UITVOERINGSVERORDENING (EU) 2018/151 VAN DE COMMISSIE

van 30 januari 2018

tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door digitaledienstverleners in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie [1], en met name artikel 16, lid 8,

Overwegende hetgeen volgt:

(1) Overeenkomstig Richtlijn (EU) 2016/1148 moeten digitaledienstverleners de vrijheid behouden om technische en organisatorische maatregelen te treffen die zij passend en evenredig achten ter beheersing van de risico's in verband met de beveiliging van hun netwerk- en informatiesystemen, zolang deze maatregelen een passend beveiligingsniveau waarborgen en rekening houden met de elementen waarin die richtlijn voorziet.

(2) Bij het bepalen van passende en evenredige technische en organisatorische maatregelen moet de digitaledienstverlener informatiebeveiliging op een systematische wijze benaderen, met een op risicoanalyse gebaseerde aanpak.

(3) Om de beveiliging van systemen en voorzieningen te waarborgen, moeten digitaledienstverleners beoordelings- en analyseprocedures toepassen. Deze activiteiten moeten betrekking hebben op het systematische beheer van netwerk- en informatiesystemen, de fysieke en omgevingsbeveiliging, de bevoorradingszekerheid en de toegangscontrole.

(4) Bij het uitvoeren van een risicoanalyse in het kader van het systematische beheer van netwerk- en informatiesystemen moeten digitaledienstverleners worden aangemoedigd om specifieke risico's te identificeren en hun omvang te meten, bijvoorbeeld door te bepalen aan welke bedreigingen kritieke voorzieningen worden blootgesteld en hoe deze van invloed kunnen zijn op de activiteiten, daarbij bepalend wat de beste manier is om deze bedreigingen af te wenden op basis van de bestaande vermogens en benodigde middelen.

(5) Het personeelsbeleid zou betrekking kunnen hebben op het beheer van vaardigheden, waaronder aspecten in verband met de ontwikkeling van vaardigheden en de bewustmaking op het gebied van beveiliging. Bij het nemen van beslissingen over passende beleidsmaatregelen met betrekking tot operationele beveiliging moeten de digitaledienstverleners worden aangemoedigd rekening te houden met aspecten van veranderingsmanagement, kwetsbaarheidsmanagement, de formalisering van de operationele en administratieve praktijken en de inkaartbrenging van systemen.

(6) In het bijzonder de scheiding van netwerken en systemen, en ook specifieke beveiligingsmaatregelen voor kritieke activiteiten, zoals administratieve activiteiten, zouden tot de beleidsmaatregelen op het gebied van beveiligingsarchitectuur kunnen behoren. Door de scheiding van netwerken en systemen zou een digitaledienstverlener een onderscheid kunnen maken tussen elementen (zoals gegevensstromen en computercapaciteit) van een klant, een groep klanten, de digitaledienstverlener zelf of derden.

(7) De maatregelen die worden genomen met betrekking tot de fysieke en omgevingsbeveiliging moeten de netwerk- en informatiesystemen van een organisatie beschermen tegen schade door incidenten zoals diefstal, brand, overstromingen of andere weersverschijnselen, en telecom- of stroomstoringen.

(8) De zekerheid van de elektriciteits-, brandstof- of koelingsbevoorrading zou de bevoorradingszekerheid van de toeleveringsketen kunnen omvatten, waaronder met name de beveiliging van externe aannemers en onderaannemers en hun beheer. Met de traceerbaarheid van kritieke voorraden wordt gedoeld op het vermogen van de digitaledienstverlener om de oorsprong van die voorraden te identificeren en te registreren.

(9) Tot de gebruikers van digitale diensten moeten natuurlijke en rechtspersonen behoren die klant of abonnee zijn van een onlinemarktplaats of cloudcomputingdienst, of die op de website van een onlinezoekmachine aan de hand van trefwoorden zoekopdrachten uitvoeren.

[1] PB L 194 van 19.7.2016, blz. 1.

(10) Bij het bepalen van de mate waarin een incident aanzienlijke gevolgen heeft, moeten de in deze verordening vermelde gevallen als een niet-limitatieve lijst van ernstige incidenten worden beschouwd. Er moeten lessen worden getrokken uit de uitvoering van deze verordening, alsook uit de door de samenwerkingsgroep verzamelde informatie over beste praktijken inzake risico's en incidenten en de door haar besproken nadere bepalingen voor de rapportage betreffende incidentmeldingen, als bedoeld in de punten i) en m) van artikel 11, lid 3), van Richtlijn (EU) 2016/1148. Dit kan uitmonden in uitvoerige richtsnoeren met betrekking tot kwantitatieve drempels voor meldingsparameters die aanleiding kunnen geven tot de bij artikel 16, lid 3, van Richtlijn (EU) 2016/1148 vastgestelde meldingsplicht voor digitaledienstverleners. Indien nodig kan de Commissie ook overwegen om de momenteel in deze verordening vastgestelde drempels te herzien.

(11) Om ervoor te zorgen dat de bevoegde autoriteiten over potentiële nieuwe risico's worden geïnformeerd, moeten de digitaledienstverleners worden aangemoedigd om op vrijwillige basis melding te maken van ieder incident met voorheen onbekende kenmerken, zoals nieuwe exploits, aanvalsvectoren of dreigingsactoren, zwakke punten en gevaren.

(12) Deze verordening moet van toepassing worden op de dag na het verstrijken van de termijn voor omzetting van Richtlijn (EU) 2016/1148.

(13) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het in artikel 22 van Richtlijn (EU) 2016/1148 bedoelde Comité beveiliging netwerk- en informatiesystemen,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp

Deze verordening specificeert nader welke elementen digitaledienstverleners in aanmerking moeten nemen wanneer zij maatregelen treffen ter waarborging van een niveau van beveiliging van netwerk- en informatiesystemen die zij gebruiken bij het aanbieden van de in bijlage III bij Richtlijn (EU) 2016/1148 bedoelde diensten, en met welke parameters rekening moet worden gehouden om te beoordelen of een incident aanzienlijke gevolgen heeft voor de verlening van die diensten.

Artikel 2

Beveiligingselementen

1. Met de in artikel 16, lid 1, onder a), van Richtlijn (EU) 2016/1148 genoemde beveiliging van systemen en voorzieningen wordt de beveiliging van netwerk- en informatiesystemen en hun fysieke omgeving bedoeld, en dit omvat de volgende elementen:

a) het systematische beheer van netwerk- en informatiesystemen, d.w.z. het in kaart brengen van informatiesystemen en het nemen van een reeks passende beleidsmaatregelen met betrekking tot het informatiebeveiligingsbeheer, inclusief risicoanalyse, personele middelen, operationele beveiliging, beveiligingsarchitectuur, het beheer van de hele levenscyclus van beveiligde data en systemen en, indien van toepassing, encryptie en het beheer ervan;

b) fysieke en omgevingsbeveiliging, d.w.z. de beschikbaarheid van een reeks maatregelen om de netwerk- en informatiesystemen van digitaledienstverleners tegen schade te beschermen door middel van een op risicoanalyse gebaseerde aanpak waarbij rekening wordt gehouden met bijvoorbeeld systeemstoringen, menselijke fouten, vijandelijke acties of natuurverschijnselen;

c) de bevoorradingszekerheid, d.w.z. de totstandbrenging en instandhouding van passende beleidsmaatregelen om de toegankelijkheid en, in voorkomend geval, de traceerbaarheid van kritieke voorraden voor de verlening van de diensten te waarborgen;

d) de toegangscontroles voor netwerk- en informatiesystemen, d.w.z. de beschikbaarheid van een reeks maatregelen om te waarborgen dat de fysieke en logische toegang tot netwerk- en informatiesystemen, inclusief de administratieve beveiliging van netwerk- en informatiesystemen, wordt toegestaan en beperkt op basis van bedrijfsmatige en beveiligingseisen.

2. Wat betreft de behandeling van incidenten als bedoeld in artikel 16, lid 1, onder b), van Richtlijn (EU) 2016/1148, omvatten de door de digitaledienstverlener te nemen maatregelen het volgende:

a) detectieprocessen en -procedures die worden gehandhaafd en getest om ervoor te zorgen dat afwijkende gebeurtenissen tijdig en passend worden opgemerkt;

b) processen en beleidsmaatregelen om incidenten te melden en tekortkomingen en zwakke plekken in hun informatiesystemen te identificeren;

c) een respons conform vastgestelde procedures en de rapportage van de resultaten van de genomen maatregelen;

d) een beoordeling van de ernst van het incident, waarbij informatie uit de analyse van het incident en relevante informatie worden verzameld die als bewijsmateriaal kunnen dienen en kunnen helpen bij het continue verbeteringsproces.

3. Het beheer van de bedrijfscontinuïteit als bedoeld in artikel 16, lid 1, onder c), van Richtlijn (EU) 2016/1148 betekent het vermogen van een organisatie om de dienstverlening na een verstorend incident te handhaven of in voorkomend geval te herstellen tot vooraf vastgestelde aanvaardbare niveaus, en omvat:

a) de vaststelling en het gebruik van rampenplannen op basis van een bedrijfsimpactanalyse ter waarborging van de continuïteit van de door digitaledienstverleners aangeboden diensten, die op regelmatige basis worden beoordeeld en getest, bijvoorbeeld door middel van oefeningen;

b) uitwijkcapaciteiten die op regelmatige basis worden beoordeeld en getest, bijvoorbeeld door middel van oefeningen.

4. Het toezicht, de controle en de testen als bedoeld in artikel 16, lid 1), onder d), van Richtlijn (EU) 2016/1148 omvatten de vaststelling en handhaving van beleidsmaatregelen inzake:

a) de uitvoering van een geplande sequentie van waarnemingen of metingen om te beoordelen of de netwerk- en informatiesystemen naar behoren werken;

b) inspectie en verificatie om na te gaan of aan een norm of reeks richtsnoeren wordt voldaan, of de gegevens accuraat zijn en of de efficiëntie- en effectiviteitsdoelstellingen worden gehaald;

c) een proces om zwakke plekken aan het licht te brengen in de beveiligingsmechanismen van een netwerk- en informatiesysteem ter bescherming van gegevens en ter behoud van de bedoelde functionaliteit. Een dergelijk proces omvat technische processen en personeelsleden die bij de activiteit betrokken zijn.

5. Onder internationale normen als bedoeld in artikel 16, lid 1), onder e), van Richtlijn (EU) 2016/1148 worden normen verstaan die zijn vastgesteld door een internationale normalisatie-instelling als bedoeld in artikel 2, lid 1, onder a), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad [1]. Overeenkomstig artikel 19 van Richtlijn (EU) 2016/1148 kunnen ook Europese of internationaal aanvaarde normen en specificaties voor de beveiliging van netwerk- en informatiesystemen, met inbegrip van bestaande nationale normen, worden gebruikt.

6. Digitaledienstverleners zorgen ervoor dat zij over passende documentatie beschikken zodat de bevoegde autoriteit kan nagaan of aan de in de leden 1 tot en met 5 bedoelde beveiligingselementen wordt voldaan.

Artikel 3

In aanmerking te nemen parameters om te bepalen of een incident aanzienlijke gevolgen heeft

1. Wat betreft het aantal gebruikers dat door het incident wordt getroffen, in het bijzonder gebruikers die de dienst nodig hebben voor de verlening van hun eigen diensten, als bedoeld in artikel 16, lid 4, onder a), van Richtlijn (EU) 2016/1148, is de digitaledienstverlener in staat het volgende ramen:

a) het aantal getroffen natuurlijke personen en rechtspersonen waarmee een dienstenovereenkomst is gesloten, of

b) het aantal getroffen gebruikers van de dienst op basis van eerdere internetverkeersgegevens.

2. Met de duur van een incident als bedoeld in artikel 16, lid 4, onder b) van Richtlijn (EU) 2016/1148 wordt de tijdspanne bedoeld vanaf het moment dat de dienst niet meer naar behoren werkt op het vlak van beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid, tot het moment van volledig herstel van de dienst.

3. Wat betreft de omvang van het geografische gebied dat door het incident is getroffen, als bedoeld in artikel 16, lid 4, onder c), van Richtlijn (EU) 2016/1148, is de digitaledienstverlener in staat na te gaan of het incident gevolgen heeft voor zijn dienstverlening in specifieke lidstaten.

4. De omvang van de verstoring van de werking van de dienst als bedoeld in artikel 16, lid 4, onder d), van Richtlijn (EU) 2016/1148, wordt gemeten met betrekking tot een of meer van de volgende kenmerken die in het gedrang komen door een incident: de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de gegevens of de daaraan gerelateerde diensten.

---

[1] Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

5. Wat betreft de omvang van de impact op de economische en maatschappelijke activiteiten als bedoeld in artikel 16, lid 4, onder e), van Richtlijn (EU) 2016/1148, is de digitaledienstverlener in staat om op basis van indicaties zoals de aard van zijn contractuele betrekkingen met de klant of, in voorkomend geval, het potentiële aantal getroffen gebruikers, te besluiten of het incident heeft geleid tot aanzienlijke materiële of immateriële schade voor de gebruikers, bijvoorbeeld op het vlak van gezondheid, veiligheid of schade aan eigendommen.

6. Voor de toepassing van de leden 1 tot en met 5 zijn de digitaledienstverleners niet verplicht aanvullende informatie te verzamelen waar zijn geen toegang toe hebben.

Artikel 4

Aanzienlijke gevolgen van een incident

1. Van een incident zal worden geacht dat het aanzienlijke gevolgen heeft indien minstens één van de volgende situaties heeft plaatsgevonden:

a) de door een digitaledienstverlener verleende dienst was gedurende meer dan 5 000 000 gebruikersuren onbeschikbaar, waarbij het begrip gebruikersuur verwijst naar het aantal gebruikers in de Unie dat getroffen is voor een tijdspanne van zestig minuten;

b) het incident heeft geleid tot een verlies aan integriteit, authenticiteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die worden aangeboden door, of toegankelijk zijn via een netwerk- en informatiesysteem van, de digitaledienstverlener, waarbij meer dan 100 000 gebruikers in de Unie zijn getroffen;

c) Het incident heeft geleid tot een risico voor de openbare veiligheid, de openbare beveiliging of tot een risico van verlies van mensenlevens;

d) het incident heeft voor minstens één gebruiker in de Unie materiële schade veroorzaakt, waarbij de schade voor die gebruiker meer dan 1 000 000 EUR bedraagt.

2. Op basis van de beste praktijken die zijn verzameld door de samenwerkingsgroep in het kader van de uitoefening van haar taken uit hoofde van artikel 11, lid 3, van Richtlijn (EU) 2016/1148 en op basis van de besprekingen als bedoeld in artikel 11, lid 3, onder m), kan de Commissie de in lid 1 vastgestelde drempels herzien.

Artikel 5

Inwerkingtreding

1. Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

2. Zij is van toepassing met ingang van 10 mei 2018.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 30 januari 2018.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER