika säkerhetsåtgärder för kritisk drift såsom förvaltningsdrift. Segregeringen av nätverk och system kan göra det möjligt för en leverantör av digitala tjänster att skilja mellan element som dataflöden och datorresurser som hör till en kund, en grupp av kunder, leverantören av digitala tjänster eller tredje part.

(7) De åtgärder som vidtas med tanke på den fysiska säkerheten och miljösäkerheten bör säkerställa att en organisations nät- och informationssystem skyddas från skador vid incidenter som stöld, brand, översvämning eller annan väderpåverkan samt telekommunikations- eller elavbrott.

(8) Försörjningstryggheten avseende sådant som el, bränsle eller nedkylning bör omfatta säkerheten i försörjningskedjan, vilket i synnerhet innefattar säkerheten hos tredjeparter som är uppdragstagare eller underleverantörer samt deras ledning. Spårbarhet för kritiska insatsprodukter avser förmågan hos leverantören av digitala tjänster att identifiera och registrera källorna till dessa insatsprodukter.

(9) Användare av digitala tjänster bör innefatta fysiska och juridiska personer som är kunder eller abonnenter till en internetbaserad marknadsplats eller en molntjänst eller som besöker en internetbaserad sökmotor för att göra sökningar på ord.

[1] EUT L 194, 19.7.2016, s. 1.

(10) När det fastställs om en incident har en avsevärd inverkan bör de fall som anges i denna förordning anses som en icke-uttömmande förteckning över betydande incidenter. Lärdomar bör dras från genomförandet av denna förordning och från samarbetsgruppens arbete när det gäller insamling av information om bästa praxis avseende risker och incidenter och diskussioner om metoder för rapportering av incidenter enligt artikel 11.3 i och m i direktiv (EU) 2016/1148. Resultatet kan vara övergripande riktlinjer för kvantitativa trösklar för rapporteringsparametrar som kan utlösa rapporteringsskyldigheten för leverantörer av digitala tjänster enligt artikel 16.3 i direktiv (EU) 2016/1148. När så är lämpligt kan kommissionen också överväga att se över de trösklar som för närvarande fastställs i denna förordning.

(11) För att de behöriga myndigheterna ska kunna hålla sig informerade om potentiella nya risker bör leverantörer av digitala tjänster uppmuntras att frivilligt rapportera alla incidenter med särdrag som tidigare varit okända för dem, t.ex. nya tillvägagångssätt, attackbärare eller hotaktörer, sårbarheter och faror.

(12) Förordningen bör börja tillämpas dagen efter det att tidsfristen löpt ut för införlivande av direktiv (EU) 2016/1148.

(13) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté för säkerhet i nätverks- och informationssystem som avses i artikel 22 i direktiv (EU) 2016/1148.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte

Genom denna förordning specificeras mer ingående de aspekter som ska beaktas av leverantörer av digitala tjänster när de fastställer och vidtar åtgärder för att säkerställa en nivå av säkerhet för de nät- och informationssystem som de använder för att erbjuda sådana tjänster som avses i bilaga III till direktiv (EU) 2016/1148 och specificeras mer ingående de parametrar som ska beaktas när det fastställs om en incident har en avsevärd inverkan på tillhandahållandet av dessa tjänster.

Artikel 2

Säkerhetsaspekter

1. Säkerheten i system och anläggningar enligt artikel 16.1 a i direktiv (EU) 2016/1148 avser säkerheten för nät- och informationssystem och deras fysiska miljö och ska innefatta följande aspekter:

a) Systematisk förvaltning av nät- och informationssystem, vilket avser mappning av informationssystem och fastställande av ett antal ändamålsenliga policyer för hantering av informationssäkerheten, inklusive riskanalys, mänskliga resurser, driftssäkerhet, säkerhetsarkitektur, säker livscykelhantering av data och system och, i förekommande fall, kryptering och hantering av sådan kryptering.

b) Fysisk säkerhet och miljösäkerhet, vilket avser tillgången till ett antal åtgärder för att skydda säkerheten för nät- och informationssystem hos leverantörer av digitala tjänster från skador med användning av en riskbaserad strategi som omfattar alla faror och som t.ex. omfattar systemfel, den mänskliga faktorn, avsiktligt skadliga handlingar eller naturfenomen.

c) Försörjningstrygghet, vilket avser införande och upprätthållande av lämpliga policyer för att säkerställa tillgängligheten och i förekommande fall spårbarheten för kritiska insatsprodukter som används för tillhandahållandet av tjänsten.

d) Åtkomstkontroll för nät- och informationssystem, vilket avser tillgången till en uppsättning åtgärder för att säkerställa att den fysiska och logiska åtkomsten till nät- och informationssystem, inklusive administrativ säkerhet för nät och informationssystem, tillåts och begränsas baserat på verksamhetskrav och säkerhetskrav.

2. När det gäller incidenthantering enligt artikel 16.1 b i direktiv (EU) 2016/1148 ska de åtgärder som vidtas av en leverantör av digitala tjänster omfatta följande:

a) Processer och förfaranden för upptäckt som underhålls och testas för att säkerställa snabb och tillräcklig medvetenhet om avvikelser.

b) Processer och metoder för rapportering av incidenter och kartläggning av brister och svagheter i deras informationssystem.

c) Svarsåtgärder i enlighet med fastställda förfaranden och rapportering av resultaten av den vidtagna åtgärden.

d) Bedömning av incidentens allvarlighetsgrad, dokumentation av kunskapen från incidentanalysen och insamling av relevant information som kan tjäna som bevis och bidra till en kontinuerlig förbättringsprocess.

3. Hantering av driftskontinuitet enligt artikel 16.1 c i direktiv (EU) 2016/1148 avser en organisations kapacitet att upprätthålla eller vid behov återställa sitt tillhandahållande av tjänster på godtagbara förhandsdefinierade nivåer efter en incident som orsakar störningar, och den ska innefatta följande:

a) Upprättande och användning av beredskapsplaner baserade på driftskonsekvensanalys för att säkerställa kontinuiteten för de tjänster som tillhandahålls av leverantörer av digitala tjänster, vilka regelbundet ska bedömas och testas, t.ex. genom övningar.

b) Kapacitet för katastrofberedskap, vilken regelbundet ska bedömas och testas, t.ex. genom övningar.

4. Övervakning, revision och testning enligt artikel 16.1 d i direktiv (EU) 2016/1148 ska innefatta fastställandet och upprätthållandet av policyer om följande:

a) Utförandet av en planerad sekvens av observationer och mätningar för att bedöma om nät- och informationssystemen fungerar som avsett.

b) Inspektion och verifiering för att kontrollera om en standard eller en uppsättning riktlinjer följs, om registreringen är tillförlitlig och om effektivitets- och ändamålsenlighetsmål uppfylls.

c) En process avsedd för att avslöja brister i ett nät- och informationssystems säkerhetsmekanismer som skyddar data och upprätthåller funktionerna som avsett. Sådana processer ska innefatta tekniska processer och personal som ingår i driftsflödet.

5. Internationella standarder enligt artikel 16.1 e i direktiv (EU) 2016/1148 avser standarder som antagits av ett internationellt standardiseringsorgan enligt artikel 2.1 a i Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([1]). I enlighet med artikel 19 i direktiv (EU) 2016/1148 får också europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerheten i nät- och informationssystem, inklusive befintliga nationella standarder, användas.

6. Leverantörer av digitala tjänster ska säkerställa att de tillhandahåller den dokumentation som den behöriga myndigheten behöver för att kunna kontrollera att de säkerhetsaspekter som fastställs i punkterna 1, 2, 3, 4 och 5 uppfylls.

Artikel 3

Parametrar som ska beaktas när det fastställs om en incident har en avsevärd inverkan

1. När det gäller antalet användare som påverkas av en incident, i synnerhet användare som är beroende av tjänsten för att tillhandahålla egna tjänster enligt artikel 16.4 a i direktiv (EU) 2016/1148, ska leverantören av digitala tjänster kunna uppskatta antingen

a) antalet påverkade fysiska eller juridiska personer med vilka ett avtal om tillhandahållande av tjänsten har ingåtts, eller

b) antalet påverkade användare som har använt tjänsten baserat på i första hand tidigare trafikdata.

2. Incidentens varaktighet enligt artikel 16.4 b avser tidsperioden från den tidpunkt då tillhandahållandet av tjänsten störs med avseende på tillgången, riktigheten, integriteten eller konfidentialiteten till den tidpunkt då situationen återställts.

3. När det gäller storleken på det geografiska område som påverkas av incidenten enligt artikel 16.4 c i direktiv (EU) 2016/1148 ska leverantören av den digitala tjänsten kunna fastställa om incidenten påverkar tillhandahållandet av leverantörens tjänster i specifika medlemsstater.

4. Den utsträckning i vilken incidenten stör tjänstens funktion enligt artikel 16.4 d i direktiv (EU) 2016/1148 ska mätas med avseende på en eller fler av följande funktioner som försämras av incidenten: Tillgången, riktigheten, integriteten eller konfidentialiteten i fråga om data eller berörda tjänster.

([1]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

5. När det gäller den utsträckning i vilken incidenten inverkar på den ekonomiska och samhälleliga verksamheten enligt artikel 16.4 e i direktiv (EU) 2016/1148 ska leverantören av digitala tjänster, baserat på sådant som arten av leverantörens avtalsförbindelse med kunden eller, när så är lämpligt, det potentiella antalet påverkade användare, kunna fastställa om incidenten har orsakat betydande materiella eller ideella förluster för användarna när det gäller sådant som hälsa, säkerhet eller egendomsskada.

6. Vid tillämpning av punkterna 1, 2, 3, 4 och 5 ska leverantörer av digitala tjänster inte åläggas att samla in ytterligare information som de inte har tillgång till.

Artikel 4

Avsevärd inverkan av en incident

1. En incident ska anses ha avsevärd inverkan när minst en av följande situationer har inträffat:

a) Den tjänst som tillhandahålls av en leverantör av digitala tjänster är otillgänglig under mer än 5 000 000 användartimmar, där begreppet användartimme avser antalet användare som påverkas i unionen under 60 minuter.

b) Incidenten medför en förlust av riktighet, integritet eller konfidentialitet för lagrade, överförda eller behandlade data eller för de tillhörande tjänster som erbjuds eller är tillgängliga via leverantörens nät- och informationssystem och påverkar fler än 100 000 användare i unionen.

c) Incidenten har gett upphov till en risk för allmän ordning, allmän säkerhet eller människoliv.

d) Incidenten orsakar materiella skador för minst en användare i unionen och skadorna för denna användare uppgår till över EUR 1 000 000.

2. Baserat på den bästa praxis som samlats in av samarbetsgruppen inom ramen för dess uppdrag enligt artikel 11.3 i direktiv (EU) 2016/1148 och på diskussionerna enligt artikel 11.3 m i samma direktiv får kommissionen se över de trösklar som fastställs i punkt 1.

Artikel 5

Ikraftträdande

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

2. Den ska tillämpas från och med den 10 maj 2018.

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

Utfärdad i Bryssel den 30 januari 2018.

På kommissionens vägnar

Jean-Claude JUNCKER

Ordförande