HENSTILLINGER

KOMMISSIONENS HENSTILLING (EU) 2019/553

af 3. april 2019

om cybersikkerhed i energisektoren

(meddelt under nummer C(2019) 2400)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 292, og

ud fra følgende betragtninger:

(1) Den europæiske energisektor er i gang med en vigtig omstilling til en kulstoffattig økonomi og sikrer samtidig forsyningssikkerheden og konkurrenceevnen. Som led i denne energiomstilling og den dermed forbundne decentralisering af elproduktionen fra vedvarende energikilder er teknologiske fremskridt, sektorkobling og digitalisering ved at omdanne Europas elnet til et »intelligent net«. Samtidig indebærer dette også nye risici, idet digitaliseringen i stigende grad eksponerer energisystemet for cyberangreb og -hændelser, som kan bringe energiforsyningssikkerheden i fare.

(2) Vedtagelsen af alle otte lovgivningsforslag ([1]) i pakken om ren energi til alle europæere, herunder om forvaltningen af energiunionen som en trædesten, gør det muligt at skabe et gunstigt miljø for den digitale omstilling af energisektoren. I aftalen anerkendes ligeledes betydningen af cybersikkerhed i energisektoren. Omarbejdningen af forordningen om det indre marked for elektricitet ([2]) indeholder navnlig bestemmelser om vedtagelse af tekniske regler om elektricitet, f.eks. netregler om sektorspecifikke regler for cybersikkerhedsaspekter af grænseoverskridende elektricitetsstrømme, om fælles minimumskrav, planlægning, overvågning, rapportering og krisestyring. Forordningen om risikoberedskab i elsektoren ([3]) følger stort set den tilgang, der er valgt i forordningen om gasforsyningssikkerhed ([4]), idet det understreges, at alle risici, herunder risici i forbindelse med cybersikkerhed, skal vurderes behørigt, og det foreslås at vedtage foranstaltninger til at forebygge og afbøde disse risici.

(3) Da Kommissionen vedtog EU-strategien for cybersikkerhed ([5]) i 2013, blev styrkelsen af Unionens cyberrobusthed identificeret som en prioritet. Et af de vigtigste mål for strategien er direktivet om net- og informationssikkerhed ([6]) (i det følgende benævnt »NIS-direktivet«), som blev vedtaget i juli 2016. Som den første horisontale EU-lovgivning om cybersikkerhed styrker NIS-direktivet det generelle cybersikkerhedsniveau i Unionen gennem udvikling af de nationale cybersikkerhedskapaciteter, øget samarbejde på EU-plan og indførelse af forpligtelser for virksomheder, der benævnes »operatører af væsentlige tjenester«, til at indberette sikkerhedshændelser. Underretning om hændelser er obligatorisk i nøglesektorer, herunder energisektoren.

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 af 11. december 2018 om fremme af anvendelsen af energi fra vedvarende energikilder (EUT L 328 af 21.12.2018, s. 82), Europa-Parlamentets og Rådets direktiv (EU) 2018/2002 af 11. december 2018 om ændring af direktiv 2012/27/EU om energieffektivitet (EUT L 328 af 21.12.2018, s. 210), Europa-Parlamentets og Rådets forordning (EU) 2018/1999 af 11. december 2018 om forvaltning af energiunionen og klimaindsatsen, om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 663/2009 og (EF) nr. 715/2009, Europa-Parlamentets og Rådets direktiv 94/22/EF, 98/70/EF, 2009/31/EF, 2009/73/EF, 2010/31/EU, 2012/27/EU og 2013/30/EU, Rådets direktiv 2009/119/EF og (EU) 2015/652 og om ophævelse af Europa-Parlamentets og Rådets forordning (EU) nr. 525/2013 (EUT L 328 af 21.12.2018, s. 1) og Europa-Parlamentets og Rådets direktiv (EU) 2018/844 af 30. maj 2018 om ændring af direktiv 2010/31/EU om bygningers energimæssige ydeevne og direktiv 2012/27/EU om energieffektivitet (EUT L 156 af 19.6.2018, s. 75). Europa-Parlamentet bekræftede de politiske aftaler, der blev indgået med Rådet om forslagene til udformning af elektricitetsmarkedet (forordningen om risikoberedskab, forordningen vedrørende Agenturet for Samarbejde mellem Energireguleringsmyndigheder (ACER) og elektricitetsdirektivet og elektricitetsforordningen på plenarforsamlingen i marts 2019. Rådets formelle vedtagelse forventes at finde sted i april, og offentliggørelsen af retsakten i EUT følger kort tid derefter.

([2]) COM(2016) 861.

([3]) COM(2016) 862.

([4]) Europa-Parlamentets og Rådets forordning (EU) 2017/1938 af 25. oktober 2017 om foranstaltninger til opretholdelse af gasforsyningssikkerheden og ophævelse af forordning (EU) nr. 994/2010 (EUT L 280 af 28.10.2017, s. 1).

([5]) JOIN(2013) 1.

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

(4) Når der gennemføres beredskabsforanstaltninger inden for cybersikkerhed, bør de relevante interessenter, herunder operatører af væsentlige energitjenester, der er udpeget i henhold til NIS-direktivet, tage hensyn til de horisontale retningslinjer udstedt af NIS-samarbejdsgruppen, der er nedsat i henhold til artikel 11 i NIS-direktivet. Denne samarbejdsgruppe, der består af repræsentanter for medlemsstaterne, Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og Kommissionen, har vedtaget vejledninger om sikkerhedsforanstaltninger og underretning om hændelser. I juni 2018 etablerede denne gruppe en særlig arbejdsstrøm om energi.

(5) I den fælles meddelelse om cybersikkerhed fra 2017 ([7]) anerkendes betydningen af sektorspecifikke overvejelser og krav på EU-plan, herunder i energisektoren. Cybersikkerhed og mulige politiske konsekvenser har været genstand for indgående drøftelser i Unionen i de seneste år. Der er derfor i dag stigende bevidsthed om, at de enkelte økonomiske sektorer står over for specifikke problemer med cybersikkerheden, og de skal derfor udvikle deres egen sektorspecifikke tilgang i en bredere sammenhæng med generelle cybersikkerhedsstrategier.

(6) Udveksling af oplysninger og tillid er afgørende for cybersikkerheden. Kommissionen sigter mod at øge udvekslingen af oplysninger mellem de relevante interessenter ved at tilrettelægge særlige arrangementer såsom rundbordsdiskussionen på højt plan om cybersikkerhed inden for energi, der blev afholdt i Rom i marts 2017, og konferencen på højt plan om cybersikkerhed inden for energi, der blev afholdt i Bruxelles i oktober 2018. Kommissionen ønsker også at styrke samarbejdet mellem relevante interessenter og specialiserede enheder såsom det europæiske informationsudvekslings- og analysecenter.

(7) Forordningen om ENISA, »EU's Agentur for Cybersikkerhed«, og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (»forordningen om cybersikkerhed« ([8])) vil styrke EU's Agentur for Cybersikkerheds mandat, således at det bedre kan støtte medlemsstaterne i håndteringen af cybersikkerhedstrusler og -angreb. Den skaber også en europæisk ramme for certificering af produkter, processer og tjenesteydelser, som vil være gyldig i hele Unionen og er af særlig interesse for energisektoren.

(8) Kommissionen har fremsat en henstilling ([9]) vedrørende cybersikkerhedsrisici ved netværksteknologier af femte generation (5G) og håndtering af disse gennem fastsættelse af retningslinjer for passende foranstaltninger til risikoanalyse og -styring på nationalt plan, for udvikling af koordineret europæisk risikoanalyse og for fastlæggelsen af en proces til at udvikle en fælles værktøjskasse med de bedste foranstaltninger til risikostyring. Når først 5G-net er blevet udbredt, vil de danne basis for en bred vifte af tjenester, der vil være afgørende for det indre markeds funktion samt for vigtige samfundsmæssige og økonomiske funktioner såsom energi.

(9) Denne henstilling bør indeholde en ikkeudtømmende vejledning til medlemsstaterne og relevante interessenter, navnlig netoperatører og teknologileverandører, i opnåelsen af et højere cybersikkerhedsniveau i lyset af de specifikke realtidskrav, der er identificeret for energisektoren, kaskadevirkninger og kombinationen af gammel og avanceret teknologi. Denne vejledning har til formål at hjælpe interessenterne med at tage hensyn til de specifikke krav i energisektoren i forbindelse med gennemførelsen af internationalt anerkendte standarder for cybersikkerhed ([10]).

(10) Kommissionen har til hensigt at revidere denne henstilling regelmæssigt på grundlag af fremskridtene i hele Unionen efter høring af medlemsstaterne og relevante interessenter. Kommissionen vil fortsætte sine bestræbelser på at styrke cybersikkerheden i energisektoren, navnlig gennem NIS-samarbejdsgruppen, som sikrer det strategiske samarbejde og udvekslingen af oplysninger mellem medlemsstaterne om cybersikkerhed —

VEDTAGET DENNE HENSTILLING:

GENSTAND

(1) I denne henstilling opstilles de vigtigste problemstillinger vedrørende cybersikkerhed i energisektoren, nemlig realtidskrav, kaskadevirkninger og kombinationen af gamle og avancerede teknologier, og den identificerer de vigtigste foranstaltninger til gennemførelse af de relevante beredskabsforanstaltninger inden for cybersikkerhed i energisektoren.

([7]) JOIN(2017) 450.

([8]) Forordningen om cybersikkerhed blev vedtaget af Europa-Parlamentet i marts 2019. Rådets formelle vedtagelse forventes at finde sted i april, og offentliggørelsen af retsakten i EUT følger kort tid derefter.

([9]) C(2019) 2335.

([10]) Internationale standardiseringsorganisationer har offentliggjort en række standarder for cybersikkerhed (ISO/IEC 27000: Informationsteknologi) og for risikoledelse (ISO/IEC31000: Risikoledelse). En specifik standard for energisektoren (ISO/IEC 27019: Informationssikkerhedskontrol for energiforsyningsindustrien) blev udstedt som led i ISO/IEC 27000-serien i oktober 2017.

(2) Ved anvendelsen af denne henstilling bør medlemsstaterne tilskynde de relevante interessenter til at opbygge viden og færdigheder inden for cybersikkerhed i energisektoren. Medlemsstaterne bør, hvor det er relevant, også lade disse overvejelser indgå i deres nationale rammer for cybersikkerhed, navnlig gennem strategier, love og administrative bestemmelser.

REALTIDSKRAV TIL ENERGIINFRASTRUKTURKOMPONENTER

(3) Medlemsstaterne bør sikre, at de relevante interessenter, navnlig energinetoperatører og teknologileverandører, og især operatører af væsentlige tjenester, der er udpeget i henhold til NIS-direktivet, gennemfører de relevante beredskabsforanstaltninger inden for cybersikkerhed vedrørende realtidskrav i energisektoren. Nogle elementer i energisystemet skal fungere i »realtid«, dvs. reagere på kommandoer inden for nogle få millisekunder, hvilket gør det vanskeligt eller endog umuligt at indføre cybersikkerhedsforanstaltninger på grund af manglende tid.

(4) Energinetoperatører bør navnlig:

a) anvende de seneste sikkerhedsstandarder for nye anlæg, når det er hensigtsmæssigt, og overveje supplerende fysiske sikringsforanstaltninger, når gamle anlægs installerede base ikke i tilstrækkelig grad kan beskyttes af cybersikkerhedsmekanismer

b) gennemføre internationale standarder for cybersikkerhed og passende specifikke tekniske standarder for sikker kommunikation i realtid, så snart de pågældende produkter kommer på markedet

c) tage højde for realtidsbegrænsninger i det overordnede sikkerhedskoncept for aktiver, navnlig i forbindelse med klassifikation af aktiver

d) overveje privatejede net for telebeskyttelsesordninger for at sikre kvaliteten af det serviceniveau, der kræves for realtidsbegrænsninger, og når operatører bruger offentlige kommunikationsnet, bør de overveje at sikre tildeling af specifik båndbredde og specifikke latenskrav og foranstaltninger inden for kommunikationssikkerhed

e) opdele det overordnede system i logiske zoner og inden for hver zone definere tids- og procesbegrænsninger, således at det er muligt at anvende passende cybersikkerhedsforanstaltninger eller overveje alternative beskyttelsesmetoder.

(5) Hvor det er muligt, bør energinetoperatører ligeledes:

a) vælge en sikker kommunikationsprotokol under hensyntagen til realtidskrav, f.eks. mellem et anlæg og dets ledelsessystemer (energistyringssystem — EMS og distributionsstyringssystem — DMS)

b) indføre en passende autentifikationsmekanisme for kommunikation mellem maskiner og tage højde for realtidskrav.

KASKADEVIRKNINGER

(6) Medlemsstaterne bør sikre, at de relevante interessenter, navnlig energinetoperatører og teknologileverandører, og især operatører af væsentlige tjenester, der er udpeget i henhold til NIS-direktivet, gennemfører de relevante beredskabsforanstaltninger inden for cybersikkerhed vedrørende kaskadevirkninger i energisektoren. Der er en stærk sammenkobling af elnet og gasledninger i hele Europa, og et cyberangreb, der fører til udfald eller afbrydelser i en del af energisystemet, kan udløse vidtrækkende kaskadevirkninger i andre dele af dette system.

(7) Ved anvendelsen af denne henstilling bør medlemsstaterne evaluere den indbyrdes afhængighed og kritikaliteten af elproduktionen og fleksible efterspørgselssystemer, transmissions- og fordelingsstationer og -ledninger og de berørte interessenter (herunder i grænseoverskridende situationer) i tilfælde af vellykkede cyberangreb eller cyberhændelser. Medlemsstaterne bør ligeledes sikre, at energinetoperatørerne har en ramme for kommunikation med alle centrale interessenter med henblik på udveksling af tidlige varslinger og samarbejde om krisestyring. Der bør være strukturerede kommunikationskanaler og aftalte formater for deling af følsomme oplysninger med alle relevante interessenter, enheder, der håndterer IT-sikkerhedshændelser, og relevante myndigheder.

(8) Energinetoperatører bør navnlig:

a) sikre, at nyt udstyr, herunder udstyr til tingenes internet, har og opretholder et cybersikkerhedsniveau, der afspejler et sites kritikalitet

b) i tilstrækkelig grad tage hensyn til de cyberfysiske virkninger i forbindelse med etableringen og den regelmæssige gennemgang af driftskontinuitetsplaner

c) fastlægge designkriterier og en arkitektur for et robust net, hvilket kan opnås ved at:

— indføre omfattende beskyttelsesforanstaltninger for de enkelte sites, der er skræddersyet til et sites kritikalitet

— identificere kritiske knudepunkter, både med hensyn til elproduktionskapacitet og kundevirkning. Der bør udformes kritiske netfunktioner for at mindske risici, der kan forårsage kaskadevirkninger, under hensyntagen til redundans, modstandsdygtighed over for fasesvingning og beskyttelse mod afskæring af kaskadebelastning

— samarbejde med andre relevante operatører og med teknologileverandører for at forhindre kaskadevirkninger ved brug af passende foranstaltninger og tjenester

— udforme og opbygge kommunikations- og kontrolnetværk for at inddæmme virkningerne af fysiske og logiske svigt til begrænsede dele af nettene og for at sikre passende og hurtige afbødende foranstaltninger.

GAMMEL OG AVANCERET TEKNOLOGI

(9) Medlemsstaterne bør sikre, at de relevante interessenter, navnlig energinetoperatører og teknologileverandører, og især operatører af væsentlige tjenester, der er udpeget i henhold til NIS-direktivet, gennemfører de relevante beredskabsforanstaltninger inden for cybersikkerhed vedrørende kombinationen af gammel og avanceret teknologi i energisektoren. Det nuværende energisystem er i realiteten baseret på to forskellige typer teknologier, der eksisterer side om side: en ældre teknologi med 30-60 år på bagen, der er udviklet, inden man begyndte at tage hensyn til cybersikkerhed, og moderne udstyr baseret på avanceret digitalisering og intelligente enheder.

(10) Ved anvendelsen af denne henstilling bør medlemsstaterne tilskynde energinetoperatører og teknologileverandører til at følge de relevante internationalt anerkendte standarder for cybersikkerhed, hvor det er muligt. I mellemtiden bør interessenter og kunder indtage en cybersikkerhedsorienteret tilgang i forbindelse med tilslutning til nettet.

(11) Teknologileverandører bør navnlig stille afprøvede løsninger på sikkerhedsproblemer i gamle eller nye teknologier gratis til rådighed, så snart der viser sig et relevant sikkerhedsproblem.

(12) Energinetoperatører bør navnlig:

a) analysere risiciene ved at forbinde begreber vedrørende gamle systemer og tingenes internet og være opmærksom på interne og eksterne grænseflader og sårbarheder

b) træffe passende foranstaltninger mod ondsindede angreb som følge af omfattende ondsindede angreb mod forbrugerudstyr eller -applikationer

c) etablere en automatiseret overvågnings- og analysekapacitet for sikkerhedsrelaterede hændelser i gamle systemer og systemer for tingenes internet såsom mislykkede loginforsøg, døralarmer ved åbning af kabinet eller andre hændelser

d) regelmæssigt gennemføre en specifik analyse af cybersikkerhedsrisici forbundet med alle gamle anlæg, navnlig i forbindelse med sammenkobling af gamle og nye teknologier — da de gamle anlæg ofte repræsenterer et meget stort antal aktiver, kan risikoanalysen eventuelt foretages efter aktivklasse

e) opdatere software og hardware i de gamle systemer og systemer for tingenes internet til den seneste version, når det er hensigtsmæssigt — energinetoperatører bør i denne forbindelse overveje supplerende foranstaltninger såsom adskillelse af systemer eller tilføjelse af eksterne sikkerhedsbarrierer, hvor patchning eller opdatering ville være tilstrækkeligt, men ikke er muligt, f.eks. i forbindelse med produkter, der ikke understøttes

f) udarbejde bud under hensyntagen til cybersikkerhed, dvs. anmode om oplysninger om sikkerhedsforanstaltninger, stille krav om overholdelse af eksisterende standarder for cybersikkerhed, sikre, at der fortsat stilles forslag om varsling, patchning og afhjælpning i tilfælde af afdækning af sårbarheder, og afklare leverandøransvar i tilfælde af cyberangreb eller -hændelser

g) samarbejde med teknologileverandører om at erstatte gamle systemer, når det er hensigtsmæssigt af sikkerhedsmæssige årsager, men under hensyntagen til kritiske systemfunktioner.

OVERVÅGNING

(13) Medlemsstaterne bør senest 12 måneder efter vedtagelsen af denne henstilling og derefter hvert andet år meddele Kommissionen detaljerede oplysninger om status for gennemførelsen af denne henstilling gennem NIS-samarbejdsgruppen.

REVISION

(14) På grundlag af oplysninger fra medlemsstaterne vil Kommissionen gennemgå gennemførelsen af denne henstilling og vurdere, om der er behov for yderligere foranstaltninger, efter høring af medlemsstaterne og de relevante interessenter.

ADRESSATER

(15) Denne henstilling er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 3. april 2019.

På Kommissionens vegne
Miguel ARIAS CAÑETE
Medlem af Kommissionen