REKOMMENDATIONER

KOMMISSIONENS REKOMMENDATION (EU) 2019/553

av den 3 april 2019

om cybersäkerhet inom energisektorn

[delgivet med nr C(2019) 2400]

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 292, och

av följande skäl:

(1) Den europeiska energisektorn genomgår en stor förändring mot en koldioxidsnål ekonomi, där samtidigt försörjningstryggheten och konkurrenskraften ska säkerställas. Som en del av denna energiomställning och den medföljande decentraliseringen av elproduktion från förnybara energikällor, är tekniska framsteg, sektorsintegration och digitalisering på väg att omvandla Europas elnät till ett smart nät. Samtidigt medför detta också nya risker eftersom digitaliseringen i allt högre grad gör energisystemet utsatt för cyberattacker och incidenter som kan äventyra en trygg energiförsörjning.

(2) Antagandet av de åtta lagstiftningsförslagen i paketet om ren energi för alla i EU ([1]), där styrningen av energiunionen är ett viktigt steg, gör det möjligt att skapa en gynnsam miljö för den digitala omvandlingen av energisektorn. Vikten av cybersäkerhet inom energisektorn framhävs också. I den omarbetade förordningen om den inre marknaden för el ([2]) föreskrivs i synnerhet att tekniska regler för el ska antas, såsom en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter vad gäller gränsöverskridande elflöden, gemensamma minimikrav, planering, övervakning, rapportering och krishantering. I förordningen om riskberedskap för el ([3]) liknar förhållningssättet i stora drag det som valts i förordningen om tryggad gasförsörjning ([4]). Man betonar behovet av att korrekt bedöma alla risker, inbegripet de som berör cybersäkerhet, och föreslår att åtgärder vidtas för att förebygga och minska dessa identifierade risker.

(3) När kommissionen antog EU:s strategi för cybersäkerhet ([5]) 2013 identifierades en förstärkning av unionens cyberberedskap som en prioritet. Ett av strategins viktigaste resultat är direktivet om säkerhet i nätverks- och informationssystem ([6]) (nedan kallat *NIS-direktivet*) som antogs i juli 2016. NIS-direktivet, som är det första steget mot en övergripande EU-lagstiftning om cybersäkerhet, innebär att den generella nivån av cybersäkerhet inom unionen stärks genom utvecklingen av den nationella kapaciteten avseende cybersäkerhet, ett ökat samarbete på EU-nivå och införandet av säkerhets- och incidentrapporteringsskyldigheter för företag, vilka går under benämningen ”leverantörer av samhällsviktiga tjänster”. Incidentrapportering är obligatorisk inom viktiga sektorer, däribland energisektorn.

([1]) Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor (EUT L 328, 21.12.2018, s. 82), Europaparlamentets och rådets direktiv (EU) 2018/2002 av den 11 december 2018 om ändring av direktiv 2012/27/EU om energieffektivitet (EUT L 328, 21.12.2018, s. 210), Europaparlamentets och rådets förordning (EU) 2018/1999 av den 11 december 2018 om styrningen av energiunionen och av klimatåtgärder samt om ändring av Europaparlamentets och rådets förordningar (EG) nr 663/2009 och (EG) nr 715/2009, Europaparlamentets och rådets direktiv 94/22/EG, 98/70/EG, 2009/31/EG, 2009/73/EG, 2010/31/EU, 2012/27/EU och 2013/30/EU samt rådets direktiv 2009/119/EG och (EU) 2015/652 och om upphävande av Europaparlamentets och rådets förordning (EU) nr 525/2013 (EUT L 328, 21.12.2018, s. 1), Europaparlamentets och rådets direktiv (EU) 2018/844 av den 30 maj 2018 om ändring av direktiv 2010/31/EU om byggnaders energiprestanda och av direktiv 2012/27/EU om energieffektivitet (EUT L 156, 19.6.2018, s. 75). Europaparlamentet bekräftade i plenarsessionen i mars 2019 de politiska överenskommelser som nåtts med rådet om förslag till utformning av elmarknaden (förordningen om riskberedskap, förordningen om byrån för samarbete mellan energitillsynsmyndigheter [Acer], eldirektivet och elförordningen). Rådets formella antagande förväntas i april. Rättsakterna kommer därefter att inom kort offentliggöras i EUT.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Europaparlamentets och rådets förordning (EU) 2017/1938 av den 25 oktober 2017 om åtgärder för att säkerställa försörjningstryggheten för gas och om upphävande av förordning (EU) nr 994/2010 (EUT L 280, 28.10.2017, s. 1).

([5]) JOIN(2013) 1.

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

(4) Vid genomförandet av beredskapsåtgärder inom cybersäkerhet bör berörda aktörer, inbegripet leverantörer av samhällsviktiga tjänster inom energisektorn som anges i NIS-direktivet, ta hänsyn till den övergripande vägledningen från samarbetsgruppen för nät- och informationssäkerhet som inrättades enligt artikel 11 i NIS-direktivet. Samarbetsgruppen, som består av företrädare från medlemsstaterna, Europeiska unionens cybersäkerhetsbyrå (Enisa) och kommissionen, har antagit dokument med riktlinjer för säkerhetsåtgärder och incidentrapportering. I juni 2018 skapade gruppen ett särskilt arbetsflöde för energisektorn.

(5) I det gemensamma meddelandet om cybersäkerhet från 2017 ([7]) framhävs vikten av sektorsspecifika överväganden och krav på EU-nivå, inbegripet inom energisektorn. Cybersäkerhet och möjliga politiska följder har varit föremål för omfattande diskussioner och debatter inom unionen under de senaste åren. I dag finns det följaktligen en ökad medvetenhet om att enskilda ekonomiska sektorer står inför specifika problem vad gäller cybersäkerhet och därmed behöver utveckla egna sektorsspecifika metoder i det bredare sammanhanget av allmänna cybersäkerhetsstrategier.

(6) Utbyte av information och förtroende är viktiga komponenter inom cybersäkerhet. Kommissionen har som mål att öka informationsutbytet bland berörda aktörer genom att anordna särskilda evenemang, som till exempel rundabordskonferensen på hög nivå om cybersäkerhet inom energisektorn som anordnades i Rom i mars 2017 och högnivåkonferensen om cybersäkerhet inom energisektorn som anordnades i Bryssel i oktober 2018. Kommissionen vill även förbättra samarbetet mellan berörda aktörer och specialiserade enheter såsom det europeiska centrumet för utbyte och analys av energiinformation (European Energy Information Sharing and Analysis Centre).

(7) Genom förordningen om en europeisk byrå för cybersäkerhet, Enisa, och om cybersäkerhetscertifiering för informations- och kommunikationsteknik (nedan kallad *cybersäkerhetsakten* ([8])) kommer att stärka mandatet för EU:s cybersäkerhetsbyrå så att den kan ge bättre stöd till medlemsstaterna att hantera hot och attacker mot cybersäkerheten. Genom akten skapas även en europeisk ram för cybersäkerhet vad gäller certifiering av produkter, processer och tjänster som kommer att vara giltig i hela unionen och som är av särskilt intresse för energisektorn.

(8) Kommissionen har lagt fram en rekommendation ([9]) avseende cybersäkerhetsrisker i den femte generationen (5G) nätverksteknik genom att fastställa riktlinjer om en lämplig riskanalys och förvaltningsåtgärder på nationell nivå, om utveckling av en samordnad europeisk riskanalys och om fastställande av ett förfarande för att utveckla en gemensam verktygslåda med bästa riskhanteringsåtgärder. När 5G-nätverken har tagits i drift kommer de att utgöra stommen i ett stort antal tjänster som är nödvändiga för den inre marknadens funktion och för driften av viktiga funktioner för samhället och ekonomin såsom energin.

(9) Denna rekommendation bör ge medlemsstaterna och berörda aktörer, i synnerhet nätoperatörer och teknikleverantörer, en icke-uttömmande vägledning för att de ska kunna uppnå en högre nivå av cybersäkerhet med tanke på de specifika realtidskrav som finns inom sektorn, kaskadeffekter och kombinationen av äldre och modern teknik. Målet med denna vägledning är att hjälpa berörda aktörer att beakta de specifika kraven inom energisektorn när de ska tillämpa internationellt erkända cybersäkerhetsstandarder ([10]).

(10) Kommissionen avser att regelbundet se över denna rekommendation på grundval av de framsteg som gjorts inom unionen, i samråd med medlemsstaterna och berörda aktörer. Kommissionen kommer att fortsätta med sina insatser för att stärka cybersäkerheten inom energisektorn, framför allt med hjälp av samarbetsgruppen för nät- och informationssäkerhet, som säkerställer ett strategiskt samarbete och informationsutbyte mellan medlemsstaterna i fråga om cybersäkerhet.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

SYFTE

1. I denna rekommendation fastställs de viktigaste frågorna i samband med cybersäkerhet inom energisektorn, nämligen realtidskrav, kaskadeffekter och kombinationen av äldre och modern teknik, och identifieras de viktigaste åtgärderna för genomförandet av relevanta beredskapsåtgärder vad gäller cybersäkerhet inom energisektorn.

([7]) JOIN(2017) 450.

([8]) Cybersäkerhetsakten antogs av Europaparlamentet i mars 2019. Rådets formella antagande förväntas i april. Rättsakterna kommer därefter att inom kort offentliggöras i EUT.

([9]) C(2019)2335

([10]) Internationella standardiseringsorganisationer har publicerat olika standarder för cybersäkerhet (ISO/IEC 27000: Information Technologies) och riskhantering (ISO/IEC 31000: Implementation of risk management). En specifik standard för energisektorn (ISO/IEC 27019: Information security controls for the energy utility industry) utfärdades som en del av ISO/IEC 27000-serien i oktober 2017.

2. Vid tillämpning av denna rekommendation bör medlemsstaterna uppmuntra de berörda aktörerna att bygga upp kunskaper och utveckla färdigheter förknippade med cybersäkerhet inom energisektorn. Medlemsstaterna bör även när det är lämpligt inkludera dessa överväganden i sina nationella ramar för cybersäkerhet, i synnerhet genom strategier, lagar, regler och andra administrativa bestämmelser.

REALTIDSKRAV FÖR ENERGIINFRASTRUKTURKOMPONENTER

3. Medlemsstaterna bör se till att de berörda aktörerna, särskilt energinätsoperatörer och teknikleverantörer och i synnerhet leverantörer av samhällsviktiga tjänster som identifieras i NIS-direktivet, genomför relevanta beredskapsåtgärder för cybersäkerhet i samband med realtidskrav inom energisektorn. Vissa delar av energisystemet måste kunna fungera i realtid, dvs. reagera på kommandon inom några millisekunder, och de korta tidsspannen gör det svårt eller till och med omöjligt att införa cybersäkerhetsåtgärder.

4. Energinätsoperatörerna bör framför allt

   a) tillämpa de senaste säkerhetsstandarderna för nya installationer där detta är lämpligt och överväga kompletterande fysiska säkerhetsåtgärder där de äldre installationerna inte kan skyddas tillräckligt av cybersäkerhetsmekanismer,

   b) tillämpa internationella standarder för cybersäkerhet och särskilda lämpliga tekniska standarder för säker kommunikation i realtid så snart en produkt blir kommersiellt tillgänglig,

   c) ta hänsyn till realtidsbegränsningar i det övergripande säkerhetskonceptet för tillgångar, särskilt i fråga om klassificeringen av tillgångar,

   d) överväga privatägda nätverk för fjärrskyddssystem för att säkerställa den kvalitetsnivå för tjänsten i fråga som krävs med tanke på realtidsbegränsningar; när offentliga kommunikationsnätverk används bör operatörerna överväga att säkerställa specifik bandbreddsallokering, latenskrav och säkerhetsåtgärder för kommunikation,

   e) dela upp det övergripande systemet i logiska zoner och inom varje zon fastställa tids- och processbegränsningar för att göra det möjligt att tillämpa lämpliga cybersäkerhetsåtgärder eller överväga alternativa skyddsmetoder.

5. I mån av tillgänglighet bör energinätsoperatörerna även

   a) välja ett säkert kommunikationsprotokoll med hänsyn tagen till realtidskrav, t.ex. mellan en installation och dess ledningssystem (energiledningssystem [EMS]/distributionsledningssystem [DMS]),

   b) införa en lämplig autentiseringsmekanism för maskin-maskin-kommunikation som hanterar realtidskrav.

KASKADEFFEKTER

6. Medlemsstaterna bör se till att de berörda aktörerna, särskilt energinätsoperatörer och teknikleverantörer och i synnerhet leverantörer av samhällsviktiga tjänster som identifieras i NIS-direktivet, genomför relevanta beredskapsåtgärder vad gäller cybersäkerhet i samband med kaskadeffekter inom energisektorn. Elnät och gasledningar är starkt sammankopplade i hela Europa och en cyberattack som orsakar ett driftavbrott eller en störning i en del av energisystemet kan utlösa långtgående kaskadeffekter i andra delar av systemet.

7. Vid tillämpning av denna rekommendation bör medlemsstaterna utvärdera ömsesidiga beroenden och kriticitet för elproduktionssystem och system för efterfrågeflexibilitet, samt stationer och ledningar i överförings- och distributionsnät, och de berörda aktörer som skulle påverkas (inbegripet vid gränsöverskridande situationer) i händelse av en framgångsrik cyberattack eller en it-incident. Medlemsstaterna bör även se till att energinätsoperatörerna har en kommunikationsram inom vilken alla centrala aktörer i ett tidigt skede kan dela med sig av varningssignaler och samarbeta vid krishantering. Det bör finnas strukturerade kommunikationskanaler och överenskomna format för att kunna dela känslig information med alla berörda aktörer, enheter för hantering av it-säkerhetsincidenter och relevanta myndigheter.

8. Energinätsoperatörerna bör framför allt

   a) se till att nya enheter, inbegripet enheter anslutna till sakernas internet, har och kommer att upprätthålla en nivå av cybersäkerhet som är lämplig med tanke på en anläggnings kriticitet,

   b) på ett lämpligt sätt beakta cyberfysiska effekter när de upprättar och regelbundet granskar affärskontinuitetsplaner,

c) upprätta konstruktionskriterier och en arkitektur för ett robust nät, vilket kan uppnås genom att

— införa djupgående försvarsåtgärder för varje anläggning som är skräddarsydda efter anläggningens kriticitet,

— identifiera kritiska noder både när det gäller kraftproduktionskapacitet och kundpåverkan; ett näts kritiska funktioner bör utformas så att de minskar riskerna för kaskadeffekter genom att beakta redundans, motståndskraft mot fassvängningar och skydd mot kaskadfel i form av bortkopplad last,

— samarbeta med andra relevanta operatörer och med teknikleverantörer för att förebygga kaskadeffekter genom att tillämpa lämpliga åtgärder och tjänster,

— utforma och bygga upp kommunikations- och kontrollnätverk i syfte att begränsa effekterna av eventuella fysiska och logiska fel till avgränsade delar av näten och att säkerställa lämpliga och snabba riskreducerande åtgärder.

ÄLDRE OCH MODERN TEKNIK

9. Medlemsstaterna bör se till att de berörda aktörerna, särskilt energinätsoperatörer och teknikleverantörer och i synnerhet leverantörer av samhällsviktiga tjänster som identifieras i NIS-direktivet, genomför relevanta beredskapsåtgärder vad gäller cybersäkerhet när äldre och modern teknik inom energisektorn kombineras. Det finns två olika typer av teknik som samverkar i dagens energisystem: en äldre teknik med en livslängd på 30 till 60 år som utformades innan några överväganden om cybersäkerhet gjordes, och modern utrustning som återspeglar den senaste digitaliseringen och smarta enheter.

10. Vid tillämpning av denna rekommendation bör medlemsstaterna uppmuntra energinätsoperatörer och teknikleverantörer att, när helst så är möjligt, följa relevanta internationellt accepterade standarder för cybersäkerhet. Under tiden bör berörda aktörer och kunder anta ett cybersäkerhetsinriktat förhållningssätt när de ansluter enheter till nätet.

11. Teknikleverantörer bör i synnerhet erbjuda beprövade lösningar på säkerhetsproblem vad gäller äldre eller ny teknik, utan kostnad och så snart ett relevant säkerhetsproblem upptäcks.

12. Energinätsoperatörerna bör framför allt

a) analysera riskerna med att koppla ihop koncept som bygger på äldre teknik och sakernas internet och känna till hur sårbara interna och externa gränssnitt är,

b) vidta lämpliga åtgärder mot skadliga angrepp från ett stort antal enheter eller applikationer på konsumentsidan som kontrolleras av obehöriga,

c) upprätta en automatiserad övervaknings- och analysfunktion för säkerhetsrelaterade händelser inom miljöer där äldre teknik och sakernas internet används, t.ex. misslyckade inloggningsförsök, dörrlarm för öppning av skåp och andra händelser,

d) regelbundet utföra specifikt inriktade analyser av risker för cybersäkerheten, särskilt vid sammankoppling av äldre och ny teknik; eftersom de äldre installationerna ofta representerar ett mycket stort antal tillgångar kan riskanalyserna ske utifrån tillgångsklasser,

e) uppdatera programvaror och hårdvaror för system som använder äldre teknik och sakernas internet till den senaste versionen när så är lämpligt; när detta görs bör energinätsoperatörerna överväga kompletterande åtgärder såsom att separera system eller lägga till externa säkerhetsbarriärer där programfixar eller uppdateringar som skulle vara lämpliga inte fungerar, till exempel för produkter som inte längre stöds,

f) formulera anbud med cybersäkerhet i åtanke, dvs. efterfråga information om säkerhetsfunktioner, kräva att befintliga cybersäkerhetsstandarder följs, se till att det kontinuerligt finns mekanismer för varningar, programfixar och riskreducerande åtgärder om sårbarheter upptäcks och klargöra leverantörens ansvarsskyldighet i händelse av cyberattacker eller it-incidenter,

g) samarbeta med teknikleverantörer för att ersätta äldre system när så är lämpligt av säkerhetsskäl, men ta hänsyn till kritiska systemfunktioner.

ÖVERVAKNING

13. Medlemsstaterna bör inom tolv månader efter antagandet av denna rekommendation, och därefter vartannat år, förse kommissionen med detaljerad information om situationen för genomförandet av denna rekommendation via samarbetsgruppen för nät- och informationssäkerhet.

ÖVERSYN

14. På grundval av de uppgifter som medlemsstaterna lämnat kommer kommissionen att i samråd med medlemsstaterna och de berörda aktörerna se över genomförandet av denna rekommendation och bedöma huruvida ytterligare åtgärder krävs.

MOTTAGARE

15. Denna rekommendation riktar sig till medlemsstaterna.

Utfärdad i Bryssel den 3 april 2019.

På kommissionens vägnar
Miguel ARIAS CAÑETE
Ledamot av kommissionen