EMPFEHLUNGEN

EMPFEHLUNG (EU) 2019/553 DER KOMMISSION

vom 3. April 2019

zur Cybersicherheit im Energiesektor

(Bekannt gegeben unter Aktenzeichen C(2019) 2400)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 292,

in Erwägung nachstehender Gründe:

(1) Angesichts des Aufbaus einer CO_2-emissionsarmen Wirtschaft befindet sich der europäische Energiesektor in einem entscheidenden Umbruch und muss gleichzeitig die Versorgungssicherheit und Wettbewerbsfähigkeit sicherstellen. Im Rahmen dieser Energiewende und der damit verbundenen Dezentralisierung der Stromerzeugung aus erneuerbaren Energiequellen, des technischen Fortschritts, der Sektorkopplung und der Digitalisierung wandelt sich das Stromnetz Europas zu einem „intelligenten Netz". Dies geht jedoch auch mit neuen Risiken einher, da das Energiesystem aufgrund der Digitalisierung zunehmend der Gefahr von Cyberangriffen und anderen Vorfällen, die die Energieversorgungssicherheit beeinträchtigen können, ausgesetzt ist.

(2) Angesichts der Verabschiedung aller acht Legislativvorschläge ([1]) des Pakets „Saubere Energie für alle Europäer", bei denen auch das Governance-System für die Energieunion einen entscheidenden Bestandteil bildet, ist es nun möglich, ein günstiges Umfeld für den digitalen Wandel im Energiesektor zu schaffen. Zudem wird in dem Paket die Bedeutung der Cybersicherheit im Energiesektor hervorgehoben. So sieht insbesondere die Neufassung der Verordnung über den Elektrizitätsbinnenmarkt ([2]) die Verabschiedung technischer Bestimmungen für die Stromversorgung vor, darunter auch einen Netzkodex mit sektorspezifischen Regeln für Cybersicherheitsaspekte bei grenzübergreifenden Stromflüssen; dieser soll auch gemeinsame Mindestanforderungen sowie eine gemeinsame Planung, Überwachung, Berichterstattung und ein gemeinsames Krisenmanagement umfassen. In der Verordnung über die Risikovorsorge im Elektrizitätssektor ([3]) wird der in der Verordnung über die Sicherheit der Gasversorgung ([4]) gewählte Ansatz im Wesentlichen weiterverfolgt, wobei die Notwendigkeit betont wird, alle Risiken, auch im Zusammenhang mit der Cybersicherheit, angemessen zu berücksichtigen; zudem wird vorgeschlagen, Maßnahmen zur Verhütung und Minderung der ermittelten Risiken zu verabschieden.

(3) In der 2013 angenommenen EU-Cybersicherheitsstrategie ([5]) der Kommission wird die Stärkung der Widerstandsfähigkeit der Union gegenüber Cyberangriffen als Priorität genannt. Einer der wichtigsten Bestandteile der Strategie ist die im Juli 2016 angenommene Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union ([6]) (im Folgenden „NIS-Richtlinie"). Als erster sektorübergreifender EU-Rechtsakt für die Cybersicherheit erhöht die NIS-Richtlinie das Niveau der Cybersicherheit in der Union insgesamt; dazu ist vorgesehen, nationale Cybersicherheitskapazitäten aufzubauen, die EU-weite Zusammenarbeit zu stärken und bestimmte Unternehmen, die sogenannten „Betreiber wesentlicher Dienste", zu verpflichten, für Sicherheit zu sorgen und sicherheitsrelevante Vorfälle zu melden. Die Meldung von Vorfällen ist in Schlüsselsektoren wie dem Energiesektor obligatorisch.

([1]) Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen (ABl. L 328 vom 21.12.2018, S. 82); Richtlinie (EU) 2018/2002 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Änderung der Richtlinie 2012/27/EU zur Energieeffizienz (ABl. L 328 vom 21.12.2018, S. 210); Verordnung (EU) 2018/1999 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über das Governance-System für die Energieunion und für den Klimaschutz, zur Änderung der Verordnungen (EG) Nr. 663/2009 und (EG) Nr. 715/2009 des Europäischen Parlaments und des Rates, der Richtlinien 94/22/EG, 98/70/EG, 2009/31/EG, 2009/73,/EG, 2010/31/EU, 2012/27/EU und 2013/30/EU des Europäischen Parlaments und des Rates, der Richtlinien 2009/119/EG und (EU) 2015/652 des Rates und zur Aufhebung der Verordnung (EU) Nr. 525/2013 des Europäischen Parlaments und des Rates (ABl. L 328 vom 21.12.2018, S. 1); Richtlinie (EU) 2018/844 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie 2010/31/EU über die Gesamtenergieeffizienz von Gebäuden und der Richtlinie 2012/27/EU über Energieeffizienz (ABl. L 156 vom 19.6.2018, S. 75). Das Europäische Parlament hat die mit dem Rat erzielte politische Einigung über die Vorschläge für die Gestaltung des Strommarktes (Verordnung über die Risikovorsorge, Verordnung über die Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER) sowie die Elektrizitätsrichtlinie und die Elektrizitätsverordnung) auf seiner Plenarsitzung im März 2019 bestätigt. Die förmliche Verabschiedung durch den Rat wird im April erwartet; kurz darauf soll der Rechtstext im Amtsblatt veröffentlicht werden.

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

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

([4]) Verordnung (EU) 2017/1938 des Europäischen Parlaments und Rates vom 25. Oktober 2017 über Maßnahmen zur Gewährleistung der sicheren Erdgasversorgung und zur Aufhebung der Verordnung (EU) Nr. 994/2010 (ABl. L 280 vom 28.10.2017, S. 1).

([5]) JOIN(2013) 1.

([6]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

(4) Bei der Umsetzung von Vorsorgemaßnahmen im Bereich der Cybersicherheit sollten die einschlägigen Akteure, darunter auch die im Rahmen der NIS-Richtlinie ermittelten Betreiber wesentlicher Dienste im Energiesektor, die sektorübergreifenden Leitlinien berücksichtigen, die von der gemäß Artikel 11 der NIS-Richtlinie eingesetzten Kooperationsgruppe für Netz- und Informationssicherheit entwickelt wurden. Die Kooperationsgruppe, der Vertreterinnen und Vertreter der Mitgliedstaaten, der Agentur der Europäischen Union für Cybersicherheit (ENISA) sowie der Kommission angehören, hat Leitlinien zu Sicherheitsmaßnahmen und zur Meldung von Vorfällen erarbeitet. Im Juni 2018 richtete die Gruppe zudem einen eigenen Arbeitsbereich für den Energiesektor ein.

(5) In der 2017 vorgelegten gemeinsamen Mitteilung zur Cybersicherheit ([7]) wird die Bedeutung EU-weiter sektorspezifischer Erwägungen und Anforderungen, auch für den Energiesektor, hervorgehoben. Die Cybersicherheit und mögliche politische Maßnahmen wurden in den letzten Jahre in der Union umfassend diskutiert. Es besteht daher heute ein zunehmendes Bewusstsein dafür, dass einzelne Wirtschaftssektoren spezifischen Cybersicherheitsproblemen gegenüberstehen und daher im breiteren Kontext allgemeiner Cybersicherheitsstrategien ihre eigenen sektorspezifischen Ansätze entwickeln müssen.

(6) Informationsaustausch und Vertrauen sind zentrale Elemente der Cybersicherheit. Die Kommission beabsichtigt daher, den Informationsaustausch zwischen den einschlägigen Akteuren zu verstärken und dazu gezielte Veranstaltungen zu organisieren, wie sie dies etwa mit dem Diskussionsforum mit hochrangigen Teilnehmern zur Cybersicherheit im Energiebereich vom März 2017 in Rom sowie mit der Konferenz mit hochrangigen Teilnehmern zur Cybersicherheit im Energiebereich vom Oktober 2018 in Brüssel bereits getan hat. Zudem möchte die Kommission die Zusammenarbeit zwischen einschlägigen Akteuren und spezialisierten Einrichtungen wie den Europäischen Zentren für den Informationsaustausch und Analysen im Energiesektor stärken.

(7) In der Verordnung über die ENISA, die „EU-Cybersicherheitsagentur", sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnologien (im Folgenden „Verordnung zum Rechtsakt zur Cybersicherheit" ([8])) wird der Auftrag der EU-Cybersicherheitsagentur gestärkt, damit die Mitgliedstaaten bei der Bewältigung von Cybersicherheitsbedrohungen und -angriffen besser unterstützt werden. Gleichzeitig wird ein europäischer Cybersicherheitsrahmen für die Zertifizierung von Produkten, Verfahren und Dienstleistungen geschaffen, der in der gesamten Union gelten soll und insbesondere für den Energiesektor relevant ist.

(8) Die Kommission hat eine Empfehlung ([9]) zu Cybersicherheitsrisiken im Zusammenhang mit Netztechnologien der 5. Generation (5G) vorgelegt, die Orientierungshilfen für eine angemessene Risikoanalyse und ein angemessenes Risikomanagement auf nationaler Ebene, die Einführung einer koordinierten europäischen Risikoanalyse und die Festlegung eines Verfahrens zur Entwicklung eines gemeinsamen Instrumentariums empfehlenswerter Risikomanagementmaßnahmen bietet. Nach ihrer Einführung werden 5G-Netze das Rückgrat einer Vielzahl von Diensten bilden, die für einen funktionierenden Binnenmarkt und wesentliche gesellschaftliche und wirtschaftliche Leistungen wie die Energieversorgung von entscheidender Bedeutung sind.

(9) Die vorliegende Empfehlung wurde als nicht erschöpfende Leitlinie für die Mitgliedstaaten und einschlägigen Akteure, insbesondere die Netzbetreiber und Technologieanbieter, entwickelt, um angesichts der besonderen Echtzeit-Herausforderungen im Energiesektor, möglicher Kaskadeneffekte und der Kombination älterer und modernster Technologien die Cybersicherheit zu stärken. Diese Leitlinie soll die beteiligten Akteure dabei unterstützen, den besonderen Anforderungen im Energiesektor bei der Umsetzung international anerkannter Cybersicherheitsnormen ([10]) Rechnung zu tragen.

(10) Die Kommission beabsichtigt, diese Empfehlung auf der Grundlage der in der gesamten Union erzielten Fortschritte in Konsultation mit den Mitgliedstaaten und einschlägigen Akteuren regelmäßig zu überprüfen. Die Kommission wird sich auch weiterhin dafür einsetzen, die Cybersicherheit im Energiesektor zu verbessern, insbesondere über die Kooperationsgruppe für Netz- und Informationssicherheit, die die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten im Bereich der Cybersicherheit gewährleistet —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

GEGENSTAND

(1) In dieser Empfehlung werden zentrale Herausforderungen für die Cybersicherheit im Energiesektor — Echtzeitanforderungen, Kaskadeneffekte und die Kombination älterer und modernster Technologien — dargestellt und wesentliche Schritte zur Umsetzung relevanter Vorsorgemaßnahmen im Bereich der Cybersicherheit im Energiesektor bestimmt.

([7]) JOIN(2017) 450.

([8]) Der Rechtsakt zur Cybersicherheit wurde im März 2019 vom Europäischen Parlament angenommen. Die förmliche Verabschiedung durch den Rat wird im April erwartet; kurz darauf soll der Rechtstext im Amtsblatt veröffentlicht werden.

([9]) C(2019) 2335.

([10]) Die Internationalen Normungsorganisationen haben mehrere Normen zur Cybersicherheit (ISO/IEC 27000: Informationstechnologien) und zum Risikomanagement (ISO/IEC 31000: Umsetzung des Risikomanagements) veröffentlicht. Im Rahmen der Reihe ISO/IEC 27000 wurde im Oktober 2017 auch eine spezifische Norm für den Energiesektor (ISO/IEC 27019: Informationssicherheitsmaßnahmen für die Energieversorgung) herausgegeben.

(2) Bei der Anwendung dieser Empfehlung sollten die Mitgliedstaaten die einschlägigen Akteure dazu auffordern, Kenntnisse und Kompetenzen im Bereich der Cybersicherheit im Energiesektor aufzubauen. Gegebenenfalls sollten die Mitgliedstaaten diese Aspekte auch in ihre nationalen Cybersicherheitsrahmen aufnehmen, etwa durch Strategien, Gesetze, Verordnungen und andere Verwaltungsvorschriften.

ECHTZEITANFORDERUNGEN VON KOMPONENTEN DER ENERGIEINFRASTRUKTUR

(3) Die Mitgliedstaaten sollten sicherstellen, dass die einschlägigen Akteure, wie Energienetzbetreiber und Technologieanbieter und insbesondere die im Rahmen der NIS-Richtlinie ermittelten Betreiber wesentlicher Dienste, die für die Echtzeitanforderungen im Energiesektor relevanten Vorsorgemaßnahmen im Bereich der Cybersicherheit umsetzen. So müssen einige Bestandteile des Energiesystems in „Echtzeit" arbeiten, d. h., sie müssen auf Befehle innerhalb weniger Millisekunden reagieren, was die Umsetzung von Cybersicherheitsmaßnahmen aufgrund der Zeitbeschränkungen erschwert oder sogar unmöglich macht.

(4) Insbesondere sollten die Energienetzbetreiber

a) bei neuen Anlagen möglichst die neuesten Sicherheitsnormen anwenden und ergänzende physische Sicherheitsmaßnahmen in Betracht ziehen, wenn die installierte Basis alter Anlagen durch Cybersicherheitsmechanismen nicht ausreichend geschützt werden kann;

b) internationale Cybersicherheitsnormen und angemessene spezifische technische Normen für eine sichere Echtzeitkommunikation umsetzen, sobald die erforderlichen Produkte auf dem Markt erhältlich sind;

c) Echtzeit-Beschränkungen im allgemeinen Sicherheitskonzept für Anlagen, insbesondere bei der Klassifizierung von Anlagen, berücksichtigen;

d) private Netze für Teleprotection-Systeme in Betracht ziehen, um die für Echtzeitanforderungen erforderliche Qualität der Dienste sicherzustellen; bei der Nutzung öffentlicher Kommunikationsnetze sollten die Betreiber eine spezifische Zuteilung von Bandbreiten, Anforderungen an die Latenzzeiten und Kommunikationssicherheitsmaßnahmen in Erwägung ziehen;

e) das Gesamtsystem in logische Bereiche unterteilen und innerhalb jedes Bereichs die Zeit- und Verfahrensanforderungen bestimmen, damit geeignete Cybersicherheitsmaßnahmen angewandt oder alternative Schutzmethoden in Betracht gezogen werden können.

(5) Soweit möglich, sollten die Energienetzbetreiber zudem

a) ein sicheres Kommunikationsprotokoll wählen, wobei sie Echtzeitanforderungen, etwa zwischen einer Anlage und ihren Managementsystemen (Energiemanagementsystem — EMS/Distribution Management System — DMS), berücksichtigen sollten;

b) einen geeigneten Authentifizierungsmechanismus für die Maschine-zu-Maschine-Kommunikation unter Berücksichtigung von Echtzeitanforderungen einführen.

KASKADENEFFEKTE

(6) Die Mitgliedstaaten sollten sicherstellen, dass die relevanten Akteure, wie Energienetzbetreiber und Technologieanbieter und insbesondere die im Rahmen der NIS-Richtlinie ermittelten Betreiber wesentlicher Dienste, die für Kaskadeneffekte im Energiesektor relevanten Vorsorgemaßnahmen im Bereich der Cybersicherheit umsetzen. Die Stromnetze und Gas-Pipelines sind in ganz Europa stark miteinander vernetzt, und ein Cyberangriff, der einen Ausfall oder eine Störung in einem Teil des Energieversorgungssystems verursacht, könnte weitreichende Kaskadeneffekte in anderen Teilen des Systems nach sich ziehen.

(7) Bei der Anwendung dieser Empfehlung sollten die Mitgliedstaaten die gegenseitigen Abhängigkeiten sowie eine mögliche kritische Bedeutung von Stromerzeugungs- und Nachfragesteuerungssystemen, von Umspannwerken und Leitungen in Übertragungs- und Verteilernetzen sowie der möglicherweise betroffenen Akteure (auch in grenzübergreifenden Konstellationen) bei einem erfolgreichen Cyberangriff oder Cybersicherheitsvorfall untersuchen. Zudem sollten die Mitgliedstaaten sicherstellen, dass die Energienetzbetreiber über einen Kommunikationsrahmen mit allen zentralen Akteuren verfügen, um Frühwarnsignale abgeben und im Krisenmanagement zusammenarbeiten zu können. Sie sollten über strukturierte Kommunikationskanäle und vereinbarte Formate verfügen, um sensible Informationen mit allen relevanten Akteuren, Computer-Notfallteams und zuständigen Behörden auszutauschen.

(8) Insbesondere sollten die Energienetzbetreiber

a) sicherstellen, dass neue Geräte, auch im Bereich des „Internets der Dinge", ein der Bedeutung eines Standorts angemessenes Cybersicherheitsniveau aufweisen und beibehalten;

b) bei der Festlegung und regelmäßigen Überprüfung von Betriebskontinuitätsplänen cyber-physische Auswirkungen angemessen berücksichtigen;

c) Auslegungskriterien und eine Architektur für ein widerstandsfähiges Netz festlegen, etwa durch folgende Maßnahmen:

— Einführung zuverlässiger, auf die Bedeutung des jeweiligen Standorts zugeschnittener Verteidigungsmaßnahmen für jeden Standort;

— Ermittlung kritischer Knotenpunkte, sowohl hinsichtlich der Stromerzeugungskapazität als auch in Bezug auf die Auswirkungen auf die Kunden; kritische Funktionen eines Netzes sollten so ausgelegt werden, dass sie das Risiko von Kaskadeneffekten mindern, etwa durch Redundanz, Widerstandsfähigkeit gegenüber Leistungspendelungen und Schutz vor einer durch Kaskadeneffekte verursachten Lasttrennung;

— Zusammenarbeit mit anderen relevanten Betreibern und Technologieanbietern, um durch Anwendung geeigneter Maßnahmen und Dienstleistungen Kaskadeneffekte zu verhindern;

— Auslegung und Aufbau von Kommunikations- und Steuerungsnetzen mit dem Ziel, die Auswirkungen physischer und logischer Fehler auf bestimmte Teile der Netze zu begrenzen und für angemessene und rasche Gegenmaßnahmen zu sorgen.

ÄLTERE UND MODERNSTE TECHNOLOGIEN

(9) Die Mitgliedstaaten sollten sicherstellen, dass die einschlägigen Akteure, wie Energienetzbetreiber und Technologieanbieter und insbesondere die im Rahmen der NIS-Richtlinie ermittelten Betreiber wesentlicher Dienste, die für die Kombination aus älteren und modernsten Technologien im Energiesektor relevanten Vorsorgemaßnahmen im Bereich der Cybersicherheit umsetzen. So bestehen derzeit im Energiesystem zwei Arten von Technologien nebeneinander: eine ältere Technologie mit einer Lebensdauer von 30 bis 60 Jahren, die entwickelt wurde, bevor Cybersicherheitsaspekte relevant waren, und neue Ausrüstung, die durch moderne Digitalisierung und intelligente Geräte gekennzeichnet ist.

(10) Bei der Anwendung dieser Empfehlung sollten die Mitgliedstaaten die Energienetzbetreiber und Technologieanbieter dazu auffordern, die einschlägigen, international anerkannten Normen im Bereich der Cybersicherheit weitestmöglich anzuwenden. In der Zwischenzeit sollten die beteiligten Akteure und Kunden beim Anschluss von Geräten an das Netz einen an der Cybersicherheit ausgerichteten Ansatz wählen.

(11) Insbesondere sollten Technologieanbieter geprüfte Lösungen für Sicherheitsprobleme älterer oder neuer Technologien kostenlos bereitstellen, sobald ein relevantes Sicherheitsproblem bekannt wird.

(12) Die Energienetzbetreiber sollten insbesondere

a) die mit der Verbindung von älteren Konzepten und den Konzepten des Internets der Dinge verbundenen Risiken analysieren und interne und externe Schnittstellen sowie deren Schwachstellen im Auge behalten;

b) geeignete Maßnahmen zum Schutz vor böswilligen Angriffen treffen, die von einer Vielzahl böswillig gesteuerter Kundengeräte oder -anwendungen ausgehen können;

c) automatisierte Überwachungs- und Analysekapazitäten für sicherheitsrelevante Vorkommnisse im Umfeld älterer Technologien sowie im Umfeld des Internets der Dinge — etwa erfolglose Log-in-Versuche, Türalarmauslösungen aufgrund einer Schaltschranköffnung oder andere Vorkommnisse — einrichten;

d) spezifische Cybersicherheitsrisiken für alle älteren Anlagen regelmäßig analysieren, insbesondere wenn alte und neue Technologien miteinander kombiniert werden; da ältere Anlagen oft sehr viele Vermögenswerte umfassen können, kann die Risikoanalyse auch für die einzelnen Kategorien von Vermögenswerten erfolgen;

e) soweit sinnvoll, die Software und Hardware von älteren Systemen und Systemen des Internets der Dinge stets auf dem aktuellen Stand halten; dabei sollten die Energienetzbetreiber auch ergänzende Maßnahmen in Betracht ziehen, wie etwa eine Systemtrennung oder die Hinzufügung externer Sicherheitsbarrieren, wenn ein Patching oder eine Aktualisierung wünschenswert wäre, aber z. B. aufgrund nicht unterstützter Produkte nicht möglich ist;

f) Ausschreibungen unter Berücksichtigung der Cybersicherheit formulieren, d. h. Informationen über Sicherheitsmerkmale anfordern, die Einhaltung bestehender Cybersicherheitsnormen verlangen, Vorschläge darüber einholen, wie kontinuierliche Meldungen, Fehlerkorrekturen und Gegenmaßnahmen sichergestellt sind, wenn Schwachstellen entdeckt werden, und die Haftung des Verkäufers bei Cyberangriffen oder Cybersicherheitsvorfällen klären;

g) mit Technologieanbietern zusammenarbeiten, um ältere Systeme zu ersetzen, wann immer dies aus Sicherheitsgründen sinnvoll ist, wobei jedoch kritische Systemfunktionen zu berücksichtigen sind.

ÜBERWACHUNG

(13) Die Mitgliedstaaten sollten der Kommission binnen zwölf Monaten nach der Abgabe dieser Empfehlung und danach alle zwei Jahre über die Kooperationsgruppe für Netz- und Informationssicherheit detaillierte Informationen über den Stand der Umsetzung dieser Empfehlung mitteilen.

ÜBERPRÜFUNG

(14) Die Kommission wird die Umsetzung dieser Empfehlung auf der Grundlage der von den Mitgliedstaaten vorgelegten Informationen überprüfen und in Konsultation mit den Mitgliedstaaten und den relevanten Akteuren bewerten, ob weitere Maßnahmen erforderlich sind.

ADRESSATEN

(15) Diese Empfehlung ist an die Mitgliedstaaten gerichtet.

Brüssel, den 3. April 2019

Für die Kommission
Miguel ARIAS CAÑETE
Mitglied der Kommission