AANBEVELINGEN

AANBEVELING (EU) 2019/553 VAN DE COMMISSIE

van 3 april 2019

over cyberbeveiliging in de energiesector

(Kennisgeving geschied onder nummer C(2019) 2400)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 292,

Overwegende hetgeen volgt:

(1) De Europese energiesector maakt een belangrijke ontwikkeling naar een koolstofvrije economie door, waarbij ook de voorzieningszekerheid en het concurrentievermogen worden gewaarborgd. In het kader van deze energietransitie en de daarmee verband houdende decentralisatie van de opwekking van elektriciteit uit hernieuwbare bronnen, maken de technologische vooruitgang, de sectorkoppeling en de digitalisering dat het Europese elektriciteitsnet in een "slim net" verandert. Dit brengt ook nieuwe risico's met zich mee, aangezien digitalisering het energiesysteem steeds meer blootstelt aan cyberaanvallen en -incidenten die de energievoorzieningszekerheid in gevaar kunnen brengen.

(2) Dankzij de aanneming van alle acht wetgevingsvoorstellen ([1]) van het pakket "Schone energie voor alle Europeanen", met de governance van de energie-unie als opstapje, kan een gunstig klimaat tot stand worden gebracht voor de digitale transformatie van de energiesector. Ook wordt belang gehecht aan cyberbeveiliging in de energiesector. Met name de herschikking van de verordening betreffende de interne markt voor elektriciteit ([2]) voorziet in de vaststelling van technische voorschriften voor elektriciteit, zoals een netcode inzake sectorspecifieke regels voor cyberbeveiligingsaspecten van grensoverschrijdende elektriciteitsstromen, inzake gemeenschappelijke minimumvereisten, planning, monitoring, rapportage en crisisbeheer. In de verordening betreffende de risicoparaatheid in de elektriciteitssector ([3]) wordt in grote lijnen de aanpak gevolgd die is gekozen in de verordening betreffende de veiligstelling van de gasleveringszekerheid ([4]), wordt benadrukt dat alle risico's naar behoren moeten worden geanalyseerd, inclusief de risico's in verband met cyberbeveiliging, en wordt voorgesteld maatregelen te nemen om deze risico's te voorkomen en te beperken.

(3) Toen de Commissie in 2013 de strategie inzake cyberbeveiliging van de Europese Unie ([5]) vaststelde, werd de cyberweerbaarheid van de Unie als een prioriteit aangemerkt. Een van de belangrijkste resultaten van de strategie is de in juli 2016 vastgestelde richtlijn cyberbeveiliging ([6]) (hierna "NIS-richtlijn" genoemd). De NIS-richtlijn is de eerste horizontale EU-wetgeving inzake cyberbeveiliging en zorgt voor een hoger algeheel niveau van cyberbeveiliging in de Unie, omdat nationale cyberbeveiligingscapaciteiten worden ontwikkeld, de samenwerking op EU-niveau wordt opgevoerd en verplichtingen inzake beveiliging en de melding van incidenten worden opgelegd aan ondernemingen waarnaar wordt verwezen als "aanbieders van essentiële diensten". De melding van incidenten is verplicht in belangrijke sectoren zoals de energiesector.

([1]) Richtlijn (EU) 2018/2001 van het Europees Parlement en de Raad van 11 december 2018 ter bevordering van het gebruik van energie uit hernieuwbare bronnen (PB L 328 van 21.12.2018, blz. 82); Richtlijn (EU) 2018/2002 van het Europees Parlement en de Raad van 11 december 2018 houdende wijziging van Richtlijn 2012/27/EU betreffende energie-efficiëntie (PB L 328 van 21.12.2018, blz. 210); Verordening (EU) 2018/1999 van het Europees Parlement en de Raad van 11 december 2018 inzake de governance van de energie-unie en van de klimaatactie, tot wijziging van Richtlijn 94/22/EG, Richtlijn 98/70/EG, Richtlijn 2009/31/EG, Verordening (EG) nr. 663/2009, Verordening (EG) nr. 715/2009, Richtlijn 2009/73/EG, Richtlijn 2009/119/EG van de Raad, Richtlijn 2010/31/EU, Richtlijn 2012/27/EU, Richtlijn 2013/30/EU en Richtlijn (EU) 2015/652 van de Raad, en tot intrekking van Verordening (EU) nr. 525/2013 (PB L 328 van 21.12.2018, blz. 1); Richtlijn (EU) 2018/844 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn 2010/31/EU betreffende de energieprestatie van gebouwen en Richtlijn 2012/27/EU betreffende energie-efficiëntie (PB L 156 van 19.6.2018, blz. 75). Tijdens de plenaire vergadering van maart 2019 bekrachtigde het Europees Parlement de politieke akkoorden met de Raad over de voorstellen voor de opzet van de elektriciteitsmarkt (de risicoparaatheidsverordening, de verordening betreffende het Agentschap voor de samenwerking tussen energieregulators (ACER), de elektriciteitsrichtlijn en de elektriciteitsverordening). De formele aanneming door de Raad volgt naar verwachting in april; de wettekst zal kort daarna in het Publicatieblad worden bekendgemaakt.

([2]) COM(2016) 861.

([3]) COM(2016) 862.

([4]) Verordening (EU) 2017/1938 van het Europees Parlement en de Raad van 25 oktober 2017 betreffende maatregelen tot veiligstelling van de gasleveringszekerheid en houdende intrekking van Verordening (EU) nr. 994/2010 (PB L 280 van 28.10.2017, blz. 1).

([5]) JOIN(2013) 1 final.

([6]) 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 (PB L 194 van 19.7.2016, blz. 1).

(4) Bij de uitvoering van paraatheidsmaatregelen op het gebied van cyberbeveiliging moeten de relevante belanghebbenden, waaronder de in de NIS-richtlijn vermelde aanbieders van essentiële diensten in de energiesector, rekening houden met de horizontale richtsnoeren van de op grond van artikel 11 van de NIS-richtlijn opgerichte NIS-samenwerkingsgroep. Die samenwerkingsgroep, die bestaat uit vertegenwoordigers van de lidstaten, het agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en de Commissie, heeft richtsnoeren vastgesteld met betrekking tot beveiligingsmaatregelen en de melding van incidenten. In juni 2018 heeft de samenwerkingsgroep een specifieke werkstroom over energie opgezet.

(5) In de gezamenlijke mededeling van 2017 over cyberbeveiliging ([7]) wordt het belang erkend van sectorspecifieke overwegingen en voorschriften op EU-niveau, onder meer in de energiesector. De voorbije jaren is in de Unie uitgebreid gedebatteerd over cyberbeveiliging en mogelijke gevolgen voor het beleid. Daarom groeit vandaag het besef dat bepaalde economische sectoren worden geconfronteerd met specifieke cyberbeveiligingsproblemen en dus een eigen sectorale benadering moeten ontwikkelen in het bredere kader van algemene cyberbeveiligingsstrategieën.

(6) Informatie-uitwisseling en vertrouwen zijn essentieel als het om cyberbeveiliging gaat. De Commissie wil ervoor zorgen dat de relevante belanghebbenden beter informatie uitwisselen en doet dit door specifieke evenementen te organiseren, zoals de in maart 2017 in Rome georganiseerde rondetafelconferentie op hoog niveau over cyberbeveiliging in de energiesector en de in oktober 2018 in Brussel gehouden conferentie op hoog niveau over cyberbeveiliging in de energiesector. De Commissie wil ook zorgen voor meer samenwerking tussen relevante belanghebbenden en gespecialiseerde entiteiten zoals het European Energy Information Sharing and Analysis Centre (Europees Centrum voor uitwisseling en analyse van informatie over energie).

(7) Met de verordening inzake Enisa (het agentschap van de Europese Unie voor cyberbeveiliging) en de verordening inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening") ([8]) wordt het mandaat van het agentschap van de Europese Unie voor cyberbeveiliging versterkt zodat het meer ondersteuning kan bieden aan de lidstaten bij hun aanpak van cyberdreigingen en -aanvallen. Ook creëert dit een Europees cyberbeveiligingskader voor de certificering van producten, processen en diensten, dat in de hele Unie geldig is en van bijzonder belang is voor de energiesector.

(8) De Commissie heeft een aanbeveling ([9]) uitgebracht met betrekking tot cyberbeveiligingsrisico's in de netwerktechnologieën van de vijfde generatie (5G) door richtsnoeren vast te stellen over passende risicoanalyse en beheersmaatregelen op nationaal niveau, de ontwikkeling van een gecoördineerde Europese risicoanalyse en de vaststelling van een proces voor de ontwikkeling van een gemeenschappelijk instrumentarium van beste risicobeheersmaatregelen. Zodra ze zijn uitgerold zullen 5G-netwerken de ruggengraat vormen van een breed scala aan diensten die van essentieel belang zijn voor de werking van de interne markt en van onmisbare maatschappelijke en economische functies zoals energie.

(9) Deze aanbeveling moet de lidstaten en relevante belanghebbenden, met name netbeheerders en technologieleveranciers, niet-exhaustieve leidraden bieden om een hoger niveau van cyberbeveiliging te bereiken, rekening houdend met de specifieke realtimevereisten die in de energiesector zijn vastgesteld, cascade-effecten en de combinatie van oudere en geavanceerde technologieën. Deze richtsnoeren zijn bedoeld om belanghebbenden te helpen rekening te houden met de specifieke eisen van de energiesector wanneer zij internationaal erkende cyberbeveiligingsnormen ([10]) toepassen.

(10) De Commissie is voornemens deze aanbeveling regelmatig te herzien op basis van de in de Unie geboekte vooruitgang, in overleg met de lidstaten en de relevante belanghebbenden. De Commissie zal zich blijven inspannen om de cyberbeveiliging in de energiesector te versterken, met name via de NIS-samenwerkingsgroep, die zorgt voor strategische samenwerking en informatie-uitwisseling tussen de lidstaten op het gebied van cyberbeveiliging.

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

ONDERWERP

1) In deze aanbeveling worden de belangrijkste kwesties in verband met cyberbeveiliging in de energiesector uiteengezet — met name realtimevereisten, cascade-effecten en de combinatie van oudere en geavanceerde technologieën — en worden de belangrijkste acties voor de uitvoering van relevante maatregelen voor cyberbeveiligingsparaatheid in de energiesector vastgesteld.

([7]) JOIN(2017) 450 final.
([8]) De cyberbeveiligingsverordening werd in maart 2019 door het Europees Parlement aangenomen. De formele aanneming door de Raad volgt naar verwachting in april; de wettekst zal kort daarna in het Publicatieblad worden bekendgemaakt.
([9]) C(2019) 2335.
([10]) Internationale normalisatieorganisaties hebben diverse cyberbeveiligingsnormen (ISO/IEC 27000: Informatietechnologie) en risicobeheernormen (ISO/IEC 31000: uitvoering van risicobeheer) vastgesteld. Een specifieke norm voor de energiesector (ISO/IEC 27019: informatiebeveiligingscontroles voor energiemaatschappijen) werd als onderdeel van de reeks ISO/IEC 27000 in oktober 2017 vastgesteld.

2) Bij de toepassing van deze aanbeveling moeten de lidstaten de relevante belanghebbenden aanmoedigen om kennis en vaardigheden op te bouwen met betrekking tot cyberbeveiliging in de energiesector. Waar passend moeten de lidstaten deze overwegingen ook opnemen in hun nationale kader voor cyberbeveiliging, met name via strategieën, wetten, voorschriften en andere administratieve bepalingen.

REALTIMEVEREISTEN VOOR COMPONENTEN VAN DE ENERGIE-INFRASTRUCTUUR

3) De lidstaten moeten ervoor zorgen dat de relevante belanghebbenden, met name energienetwerkbeheerders en technologieleveranciers, en in het bijzonder aanbieders van essentiële diensten die in het kader van de NIS-richtlijn zijn aangemerkt, de relevante maatregelen voor cyberbeveiligingsparaatheid treffen als het gaat om de realtimevereisten in de energiesector. Sommige elementen van het energiesysteem moeten in real time werken, d.w.z. binnen een paar milliseconden reageren op commando's. Door dit gebrek aan tijd wordt het moeilijk of zelfs onmogelijk om cyberbeveiligingsmaatregelen te treffen.

4) Energienetwerkbeheerders moeten met name:

a) waar passend de meest recente beveiligingsnormen toepassen voor nieuwe installaties en aanvullende fysieke beveiligingsmaatregelen overwegen wanneer de geïnstalleerde basis van oude installaties niet voldoende kan worden beschermd met cyberbeveiligingsmechanismen;

b) internationale cyberbeveiligingsnormen en adequate specifieke technische normen toepassen met het oog op veilige realtimecommunicatie zodra de respectieve producten in de handel verkrijgbaar zijn;

c) realtimebeperkingen overwegen in het algehele beveiligingsconcept voor activa, met name met betrekking tot de classificatie van activa;

d) netwerken in particulier bezit overwegen wanneer het gaat om regelingen voor beveiliging met signaaloverdracht, om de kwaliteit van de dienstverlening te waarborgen die nodig is voor realtimebeperkingen; bij het gebruik van openbare communicatienetwerken moeten de beheerders toekenning van specifieke bandbreedtes, eisen inzake latentietijden en maatregelen op het gebied van communicatiebeveiliging in overweging nemen;

e) het algemene systeem in logische zones verdelen en binnen elke zone tijds- en procesbeperkingen vaststellen zodat passende maatregelen op het gebied van cyberbeveiliging kunnen worden getroffen of alternatieve beschermingsmethoden kunnen worden overwogen.

5) Waar mogelijk moeten de energienetwerkbeheerders ook:

a) een beveiligd communicatieprotocol kiezen, rekening houdend met realtimevereisten, bijvoorbeeld tussen een installatie en de bijbehorende beheersystemen (energiebeheersysteem (EMS)/distributiebeheersysteem (DMS));

b) een passend authenticatiemechanisme voor communicatie tussen machines invoeren, waarbij de realtimevereisten worden aangepakt.

CASCADE-EFFECTEN

6) De lidstaten moeten ervoor zorgen dat de relevante belanghebbenden, met name energienetwerkbeheerders en technologieleveranciers, en in het bijzonder aanbieders van essentiële diensten die in het kader van de NIS-richtlijn zijn aangemerkt, de relevante maatregelen voor cyberbeveiligingsparaatheid treffen als het gaat om cascade-effecten in de energiesector. Elektriciteitsnetten en gaspijpleidingen zijn in Europa sterk met elkaar verbonden en een cyberaanval die een onderbreking of verstoring in een deel van het energiesysteem veroorzaakt, kan verreikende cascade-effecten teweegbrengen in andere delen van dat systeem.

7) Bij de toepassing van deze aanbeveling moeten de lidstaten een beoordeling maken van de onderlinge afhankelijkheid en het kritieke karakter van systemen voor elektriciteitsopwekking en systemen voor flexibele vraag, onderstations en lijnen voor transmissie en distributie, en de getroffen belanghebbenden (ook in grensoverschrijdende situaties) in het geval van een succesvolle cyberaanval of een cyberincident. De lidstaten moeten er ook voor zorgen dat energienetwerkbeheerders over een kader voor communicatie met alle belangrijke belanghebbenden beschikken zodat ze vroegtijdige waarschuwingssignalen kunnen delen en kunnen samenwerken op het vlak van crisisbeheer. Er moeten gestructureerde communicatiekanalen en overeengekomen formaten worden vastgesteld om gevoelige informatie te delen met alle relevante belanghebbenden, Computer Security Incident Response Teams en relevante autoriteiten.

8) Energienetwerkbeheerders moeten met name:

a) ervoor zorgen dat nieuwe apparaten, waaronder toestellen die verbonden zijn met het internet der dingen (Internet of Things — IoT), een cyberbeveiligingsniveau hebben en behouden dat passend is voor het kritieke karakter van een locatie;

b) cyberfysieke effecten op een passende manier in overweging nemen bij de vaststelling en periodieke herziening van bedrijfscontinuïteitsplannen;

c) ontwerpcriteria vaststellen, alsook een architectuur voor een weerbaar net, hetgeen kan worden bereikt door:

— de invoering van grondige beschermingsmaatregelen per locatie, aangepast aan het kritieke karakter van de locatie;

— kritieke knooppunten in kaart te brengen, zowel wat de productiecapaciteit als de impact op de afnemers betreft; Bij het ontwerp van kritieke functies van een net moet het risico op cascade-effecten worden beperkt door na te denken over redundantie, weerbaarheid tegen fase-oscillatie en bescherming tegen belastingsuitschakeling in cascade;

— samen te werken met andere relevante beheerders en technologieleveranciers om cascade-effecten te voorkomen door middel van passende maatregelen en diensten;

— communicatie- en controlenetwerken te ontwerpen en te bouwen om de gevolgen van fysieke en logische storingen te beperken tot afgebakende delen van de netwerken en om te zorgen voor adequate en snelle risicobeperkende maatregelen.

OUDERE EN GEAVANCEERDE TECHNOLOGIE

9) De lidstaten moeten ervoor zorgen dat de relevante belanghebbenden, met name energienetwerkbeheerders en technologieleveranciers, en in het bijzonder aanbieders van essentiële diensten die in het kader van de NIS-richtlijn zijn aangemerkt, de relevante maatregelen voor cyberbeveiligingsparaatheid treffen als het gaat om de combinatie van oudere en geavanceerde technologie in de energiesector. In het huidige energiesysteem worden namelijk twee verschillende technologieën naast elkaar gebruikt: een oudere technologie met een levensduur van 30 tot 60 jaar die is ontworpen toen er nog rekening moest worden gehouden met cyberbeveiliging, en moderne apparatuur, die is aangepast aan de meest recente digitalisering en aan slimme apparaten.

10) Bij de toepassing van deze aanbeveling dienen de lidstaten de energienetwerkbeheerders en technologieleveranciers aan te moedigen waar mogelijk de relevante internationaal aanvaarde cyberbeveiligingsnormen te volgen. Belanghebbenden en afnemers moeten op hun beurt een aanpak volgen die gericht is op cyberbeveiliging wanneer zij dergelijke apparaten op het net aansluiten.

11) Met name de technologieleveranciers moeten, zodra een relevant veiligheidsprobleem met betrekking tot oudere of nieuwe technologieën wordt vastgesteld, kosteloos beproefde oplossingen aanbieden.

12) Energienetwerkbeheerders moeten met name:

a) analyseren welke risico's verbonden zijn aan het verbinden van oudere concepten met IoT-concepten en moeten zich bewust zijn van interne en externe interfaces en hun kwetsbaarheden;

b) passende maatregelen nemen tegen kwaadwillige aanvallen die afkomstig zijn van een groot aantal kwaadwillig gecontroleerde consumentenapparaten of -toepassingen;

c) zorgen voor een geautomatiseerde monitoring- en analysecapaciteit voor beveiligingsgerelateerde gebeurtenissen in oudere omgevingen en IoT-omgevingen, zoals mislukte pogingen om in te loggen, deuralarmen die afgaan bij het openen van een kast, of andere gebeurtenissen.

d) regelmatig specifieke risicoanalyses met betrekking tot cyberbeveiliging uitvoeren op alle oudere installaties, met name wanneer oude en nieuwe technologieën met elkaar worden verbonden; aangezien de oudere installaties vaak een zeer groot aantal activa vertegenwoordigen, kan een risicoanalyse worden uitgevoerd aan de hand van klassen van activa;

e) software en hardware van oudere systemen en IoT-systemen waar nodig updaten naar de meest recente versie; wanneer patches of updates adequaat zouden zijn, maar niet kunnen worden geïnstalleerd, bijvoorbeeld bij niet-ondersteunde producten, moeten de energienetwerkbeheerders aanvullende maatregelen overwegen, zoals de opdeling van het systeem of het toevoegen van externe veiligheidsbarrières;

f) bij het uitschrijven van aanbestedingen rekening houden met cyberbeveiliging, dat wil zeggen informatie vragen over veiligheidskenmerken, eisen dat bestaande cyberbeveiligingsnormen worden nageleefd, dat er op continue basis voor waarschuwingen, patches en voorstellen voor risicobeperkende maatregelen wordt gezorgd als er zwakke plekken worden ontdekt, en de aansprakelijkheid van de verkoper in geval van cyberaanvallen of -incidenten verduidelijken;

g) samenwerken met technologieleveranciers om oudere systemen te vervangen wanneer dat om veiligheidsredenen nuttig is, maar daarbij rekening houden met de kritieke functies van de systemen.

TOEZICHT

13) De lidstaten moeten de Commissie via de NIS-samenwerkingsgroep binnen twaalf maanden na de vaststelling van deze aanbeveling en vervolgens om de twee jaar gedetailleerde informatie verstrekken over de stand van uitvoering van deze aanbeveling.

EVALUATIE

14) Op basis van de door de lidstaten verstrekte informatie zal de Commissie de uitvoering van deze aanbeveling evalueren en in overleg met de lidstaten en de relevante belanghebbenden beoordelen of eventuele verdere maatregelen nodig zijn.

ADRESSATEN

15) Deze aanbeveling is gericht tot de lidstaten.

Gedaan te Brussel, 3 april 2019.

Voor de Commissie
Miguel ARIAS CAÑETE
Lid van de Commissie