Delegierte Verordnung (EU) 2024/1366 der Kommission vom 11. März 2024 zur Ergänzung der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates durch Festlegung eines Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse

Vom 11. März 2024 (ABl. EU Reihe L 24.05.2024)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt[1], insbesondere auf Artikel 59 Absatz 2 Buchstabe e,

in Erwägung nachstehender Gründe:

(1) Das Risikomanagement im Bereich der Cybersicherheit ist für die Aufrechterhaltung der Stromversorgungssicherheit und die Gewährleistung eines hohen Cybersicherheitsniveaus im Elektrizitätssektor von entscheidender Bedeutung.

(2) Digitalisierung und Cybersicherheit sind entscheidend für die Erbringung wesentlicher Dienste und daher von strategischer Bedeutung für kritische Energieinfrastrukturen.

(3) In der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[2] sind Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union festgelegt. Die Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates[3] ergänzt die Richtlinie (EU) 2022/2555 dahin gehend, dass Cybersicherheits-

[1] ABl. L 158 vom 14.6.2019, S. 54.

[2] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

[3] Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über die Risikovorsorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG (ABl. L 158 vom 14.6.2019, S. 1).

vorfälle im Elektrizitätssektor ordnungsgemäß als Risiko bestimmt und in den Risikovorsorgeplänen angemessene Maßnahmen zu ihrer Bewältigung vorgesehen werden. Die Verordnung (EU) 2019/943 ergänzt die Richtlinie (EU) 2022/2555 und die Verordnung (EU) 2019/941 durch spezifische Vorschriften für den Elektrizitätssektor auf Unionsebene. Die vorliegende Delegierte Verordnung ergänzt darüber hinaus die Bestimmungen der Richtlinie (EU) 2022/2555 in Bezug auf den Elektrizitätssektor, soweit grenzüberschreitende Stromflüsse betroffen sind.

(4) Angesichts vernetzter digitalisierter Elektrizitätssysteme kann die Prävention und Bewältigung von Stromversorgungskrisen im Zusammenhang mit Cyberangriffen nicht als rein nationale Aufgabe angesehen werden. Das Potenzial für effizientere und kostengünstigere Maßnahmen sollte durch eine regionale und unionsweite Zusammenarbeit vollständig erschlossen werden. Dazu bedarf es eines gemeinsamen Regelwerks und besser koordinierter Verfahren, um sicherzustellen, dass die Mitgliedstaaten und andere Akteure wirksam grenzübergreifend zusammenarbeiten können, und um so Transparenz, Vertrauen und Solidarität zwischen den Mitgliedstaaten und den für die Bereiche Elektrizität und Cybersicherheit zuständigen Behörden zu stärken.

(5) Das Risikomanagement im Bereich der Cybersicherheit im Anwendungsbereich dieser Verordnung erfordert ein strukturiertes Verfahren, das unter anderem die Ermittlung der mit Cyberangriffen verbundenen Risiken für grenzüberschreitende Stromflüsse, die damit einhergehenden operativen Prozesse und Perimeter sowie die entsprechenden Cybersicherheitskontrollen und Überprüfungsmechanismen umfasst. Wenngleich sich der gesamte Prozess über Jahre erstreckt, sollte jeder einzelne Schritt zu einem hohen gemeinsamen Cybersicherheitsniveau in dem Sektor sowie zur Minderung von Cybersicherheitsrisiken beitragen. Alle an diesem Prozess Beteiligten sollten sich nach besten Kräften bemühen, die Methoden so bald wie möglich, d. h. unverzüglich, in jedem Fall aber spätestens innerhalb der in dieser Verordnung festgelegten Fristen, zu entwickeln und zu vereinbaren.

(6) Die in dieser Verordnung vorgesehenen Bewertungen des Cybersicherheitsrisikos auf der Ebene der Union, der Mitgliedstaaten, der Regionen und der einzelnen Einrichtungen können auf Risiken beschränkt werden, die sich aus Cyberangriffen im Sinne der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Ra-

tes[4] ergeben, sodass beispielsweise physische Angriffe, Naturkatastrophen und Ausfälle aufgrund eines Verlusts von Anlagen oder Humanressourcen ausgenommen sind. Unionsweite und regionale Risiken im Zusammenhang mit physischen Angriffen oder Naturkatastrophen im Elektrizitätsbereich sind bereits von anderen bestehenden Rechtsvorschriften der Union erfasst, etwa von Artikel 5 der Verordnung (EU) 2019/941 oder der Verordnung (EU) 2017/1485 der Kommission[5] zur Festlegung einer Leitlinie für den Übertragungsnetzbetrieb. Die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates[6] über die Resilienz kritischer Einrichtungen zielt ebenfalls darauf ab, Schwachstellen zu verringern und die physische Resilienz kritischer Einrichtungen zu stärken, und deckt alle relevanten natürlichen und vom Menschen verursachten Risiken ab, die sich auf die Erbringung wesentlicher Dienste auswirken können, wie z. B. Unfälle, Naturkatastrophen, Notlagen im Bereich der öffentlichen Gesundheit wie Pandemien, hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten, krimineller Unterwanderung und Sabotage.

(7) Der in dieser Verordnung eingeführte Begriff „Einrichtungen mit erheblichen oder kritischen Auswirkungen“ ist von grundlegender Bedeutung, um zu bestimmen, welche Einrichtungen den Verpflichtungen aus dieser Verordnung unterliegen. Der in den verschiedenen Bestimmungen dargelegte risikobasierte Ansatz zielt darauf ab, Prozesse, die Auswirkungen auf grenzüberschreitende Stromflüsse haben, sowie die damit verbundenen Vermögenswerte und die sie betreibenden Einrichtungen zu ermitteln. Die Auswirkungen, die mögliche Cyberangriffe auf deren Tätigkeiten im Bereich grenzüberschreitender Stromflüsse haben können, können als „erhebliche Auswirkungen“ oder „kritische Auswirkungen“ eingestuft werden. In Artikel 3 der Richtlinie (EU) 2022/2555 sind die Begriffe „wesentliche Einrichtungen“ und „wichtige

[4] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).

[5] Verordnung (EU) 2017/1485 der Kommission vom 2. August 2017 zur Festlegung einer Leitlinie für den Übertragungsnetzbetrieb (ABl. L 220 vom 25.8.2017, S. 1).

[6] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

Einrichtungen“ und die Kriterien für die Bestimmung von Einrichtungen in diesen Kategorien festgelegt. Wenngleich viele Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 der vorliegenden Verordnung gleichzeitig als „wesentliche Einrichtungen“ im Sinne des Artikels 3 der Richtlinie (EU) 2022/2555 betrachtet und eingestuft werden dürften, beziehen sich die in dieser Verordnung festgelegten Kriterien nur auf ihre Rolle und Auswirkungen in Elektrizitätsprozessen, die grenzüberschreitende Stromflüsse betreffen, ohne dass dabei die in Artikel 3 der Richtlinie (EU) 2022/2555 festgelegten Kriterien berücksichtigt werden.

(8) Bei den Einrichtungen, die als Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 in den Anwendungsbereich dieser Verordnung fallen und den darin festgelegten Verpflichtungen unterliegen, handelt es sich in erster Linie um Einrichtungen, die unmittelbare Auswirkungen auf grenzüberschreitende Stromflüsse in der EU haben.

(9) Diese Verordnung greift auf bestehende Mechanismen und Instrumente zurück, die bereits in anderen Rechtsvorschriften vorgesehen sind, um für Effizienz zu sorgen und Doppelarbeit bei der Verwirklichung der Ziele zu vermeiden.

(10) Bei der Anwendung dieser Verordnung sollten die Mitgliedstaaten, die zuständigen Behörden und die Netzbetreiber vereinbarte europäische Normen und technische Spezifikationen der europäischen Normungsorganisationen berücksichtigen und im Einklang mit den Rechtsvorschriften der Union über das Inverkehrbringen oder die Inbetriebnahme von Produkten handeln, die diesen Rechtsvorschriften der Union unterliegen.

(11) Zur Minderung von Cybersicherheitsrisiken ist es erforderlich, ein detailliertes Regelwerk für die Maßnahmen und die Zusammenarbeit zwischen den einschlägigen Interessenträgern, deren Tätigkeiten Cybersicherheitsaspekte grenzüberschreitender Stromflüsse betreffen, zu erstellen, um die Systemsicherheit zu gewährleisten. Diese organisatorischen und technischen Vorschriften sollten sicherstellen, dass die meisten Vorfälle bei der Stromversorgung, denen Cybersicherheitsursachen zugrunde liegen, auf operativer Ebene wirksam bewältigt werden. Dazu ist festzulegen, was die einschlägigen Interessenträger tun sollten, um solche Krisen zu verhindern, und welche Maßnahmen sie ergreifen können, wenn die Vorschriften für den Systembetrieb allein nicht mehr ausreichen. Daher ist es erforderlich, einen gemeinsamen Rechtsrahmen für die Prävention und Bewältigung zeitgleich auftretender Stromversorgungskrisen mit zugrunde liegenden Cybersicherheitsursachen und die Vorsorge für

solche Krisen zu schaffen. So wird die Transparenz bei der Vorsorge und während einer zeitgleich auftretenden Stromversorgungskrise erhöht und sichergestellt, dass zusammen mit den für die Cybersicherheit zuständigen Behörden in den Mitgliedstaaten koordinierte und wirksame Maßnahmen getroffen werden. Die Mitgliedstaaten und die einschlägigen Einrichtungen sollten verpflichtet werden, auf regionaler Ebene und gegebenenfalls bilateral solidarisch zusammenzuarbeiten. Diese Zusammenarbeit und diese Vorschriften sollen die Risikovorsorge im Bereich der Cybersicherheit, auch im Einklang mit den Zielen der Richtlinie (EU) 2022/2555, bei geringeren Kosten verbessern. Zudem erscheint es notwendig, den Elektrizitätsbinnenmarkt durch Förderung des Vertrauens in allen Mitgliedstaaten zu stärken, sodass insbesondere das Risiko einer unzulässigen Einschränkung grenzüberschreitender Stromflüsse gemindert und somit auch das Risiko negativer Ausstrahlungseffekte auf benachbarte Mitgliedstaaten verringert wird.

(12) Um die Stromversorgungssicherheit zu gewährleisten, bedarf es einer wirksamen Zusammenarbeit der Mitgliedstaaten, der Organe, Einrichtungen und sonstigen Stellen der Union sowie der maßgeblichen Interessenträger. Verteilernetzbetreiber und Übertragungsnetzbetreiber spielen gemäß den Artikeln 31 und 40 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates[7] bei der Gewährleistung eines sicheren, zuverlässigen und effizienten Elektrizitätssystems eine Schlüsselrolle. Auch die einzelnen Regulierungsbehörden und anderen zuständigen nationalen Behörden haben bei der Wahrnehmung ihrer Aufgaben aus den Richtlinien (EU) 2019/944 und (EU) 2022/2555 große Bedeutung für die Gewährleistung und Überwachung der Cybersicherheit der Stromversorgung. Die Mitgliedstaaten sollten eine bestehende oder neue Stelle als für die Durchführung dieser Verordnung zuständige nationale Behörde benennen, um eine transparente und inklusive Beteiligung aller Akteure, eine effiziente Vorbereitung und ordnungsgemäße Umsetzung dieser Beteiligung sowie die Zusammenarbeit zwischen den verschiedenen einschlägigen Interessenträgern und zuständigen Behörden in den Bereichen Elektrizität und Cybersicherheit zu gewährleisten und die Prävention und Ex-post-Bewertung von Stromversorgungskrisen, denen Cybersicherheitsursachen zugrunde liegen, sowie den damit

[7] Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU (ABl. L 158 vom 14.6.2019, S. 125).

verbundenen Informationsaustausch zu erleichtern.

(13) Wenn eine Einrichtung mit erheblichen oder kritischen Auswirkungen in mehr als einem Mitgliedstaat Dienstleistungen erbringt oder ihren Sitz oder eine Niederlassung oder Vertretung in einem Mitgliedstaat hat, sich ihre Netz- und Informationssysteme jedoch in einem oder mehreren anderen Mitgliedstaaten befinden, sollten diese Mitgliedstaaten ihre jeweiligen zuständigen Behörden dazu anhalten, sich nach besten Kräften um Zusammenarbeit zu bemühen und einander bei Bedarf zu unterstützen.

(14) Die Mitgliedstaaten sollten sicherstellen, dass die zuständigen Behörden über die erforderlichen Befugnisse verfügen, um bei Einrichtungen mit erheblichen oder kritischen Auswirkungen die Einhaltung dieser Verordnung zu fördern. Diese Befugnisse sollten es den zuständigen Behörden ermöglichen, sowohl Vor-Ort-Inspektionen als auch externe Aufsichtsmaßnahmen durchzuführen. Dies kann stichprobenartige Kontrollen, regelmäßige Audits, gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen und Sicherheitsscans nach objektiven, diskriminierungsfreien, fairen und transparenten Risikobewertungskriterien umfassen, einschließlich der Einholung von Informationen, die für die Bewertung der Cybersicherheitsmaßnahmen der Einrichtung erforderlich sind. Zu diesen Informationen sollten dokumentierte Cybersicherheitskonzepte, Zugangsdaten, Unterlagen und alle Angaben gehören, die für die Wahrnehmung ihrer Aufsichtsaufgaben erforderlich sind; zudem sollten sie Nachweise für die Umsetzung von Cybersicherheitskonzepten, wie die Ergebnisse von Sicherheitsaudits, die von einem qualifizierten Prüfer durchgeführt wurden, und die zugrunde liegenden Nachweise umfassen.

(15) Um Lücken sowie Überschneidungen zwischen den Risikomanagementverpflichtungen von Einrichtungen mit erheblichen oder kritischen Auswirkungen im Bereich der Cybersicherheit zu vermeiden, sollten die nationalen Behörden gemäß der Richtlinie (EU) 2022/2555 und die gemäß der vorliegenden Verordnung zuständigen Behörden bei der Umsetzung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit und der Überwachung der Einhaltung dieser Maßnahmen auf nationaler Ebene zusammenarbeiten. Hält eine Einrichtung die in dieser Verordnung festgelegten Anforderungen an das Cybersicherheitsrisikomanagement ein, könnte dies von den gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden auch als Gewährleistung der Einhaltung der entsprechenden Anforderungen der genannten Richtlinie betrachtet werden und umgekehrt.

(16) Für einen gemeinsamen Ansatz bei der Prävention und Bewältigung zeitgleich auftretender Stromversorgungskrisen ist ein gemeinsames Verständnis der Mitgliedstaaten darüber erforderlich, was unter einer zeitgleich auftretenden Stromversorgungskrise zu verstehen ist und wann ein Cyberangriff dabei ein wichtiger Faktor ist. Insbesondere sollte die Koordination zwischen den Mitgliedstaaten und den einschlägigen Einrichtungen erleichtert werden, um Situationen zu bewältigen, in denen aufgrund eines Cyberangriffs potenziell das Risiko einer erheblichen Stromknappheit oder einer Unterbrechung der Stromversorgung von Kunden besteht oder unmittelbar bevorsteht.

(17) In Erwägungsgrund 1 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[8] wird die entscheidende Rolle von Netz- und Informationssystemen sowie von elektronischen Kommunikationsnetzen und -diensten für die Aufrechterhaltung der Wirtschaft in Schlüsselsektoren wie dem Energiesektor anerkannt, und in Erwägungsgrund 44 wird auf die Notwendigkeit der Zusammenarbeit zwischen der Agentur der Europäischen Union für Cybersicherheit (ENISA) und der Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER) hingewiesen.

(18) In der Verordnung (EU) 2019/943 werden Übertragungsnetzbetreibern (ÜNB) und Verteilernetzbetreibern (VNB) besondere Zuständigkeiten im Bereich der Cybersicherheit übertragen. Ihre europäischen Verbände, d. h. das Europäische Netz der Übertragungsnetzbetreiber (ENTSO-E) und die Europäische Organisation der VNB (EU-VNBO), müssen nach Artikel 30 bzw. 55 der genannten Verordnung die Cybersicherheit in Zusammenarbeit mit den maßgeblichen Behörden und regulierten Unternehmen fördern.

(19) Im Hinblick auf einen gemeinsamen Ansatz für die Prävention und Bewältigung zeitgleich auftretender Stromversorgungskrisen mit zugrunde liegenden Cybersicherheitsursachen müssen zudem alle einschlägigen Interessenträger harmonisierte Methoden und Definitionen anwenden, um Risiken im Zusammenhang mit der Cybersicherheit der Stromversorgung zu ermitteln. Darüber hinaus muss es möglich sein,

[8] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

effektiv zu vergleichen, wie gut sie und ihre Nachbarn in diesem Bereich handeln. Dazu ist es erforderlich, die Verfahren, Rollen und Zuständigkeiten für die Entwicklung und Aktualisierung von Risikomanagementmethoden, von Skalen für die Einstufung von Sicherheitsvorfällen und von Cybersicherheitsmaßnahmen festzulegen, die an Cybersicherheitsrisiken mit Auswirkungen auf grenzüberschreitende Stromflüsse angepasst sind.

(20) Die Mitgliedstaaten sind über die gemäß dieser Verordnung benannte zuständige Behörde dafür verantwortlich, die Einrichtungen zu ermitteln, die die Kriterien für die Einstufung als Einrichtungen mit erheblichen Auswirkungen oder als Einrichtungen mit kritischen Auswirkungen erfüllen. Um die Unterschiede zwischen den Mitgliedstaaten in diesem Bereich zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und der Berichterstattungspflichten zu gewährleisten, sollte eine Reihe von Kriterien dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Verordnung fallen. Diese Kriterien sollten im Rahmen des Verfahrens für die Entwicklung und Annahme der in dieser Verordnung genannten Modalitäten und Methoden festgelegt und regelmäßig aktualisiert werden.

(21) Die Bestimmungen dieser Verordnung sollten das Unionsrecht, das spezifische Vorschriften für die Zertifizierung von Produkten, Diensten und Prozessen der Informations- und Kommunikationstechnologie (IKT) enthält, unberührt lassen, insbesondere die Verordnung (EU) 2019/881 in Bezug auf den Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung. Im Rahmen der vorliegenden Verordnung sollten IKT- Produkte auch technische Geräte und Software umfassen, die eine direkte Interaktion mit dem elektrotechnischen Netz ermöglichen, insbesondere industrielle Steuerungssysteme, die für die Energieübertragung, Energieverteilung und Energieerzeugung sowie für die Erhebung und Übermittlung damit zusammenhängender Informationen genutzt werden können. Die Bestimmungen sollten sicherstellen, dass die einschlägigen Sicherheitsziele aus Artikel 51 der Verordnung (EU) 2019/881 von den zu beschaffenden IKT-Produkten, -Diensten und -Prozessen erfüllt werden.

(22) Wie aktuelle Cyberangriffe gezeigt haben, sind Einrichtungen zunehmend von Angriffen auf Lieferketten betroffen. Diese Angriffe auf die Lieferkette wirken sich nicht nur auf einzelne Einrichtungen im Anwendungsbereich aus, sondern können auch Kaskadenwirkung haben und zu größeren Angriffe führen, die auch die mit

ihnen über das Stromnetz verbundenen Einrichtungen in Mitleidenschaft ziehen. Daher wurden auch Bestimmungen und Empfehlungen aufgenommen, die dazu beitragen sollen, die Cybersicherheitsrisiken im Zusammenhang mit Prozessen zu mindern, die die Lieferketten, insbesondere die Auftragsvergabe, betreffen und Auswirkungen auf grenzüberschreitende Stromflüsse haben.

(23) Da bei der Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche Unterbrechungen der Energieversorgung und Schäden für Wirtschaft und Verbraucher entstehen können, sollten diese Schwachstellen rasch ermittelt und behoben werden, um die mit ihnen verbundenen Risiken zu verringern. Zur Unterstützung einer wirksamen Durchführung dieser Verordnung sollten die einschlägigen Einrichtungen und zuständigen Behörden zusammenarbeiten, um für diesen Zweck als angemessen erachtete Tätigkeiten zu üben und zu prüfen, einschließlich des Informationsaustauschs über Cyberbedrohungen, Cyberangriffe, Schwachstellen, Instrumente und Methoden, Taktiken, Techniken und Verfahren, der Vorsorge für das Cybersicherheitskrisenmanagement und anderer Maßnahmen. Da sich die Technik ständig weiterentwickelt und der Elektrizitätssektor rasch digitalisiert wird, sollte die Umsetzung der angenommenen Bestimmungen Innovationen nicht behindern und keine Hindernisse für den Zugang neuer Unternehmen zum Strommarkt und die anschließende Nutzung innovativer Lösungen schaffen, die zu einer effizienteren und nachhaltigeren Gestaltung des Elektrizitätssystems beitragen.

(24) Die zur Überwachung der Durchführung dieser Verordnung erhobenen Informationen sollten nach dem Grundsatz „Kenntnis nur, wenn nötig“ angemessen beschränkt werden. Die Fristen für die Übermittlung dieser Informationen sollten für die beteiligten Interessenträger umsetzbar und wirksam sein. Doppelmeldungen sollten vermieden werden.

(25) Der Cybersicherheitsschutz endet nicht an den Grenzen der Union. Um ein sicheres System zu gewährleisten, müssen auch benachbarte Drittländer einbezogen werden. Die Union und ihre Mitgliedstaaten sollten sich darum bemühen, benachbarte Drittländer, deren Strominfrastruktur mit dem europäischen Netz verbunden ist, bei der Anwendung ähnlicher Cybersicherheitsvorschriften wie den in dieser Verordnung enthaltenen Vorschriften zu unterstützen.

(26) Um die Koordination im Bereich der Sicherheit rasch zu verbessern und künftige verbindliche Modalitäten und Methoden zu prüfen, sollten ENTSO-E, die EU-VNBO und die zuständigen Behörden unmittelbar nach dem Inkrafttreten dieser Verordnung

mit der Ausarbeitung unverbindlicher Leitlinien beginnen. Diese Leitlinien werden als Ausgangsbasis für die Entwicklung künftiger Modalitäten und Methoden dienen. Parallel dazu sollten die zuständigen Behörden Einrichtungen ermitteln, die als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft werden könnten, damit diese auf freiwilliger Basis mit der Erfüllung der Verpflichtungen beginnen können.

(27) Diese Verordnung wurde in enger Zusammenarbeit mit der ACER, der ENISA, ENTSO-E, der EU-VNBO und weiteren Interessenträgern erarbeitet, um auf transparente und partizipative Weise wirksame, ausgewogene und verhältnismäßige Vorschriften zu erlassen.

(28) Diese Verordnung ergänzt und erweitert die im EU-Rahmen für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 der Kommission[9] festgelegten Krisenmanagementmaßnahmen. Ein Cyberangriff könnte auch eine Stromversorgungskrise im Sinne des Artikels 2 Nummer 9 der Verordnung (EU) 2019/941 mit Auswirkungen auf grenzüberschreitende Stromflüsse verursachen, dazu beitragen oder mit ihr zusammenfallen. Eine solche Stromversorgungskrise könnte zu einer zeitgleich auftretenden Stromversorgungskrise im Sinne des Artikels 2 Nummer 10 der Verordnung (EU) 2019/941 führen. Ein solcher Vorfall könnte sich auch auf andere, von der Stromversorgungssicherheit abhängige Sektoren auswirken. Sollte ein solcher Vorfall zu einem Cybersicherheitsvorfall großen Ausmaßes im Sinne des Artikels 16 der Richtlinie (EU) 2022/2555 eskalieren, sollten die Bestimmungen des genannten Artikels zur Einrichtung des Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) angewandt werden. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen gemäß dem Durchführungsbeschluss (EU) 2018/1993 des Rates[10] (IPCR-Regelung) stützen.

(29) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergrei-

[9] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

[10] Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die Integrierte EU-Regelung für die politische Reaktion auf Krisen (ABl. L 320 vom 17.12.2018, S. 28).

fen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Verordnung unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht.

(30) Diese Verordnung gilt zwar grundsätzlich auch für Einrichtungen, die in der Erzeugung von Strom aus Kernkraftwerken tätig sind, einige dieser Tätigkeiten können jedoch mit der nationalen Sicherheit in Verbindung stehen.

(31) Jede Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung sollte dem Unionsrecht zum Datenschutz und zum Schutz der Privatsphäre unterliegen. Insbesondere lässt diese Verordnung die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[11], die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[12] und die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[13] unberührt. Diese Verordnung sollte daher unter anderem nicht die Aufgaben und Befugnisse der Behörden berühren, die für die Überwachung der Einhaltung des geltenden Unionsrechts zum Datenschutz und zum Schutz der Privatsphäre zuständig sind.

(32) Angesichts der Bedeutung der internationalen Zusammenarbeit im Bereich der Cybersicherheit sollten sich die von den Mitgliedstaaten benannten, für die Wahrnehmung der ihnen im Rahmen dieser Verordnung übertragenen Aufgaben zuständigen Behörden an internationalen Kooperationsnetzen beteiligten können. Zur Wahrnehmung ihrer Aufgaben sollten die zuständigen Behörden daher Informationen, einschließlich personenbezogener Daten, mit den zuständigen Behörden von

---

[11] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[12] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

[13] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

Drittländern austauschen können, sofern die Bedingungen des Datenschutzrechts der Union für die Übermittlung personenbezogener Daten in Drittländer erfüllt sind, einschließlich der Bedingungen aus Artikel 49 der Verordnung (EU) 2016/679.

(33) Die Verarbeitung personenbezogener Daten durch Einrichtungen mit erheblichen oder kritischen Auswirkungen in dem zur Gewährleistung der Sicherheit von Vermögenswerten erforderlichen und verhältnismäßigen Umfang könnte auf der Grundlage als rechtmäßig angesehen werden, dass diese Verarbeitung einer rechtlichen Verpflichtung entspricht, der der Verantwortliche gemäß Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 unterliegt. Die Verarbeitung personenbezogener Daten kann auch für berechtigte Interessen erforderlich sein, die von Einrichtungen mit erheblichen oder kritischen Auswirkungen sowie von Anbietern von Sicherheitstechnologien und -diensten, die im Namen dieser Einrichtungen handeln, gemäß Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 wahrgenommen werden, auch wenn eine solche Verarbeitung für Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder die freiwillige Mitteilung relevanter Informationen gemäß der vorliegenden Verordnung erforderlich ist. Maßnahmen zur Verhütung, Erkennung, Identifizierung, Eindämmung, Analyse und Bewältigung von Cyberangriffen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, der Informationsaustausch zur Behebung und zur koordinierten Offenlegung von Schwachstellen, der freiwillige Austausch von Informationen über solche Cyberangriffe sowie über Cyberbedrohungen und Schwachstellen, Kompromittierungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools können es erforderlich machen, bestimmte Kategorien personenbezogener Daten wie IP-Adressen, URL-Adressen, Domänennamen, E-Mail-Adressen oder, sofern diese personenbezogene Daten enthalten, Zeitstempel zu verarbeiten. Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden, zentralen Anlaufstellen und CSIRTs kann eine rechtliche Verpflichtung darstellen oder für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem jeweiligen Verantwortlichen gemäß Artikel 6 Absatz 1 Buchstabe c oder e und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 übertragen wurde, oder zur Verfolgung eines berechtigten Interesses von Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 6 Absatz 1 Buchstabe f jener Verordnung als erforderlich angesehen werden. Darüber hinaus können im nationalen Recht Vorschriften festgelegt werden,

die es den zuständigen Behörden, zentralen Anlaufstellen und CSIRTs ermöglichen, besondere Kategorien personenbezogener Daten gemäß Artikel 9 der Verordnung (EU) 2016/679 zu verarbeiten, soweit dies zur Gewährleistung der Sicherheit der Netz- und Informationssysteme von Einrichtungen mit erheblichen oder kritischen Auswirkungen erforderlich und verhältnismäßig ist, wozu insbesondere geeignete und besondere Maßnahmen zum Schutz der Grundrechte und Interessen natürlicher Personen vorgesehen werden, einschließlich technischer Beschränkungen für die Weiterverwendung solcher Daten und die Anwendung modernster Sicherheits- und Datenschutzvorkehrungen wie Pseudonymisierung oder Verschlüsselung, wenn die Anonymisierung den verfolgten Zweck erheblich beeinträchtigen könnte.

(34) Häufig ist bei Cyberangriffen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden mit den in der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG genannten Behörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.

(35) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und hat am 17. November 2023 eine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Kapitel I – Allgemeine Bestimmungen

Artikel 1 Gegenstand

Diese Verordnung enthält einen Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse, einschließlich Vorschriften über gemeinsame Mindestanforderungen, Planung, Beobachtung, Berichterstattung und die Krisenbewältigung.

Artikel 2 Anwendungsbereich

(1) Diese Verordnung gilt für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse bei den Tätigkeiten der folgenden Einrichtungen, soweit diese gemäß Artikel 24 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft werden:

a) Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944;

b) nominierte Strommarktbetreiber (NEMOs) im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943;

c) organisierte Marktplätze oder organisierte Märkte im Sinne des Artikels 2 Nummer 4 der Durchführungsverordnung (EU) Nr. 1348/2014 der Kommission[14], die Transaktionen mit Produkten arrangieren, die für grenzüberschreitende Stromflüsse relevant sind;

d) Anbieter kritischer IKT-Dienste im Sinne des Artikels 3 Nummer 9 dieser Verordnung;

e) ENTSO-E, das gemäß Artikel 28 der Verordnung (EU) 2019/943 eingerichtet wurde;

f) die EU-VNBO, die gemäß Artikel 52 der Verordnung (EU) 2019/943 eingerichtet wurde;

g) Bilanzkreisverantwortliche im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/943;

h) Betreiber von Ladepunkten im Sinne des Anhangs I der Richtlinie (EU) 2022/2555;

i) regionale Koordinierungszentren (RCC) gemäß Artikel 35 der Verordnung (EU) 2019/943;

j) Anbieter verwalteter Sicherheitsdienste (MSSP) gemäß Artikel 6 Nummer 40 der Richtlinie (EU) 2022/2555;

k) alle sonstigen Einrichtungen oder Dritte, denen gemäß dieser Verordnung Zuständigkeiten übertragen oder zugewiesen werden.

(2) Die folgenden Behörden sind im Rahmen ihres derzeitigen Auftrags für die Wahrnehmung der in dieser Verordnung festgelegten Aufgaben zuständig:

[14] Durchführungsverordnung (EU) Nr. 1348/2014 der Kommission vom 17. Dezember 2014 über die Datenmeldung gemäß Artikel 8 Absätze 2 und 6 der Verordnung (EU) Nr. 1227/2011 des Europäischen Parlaments und des Rates über die Integrität und Transparenz des Energiegroßhandelsmarkts (ABl. L 363 vom 18.12.2014, S. 121).

a) die mit der Verordnung (EU) 2019/942 des Europäischen Parlaments und des Rates[15]eingerichtete Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER);

b) die nationalen zuständigen Behörden, die für die Wahrnehmung der ihnen gemäß dieser Verordnung übertragenen Aufgaben verantwortlich sind und von den Mitgliedstaaten gemäß Artikel 4 als „zuständige Behörde“ benannt wurden;

c) die gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944 benannten nationalen Regulierungsbehörden (NRB) der einzelnen Mitgliedstaaten;

d) die gemäß Artikel 3 der Verordnung (EU) 2019/941 benannten für die Risikovorsorge zuständigen Behörden (RP-NCA);

e) die gemäß Artikel 10 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten Computer-Notfallteams (CSIRTs);

f) die gemäß Artikel 8 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten für die Cybersicherheit zuständigen Behörden (CS-NCA);

g) die gemäß der Verordnung (EU) 2019/881 errichtete Agentur der Europäischen Union für Cybersicherheit;

h) alle sonstigen Behörden oder Dritte, denen gemäß Artikel 4 Absatz 3 Zuständigkeiten übertragen oder zugewiesen werden.

(3) Diese Verordnung gilt auch für alle Einrichtungen, die nicht in der Union niedergelassen sind, aber Dienstleistungen für Einrichtungen in der Union erbringen, sofern sie von den zuständigen Behörden gemäß Artikel 24 Absatz 2 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

(4) Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, einschließlich der Wahrung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung, unberührt.

(5) Diese Verordnung lässt die Zuständigkeit der Mitgliedstaaten für die Aufrechter-

[15] Verordnung (EU) 2019/942 des Europäischen Parlaments und des Rates vom 5. Juni 2019 zur Gründung einer Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ABl. L 158 vom 14.6.2019, S. 22).

haltung der nationalen Sicherheit in Bezug auf Tätigkeiten zur Stromerzeugung in Kernkraftwerken, einschließlich Tätigkeiten innerhalb der nuklearen Wertschöpfungskette, im Einklang mit den Verträgen unberührt.

(6) Soweit dies für die Zwecke dieser Verordnung erforderlich ist, werden personenbezogene Daten von Einrichtungen, den zuständigen Behörden, den zentralen Anlaufstellen auf Ebene der Einrichtung und den CSIRTs im Einklang mit der Verordnung (EU) 2016/679, insbesondere auf der Grundlage von Artikel 6 der genannten Verordnung, verarbeitet.

Artikel 3 Begriffsbestimmungen

Es gelten die folgenden Begriffsbestimmungen:

1. „Vermögenswert“ bezeichnet alle Informationen sowie jede Software oder Hardware, gleich ob materieller oder immaterieller Art, in Netz- und Informationssystemen, die für eine natürliche Person, eine Organisation oder eine Regierung von Wert sind;
2. „für die Risikovorsorge zuständige Behörde“ bezeichnet die gemäß Artikel 3 der Verordnung (EU) 2019/941 benannte zuständige Behörde;
3. „Computer-Notfallteam“ bezeichnet ein gemäß Artikel 10 der Richtlinie (EU) 2022/2555 für die Bewältigung von Risiken und Sicherheitsvorfällen zuständiges Team;
4. „Vermögenswert mit kritischen Auswirkungen“ bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit kritischen Auswirkungen erforderlich ist;
5. „Einrichtung mit kritischen Auswirkungen“ bezeichnet eine Einrichtung, die einen Prozess mit kritischen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 bestimmt wird;
6. „Perimeter mit kritischen Auswirkungen“ bezeichnet einen von einer in Artikel 2 Absatz 1 genannten Einrichtung definierten Perimeter, der alle Vermögenswerte mit kritischen Auswirkungen umfasst und in dem der Zugang zu diesen Vermögenswerten kontrolliert werden kann und der den Anwendungsbereich bestimmt, in dem die erweiterten Cybersicherheitskontrollen anzuwenden sind;

7. „Prozess mit kritischen Auswirkungen“ bezeichnet einen Geschäftsprozess einer Einrichtung, dessen Indizes für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor über dem Schwellenwert für kritische Auswirkungen liegen;

8. „Schwellenwert für kritische Auswirkungen“ bezeichnet die Werte der in Artikel 19 Absatz 3 Buchstabe b genannten Indizes für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor, bei deren Überschreitung ein Cyberangriff auf einen Geschäftsprozess zu einer kritischen Störung grenzüberschreitender Stromflüsse führt;

9. „Anbieter kritischer IKT-Dienste“ bezeichnet eine Einrichtung, die einen IKT-Dienst oder einen IKT-Prozess bereitstellt, der für einen Prozess mit kritischen oder erheblichen Auswirkungen, der sich auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse auswirkt, erforderlich ist und bei dessen Kompromittierung ein Cyberangriff erfolgen könnte, dessen Auswirkungen den Schwellenwert für kritische oder erhebliche Auswirkungen überschreiten;

10. „grenzüberschreitender Stromfluss“ bezeichnet einen grenzüberschreitenden Stromfluss im Sinne des Artikels 2 Nummer 3 der Verordnung (EU) 2019/943;

11. „Cyberangriff“ bezeichnet einen Vorfall im Sinne des Artikels 3 Nummer 14 der Verordnung (EU) 2022/2554;

12. „Cybersicherheit“ bezeichnet Cybersicherheit im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2019/881;

13. „Cybersicherheitskontrolle“ bezeichnet die zur Vermeidung, Erkennung, Bekämpfung oder Minimierung von Cybersicherheitsrisiken durchgeführten Maßnahmen oder Verfahren;

14. „Cybersicherheitsvorfall“ bezeichnet einen Vorfall im Sinne des Artikels 6 Nummer 6 der Richtlinie (EU) 2022/2555;

15. „Cybersicherheitsmanagementsystem“ bezeichnet die Konzepte, Verfahren, Leitlinien sowie die damit verbundenen Ressourcen und Tätigkeiten, die von einer Einrichtung insgesamt verwaltet werden, um ihre Informationsressourcen vor Cyberbedrohungen zu schützen, wobei die Sicherheit der Netz- und Informationssysteme einer Organisation systematisch bestimmt, umgesetzt, betrieben, überwacht, überprüft, aufrechterhalten und verbessert wird;

16. „Betriebszentrum für Cybersicherheit“ bezeichnet ein spezielles Zentrum, in dem ein aus einem oder mehreren Sachverständigen bestehendes technisches Team mithilfe von IT-Systemen für Cybersicherheit sicherheitsbezogene Aufgaben (Dienste von Cybersicherheits-Betriebszentren, CSOC-Dienste) wahrnimmt, wie z. B. den Umgang mit Cyberangriffen und Fehlern bei der Sicherheitskonfiguration, Sicherheitsüberwachung, Protokollanalyse und die Erkennung von Cyberangriffen;

17. „Cyberbedrohung“ bezeichnet eine Cyberbedrohung im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/881;

18. „Schwachstellenmanagement im Bereich der Cybersicherheit“ bezeichnet die Praxis, Schwachstellen zu ermitteln und zu beheben;

19. „Einrichtung“ bezeichnet eine Einrichtung im Sinne des Artikels 6 Nummer 38 der Richtlinie (EU) 2022/2555;

20. „Frühwarnung“ bezeichnet die erforderliche Unterrichtung, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

21. „Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor“ (ECII) bezeichnet einen Index oder eine Klassifizierungsskala, mit dem/der die möglichen Folgen von Cyberangriffen auf Geschäftsprozesse im Zusammenhang mit grenzüberschreitenden Stromflüssen eingestuft werden;

22. „europäisches Schema für die Cybersicherheitszertifizierung“ bezeichnet ein Schema im Sinne des Artikels 2 Nummer 9 der Verordnung (EU) 2019/881;

23. „Einrichtung mit erheblichen Auswirkungen“ bezeichnet eine Einrichtung, die einen Prozess mit erheblichen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 ermittelt wird;

24. „Prozess mit erheblichen Auswirkungen“ bezeichnet jeden Geschäftsprozess einer Einrichtung, dessen Indizes für die Auswirkungen von Cybersicherheitsvorfällen im Elektrizitätssektor über den Schwellenwerten für erhebliche Auswirkungen liegen;

25. „Vermögenswert mit erheblichen Auswirkungen“ bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit erheblichen Auswirkungen erforderlich ist;

26. „Schwellenwert für erhebliche Auswirkungen“ bezeichnet die Werte der in Artikel 19 Absatz 3 Buchstabe b genannten Indizes für die Auswirkungen von Cybersicherheitsvorfällen im Elektrizitätssektor, bei deren Überschreitung ein erfolgreich durchgeführter Cyberangriff auf einen Prozess zu einer erheblichen Störung grenzüberschreitender Stromflüsse führt;

27. „Perimeter mit erheblichen Auswirkungen“ bezeichnet einen von einer der in Artikel 2 Absatz 1 aufgeführten Einrichtungen definierten Perimeter, der alle Vermögenswerte mit erheblichen Auswirkungen umfasst und in dem der Zugang zu diesen Vermögenswerten kontrolliert werden kann und der den Anwendungsbereich bestimmt, in dem die Mindestsicherheitskontrollen anzuwenden sind;

28. „IKT-Produkt“ bezeichnet ein IKT-Produkt im Sinne des Artikels 2 Nummer 12 der Verordnung (EU) 2019/881;

29. „IKT-Dienst“ bezeichnet einen IKT-Dienst im Sinne des Artikels 2 Nummer 13 der Verordnung (EU) 2019/881;

30. „IKT-Prozess“ bezeichnet einen IKT-Prozess im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/881;

31. „Altsystem“ bezeichnet ein IKT-Altsystem im Sinne des Artikels 3 Nummer 3 der Verordnung (EU) 2022/2554;

32. „nationale zentrale Anlaufstelle“ bezeichnet die von jedem Mitgliedstaat gemäß Artikel 8 Absatz 3 der Richtlinie (EU) 2022/2555 benannte oder eingerichtete zentrale Anlaufstelle;

33. „NIS-Behörden für das Cyberkrisenmanagement“ bezeichnet die gemäß Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten Behörden;

34. „Urheber“ bezeichnet eine Einrichtung, die einen Informationsaustausch, eine Informationsübermittlung oder die Speicherung von Informationen einleitet;

35. „Spezifikationen für die Auftragsvergabe“ bezeichnet die von Einrichtungen für die Beschaffung neuer oder aktualisierter IKT-Produkte, -Prozesse oder -Dienste festgelegten Spezifikationen;

36. „Vertreter“ bezeichnet eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich dafür benannt wurde, im Namen einer Ein-

richtung mit erheblichen oder kritischen Auswirkungen, die nicht in der Union niedergelassen ist, aber Dienstleistungen für Einrichtungen in der Union erbringt, zu handeln, und an die sich eine zuständige Behörde oder ein CSIRT — statt an die Einrichtung mit erheblichen oder kritischen Auswirkungen — in Bezug auf die in dieser Verordnung festgelegten Verpflichtungen dieser Einrichtung wenden kann;

37. „Risiko“ bezeichnet ein Risiko im Sinne des Artikels 6 Nummer 9 der Richtlinie (EU) 2022/2555;

38. „Risiko-Auswirkungs-Matrix“ bezeichnet eine Matrix, die bei der Risikobewertung genutzt wird, um für jedes bewertete Risiko die mit ihm verbundenen Auswirkungen zu bestimmen;

39. „zeitgleich auftretende Stromversorgungskrise“ bezeichnet eine Stromversorgungskrise im Sinne des Artikels 2 Nummer 10 der Verordnung (EU) 2019/941;

40. „zentrale Anlaufstelle auf Ebene der Einrichtung“ bezeichnet eine zentrale Anlaufstelle bei der Einrichtung gemäß Artikel 38 Absatz 1 Buchstabe c;

41. „Interessenträger“ bezeichnet jede Partei, die am Erfolg und laufenden Betrieb einer Organisation oder eines Prozesses beteiligt ist, wie z. B. Beschäftigte, Direktoren, Anteilseigner, Regulierungsbehörden, Verbände, Lieferanten und Kunden;

42. „Norm“ bezeichnet eine Norm im Sinne des Artikels 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[16];

43. „Netzbetriebsregion“ bezeichnet die gemäß Artikel 36 der Verordnung (EU) 2019/943 festgelegten Netzbetriebsregionen, die in Anhang I der Entschei-

[16] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

dung 05-2022 der ACER über die Definition der Netzbetriebsregionen bestimmt wurden;

44. „Netzbetreiber“ bezeichnet „Verteilernetzbetreiber“ (VNB) und „Übertragungsnetzbetreiber“ (ÜNB) im Sinne des Artikels 2 Nummer 29 bzw. Nummer 35 der Richtlinie (EU) 2019/944;

45. „unionsweiter Prozess mit kritischen Auswirkungen“ bezeichnet jeden Prozess im Elektrizitätssektor, an dem mehrere Einrichtungen beteiligt sein können und bei dem die möglichen Auswirkungen eines Cyberangriffs bei der Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos für kritisch erachtet werden können;

46. „unionsweiter Prozess mit erheblichen Auswirkungen“ bezeichnet jeden Prozess im Elektrizitätssektor, an dem mehrere Einrichtungen beteiligt sein können und bei dem die möglichen Auswirkungen eines Cyberangriffs bei der Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos für erheblich erachtet werden können;

47. „aktiv ausgenutzte Schwachstelle ohne Patch“ bezeichnet eine noch nicht öffentlich bekannt gegebene und noch nicht mit einem Patch versehene Schwachstelle, in Bezug auf die verlässliche Nachweise dafür vorliegen, dass ein Akteur ohne Zustimmung des Systemeigners einen schädlichen Programmcode in einem System ausgeführt hat;

48. „Schwachstelle“ bezeichnet eine Schwachstelle im Sinne des Artikels 6 Nummer 15 der Richtlinie (EU) 2022/2555.

Artikel 4 Zuständige Behörde

(1) So bald wie möglich, in jedem Fall aber bis zum 13 Dezember 2024, benennt jeder Mitgliedstaat eine nationale Regierungs- oder Regulierungsbehörde, die für die Wahrnehmung der ihr in dieser Verordnung übertragenen Aufgaben zuständig ist (im Folgenden „zuständige Behörde“). Bis die Aufgaben im Rahmen dieser Verordnung auf die zuständige Behörde übertragen wurden, nimmt die von jedem Mitgliedstaat gemäß Artikel 57 Absatz 1 der Richtlinie (EU) 2019/944 benannte Regulierungsbehörde die Aufgaben der zuständigen Behörde im Einklang mit dieser Verordnung wahr.

(2) Die Mitgliedstaaten unterrichten die Kommission, die ACER, die ENISA, die ge-

mäß Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzte NIS-Kooperationsgruppe und die gemäß Artikel 1 des Beschlusses der Kommission vom 15. November 2012[17] eingesetzte Koordinierungsgruppe „Strom“ unverzüglich und teilen ihnen den Namen und die Kontaktdaten ihrer gemäß Absatz 1 des vorliegenden Artikels benannten zuständigen Behörde sowie etwaige spätere Änderungen in Bezug auf diese Behörde mit.

(3) Die Mitgliedstaaten können ihrer zuständigen Behörde gestatten, Aufgaben, die ihr in dieser Verordnung übertragen wurden, an andere nationale Behörden zu delegieren, mit Ausnahme der in Artikel 5 aufgeführten Aufgaben. Jede zuständige Behörde überwacht die Anwendung dieser Verordnung durch die Behörden, an die sie Aufgaben delegiert hat. Die zuständige Behörde teilt der Kommission, der ACER, der Koordinierungsgruppe „Strom“, der ENISA und der NIS- Kooperationsgruppe den Namen der Behörden, an die sie Aufgaben delegiert hat, deren Kontaktdaten, die ihnen übertragenen Aufgaben sowie etwaige spätere Änderungen mit.

Artikel 5 Zusammenarbeit zwischen den zuständigen Behörden und Stellen auf nationaler Ebene

Die zuständigen Behörden koordinieren und gewährleisten eine angemessene Zusammenarbeit zwischen den für Cybersicherheit zuständigen Behörden, den Behörden für das Cyberkrisenmanagement, den NRB, den für die Risikovorsorge zuständigen Behörden und den CSIRTs im Hinblick auf die Erfüllung der in dieser Verordnung festgelegten einschlägigen Verpflichtungen. Zudem stimmen sich die zuständigen Behörden mit anderen von den einzelnen Mitgliedstaaten bestimmten Stellen oder Behörden ab, um effiziente Verfahren sicherzustellen und Überschneidungen von Aufgaben und Pflichten zu vermeiden. Die zuständigen Behörden können die jeweiligen NRB anweisen, die ACER gemäß Artikel 8 Absatz 3 um eine Stellungnahme zu ersuchen.

Artikel 6 Modalitäten oder Methoden oder Pläne

(1) Die ÜNB entwickeln in Zusammenarbeit mit der EU-VNBO Vorschläge für die Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3.

[17] Beschluss der Kommission vom 15. November 2012 zur Einsetzung der Koordinierungsgruppe „Strom“ (2012/C 353/02) (ABl. C 353 vom 17.11.2012, S. 2).

(2) Die folgenden Modalitäten oder Methoden und etwaige Änderungen dieser Modalitäten oder Methoden bedürfen der Genehmigung aller zuständigen Behörden:

a) die Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

b) der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;

c) die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29, der Vergleich der Cybersicherheitskontrollen im Elektrizitätssektor anhand von Normen gemäß Artikel 34, einschließlich Mindest-Cybersicherheitskontrollen und erweiterter Cybersicherheitskontrollen in der Lieferkette gemäß Artikel 33;

d) eine Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;

e) die Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8.

(3) Die Vorschläge für die regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22 bedürfen der Genehmigung aller zuständigen Behörden der betreffenden Netzbetriebsregion.

(4) Die Vorschläge für Modalitäten oder Methoden gemäß Absatz 2 bzw. für Pläne gemäß Absatz 3 müssen einen Vorschlag für den Zeitplan für ihre Umsetzung und eine Beschreibung ihrer erwarteten Auswirkungen auf die Ziele dieser Verordnung enthalten.

(5) Die EU-VNBO kann den betreffenden ÜNB bis zu drei Wochen vor Ablauf der Frist für die Übermittlung des Vorschlags für Modalitäten, Methoden oder Pläne an die zuständigen Behörden eine mit Gründen versehene Stellungnahme übermitteln. Die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständigen ÜNB berücksichtigen die mit Gründen versehene Stellungnahme der EU-VNBO, bevor sie den Vorschlag den zuständigen Behörden zur Genehmigung vorlegen. Wenn die ÜNB die Stellungnahme der EU-VNBO nicht berücksichtigen, begründen sie dies.

(6) Bei der gemeinsamen Entwicklung von Modalitäten, Methoden und Plänen arbeiten die teilnehmenden ÜNB eng zusammen. Die ÜNB unterrichten die zuständigen Behörden und die ACER mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO regelmäßig über die Fortschritte bei der Entwicklung der Modalitäten, Methoden oder Pläne.

Artikel 7 Vorschriften für Abstimmungen der ÜNB

(1) Können ÜNB bei der Entscheidung über Vorschläge für Modalitäten oder Methoden keine Einigung erzielen, so entscheiden sie mit qualifizierter Mehrheit. Die qualifizierte Mehrheit für diese Vorschläge wird wie folgt berechnet:

a) ÜNB, die mindestens 55 % der Mitgliedstaaten vertreten, und

b) ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der Union umfassen.

(2) Eine Sperrminorität bei Entscheidungen über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden ist mit ÜNB erreicht, die mindestens vier Mitgliedstaaten vertreten; andernfalls gilt die qualifizierte Mehrheit als erreicht.

(3) Können ÜNB einer Netzbetriebsregion bei der Entscheidung über Vorschläge für die in Artikel 6 Absatz 2 genannten Pläne keine Einigung erzielen und besteht die betreffende Netzbetriebsregion aus mehr als fünf Mitgliedstaaten, so entscheiden die ÜNB mit qualifizierter Mehrheit. Bei Vorschlägen gemäß Artikel 6 Absatz 2 ist für eine qualifizierte Mehrheit folgende Mehrheit erforderlich:

a) ÜNB, die mindestens 72 % der betroffenen Mitgliedstaaten vertreten, und

b) ÜNB, die Mitgliedstaaten vertreten, die mindestens 65 % der Bevölkerung der betroffenen Region umfassen.

(4) Eine Sperrminorität für Entscheidungen über Vorschläge für die Pläne muss eine Mindestanzahl von ÜNB umfassen, die mehr als 35 % der Bevölkerung der teilnehmenden Mitgliedstaaten vertreten, zuzüglich ÜNB, die mindestens einen weiteren betroffenen Mitgliedstaat vertreten; ansonsten gilt die qualifizierte Mehrheit als erreicht.

(5) Bei Entscheidungen der ÜNB über Vorschläge für in Artikel 6 Absatz 2 aufgeführte Modalitäten oder Methoden erhält jeder Mitgliedstaat eine Stimme. Gibt es im Hoheitsgebiet eines Mitgliedstaats mehr als einen ÜNB, teilt der Mitgliedstaat die Stimmrechte unter den ÜNB auf.

(6) Legen ÜNB den jeweils zuständigen Behörden nicht innerhalb der in dieser Verordnung festgelegten Fristen in Zusammenarbeit mit der EU-VNBO einen ersten oder geänderten Vorschlag für Modalitäten oder Methoden oder für Pläne vor, so übermitteln sie den jeweils zuständigen Behörden und der ACER entsprechende Entwürfe der Modalitäten oder Methoden bzw. der Pläne. Sie erläutern, warum keine Einigung erzielt wurde. Die zuständigen Behörden treffen gemeinsam geeignete Maßnahmen

für die Annahme der erforderlichen Modalitäten oder Methoden bzw. der erforderlichen Pläne. Dies kann z. B. durch Ersuchen um Änderungen der Entwürfe gemäß diesem Absatz, durch Überarbeitung und Vervollständigung dieser Entwürfe oder, falls keine Entwürfe vorgelegt wurden, durch Festlegung und Genehmigung der erforderlichen Modalitäten, Methoden oder Pläne erfolgen.

Artikel 8 Einreichung von Vorschlägen bei den zuständigen Behörden

(1) Die ÜNB legen den jeweils zuständigen Behörden innerhalb der in den Artikeln 18, 23, 29, 33, 34, 35 und 37 festgelegten Fristen die Vorschläge für Modalitäten oder Methoden bzw. für Pläne zur Genehmigung vor. Die zuständigen Behörden können diese Fristen in Ausnahmefällen gemeinsam verlängern, insbesondere wenn eine Frist aufgrund von Umständen außerhalb des Verantwortungsbereichs der ÜNB oder der EU-VNBO nicht eingehalten werden kann.

(2) Vorschläge für Modalitäten, Methoden oder bzw. Pläne gemäß Absatz 1 werden zeitgleich mit der Übermittlung an die zuständigen Behörden auch der ACER zur Information vorgelegt.

(3) Auf gemeinsames Ersuchen der NRB gibt die ACER innerhalb von sechs Monaten nach Eingang des Vorschlags für Modalitäten oder Methoden oder für die Pläne eine Stellungnahme zu dem Vorschlag ab und übermittelt sie den NRB und den zuständigen Behörden. Die NRB, die CS-NCA und alle anderen als zuständige Behörden benannten Behörden stimmen sich untereinander ab, bevor die NRB die ACER um eine Stellungnahme ersuchen. Die ACER kann in dieser Stellungnahme Empfehlungen abgeben. Die ACER konsultiert die ENISA, bevor sie eine Stellungnahme zu den in Artikel 6 Absatz 2 aufgeführten Vorschlägen abgibt.

(4) Die zuständigen Behörden konsultieren einander, arbeiten eng zusammen und stimmen sich untereinander ab, um zu einer Einigung über die vorgeschlagenen Modalitäten, Methoden oder Pläne zu gelangen. Vor der Genehmigung der Modalitäten oder Methoden oder der Pläne überarbeiten und ergänzen sie die Vorschläge nach Konsultation von ENTSO-E und der EU-VNBO erforderlichenfalls, um sicherzustellen, dass die Vorschläge mit dieser Verordnung im Einklang stehen und zu einem hohen gemeinsamen Cybersicherheitsniveau in der gesamten Union beitragen.

(5) Die zuständigen Behörden entscheiden über die Modalitäten oder Methoden oder die Pläne innerhalb von sechs Monaten nach Eingang der Modalitäten oder Methoden bzw. der Pläne bei der jeweils zuständigen Behörde oder gegebenenfalls bei der

letzten betroffenen zuständigen Behörde.

(6) Gibt die ACER eine Stellungnahme ab, so tragen die jeweils zuständigen Behörden dieser Stellungnahme Rechnung und treffen ihre Entscheidungen innerhalb von sechs Monaten nach Eingang der Stellungnahme.

(7) Verlangen die zuständigen Behörden für ihre Genehmigung gemeinsam eine Änderung der vorgeschlagenen Modalitäten oder Methoden oder der Pläne, so entwickeln die ÜNB in Zusammenarbeit mit der EU-VNBO einen Vorschlag für eine solche Änderung der Modalitäten oder Methoden bzw. der Pläne. Die ÜNB legen den zuständigen Behörden den geänderten Vorschlag innerhalb von zwei Monaten nach deren Aufforderung zur Genehmigung vor. Die zuständigen Behörden entscheiden über die geänderten Modalitäten oder Methoden oder Pläne innerhalb von zwei Monaten nach deren Vorlage.

(8) Konnten die zuständigen Behörden innerhalb der in Absatz 5 oder Absatz 7 genannten Frist keine Einigung erzielen, so unterrichten sie die Kommission. Die Kommission kann geeignete Maßnahmen ergreifen, um die Annahme der erforderlichen Modalitäten, Methoden oder Pläne zu ermöglichen.

(9) Die ÜNB veröffentlichen mit Unterstützung von ENTSO-E und der EU-VNBO die Modalitäten oder Methoden oder die Pläne nach der Genehmigung durch die jeweils zuständigen Behörden auf ihren Websites, soweit diese Informationen nicht gemäß Artikel 47 als vertraulich betrachtet werden.

(10) Die zuständigen Behörden können von den ÜNB und der EU-VNBO gemeinsam Vorschläge für Änderungen der genehmigten Modalitäten oder Methoden oder der genehmigten Pläne anfordern und eine Frist für die Einreichung dieser Vorschläge festlegen. Die ÜNB können den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auch auf eigene Initiative Änderungen vorschlagen. Die Vorschläge zur Änderung der Modalitäten oder Methoden bzw. zur Änderung der Pläne werden nach dem Verfahren dieses Artikels entwickelt und genehmigt.

(11) Mindestens alle drei Jahre nach der ersten Annahme der jeweiligen Modalitäten oder Methoden bzw. der Annahme der jeweiligen Pläne überprüfen die ÜNB in Zusammenarbeit mit der EU-VNBO die Wirksamkeit der angenommenen Modalitäten oder Methoden bzw. der angenommenen Pläne und teilen den zuständigen Behörden und der ACER die Ergebnisse der Überprüfung unverzüglich mit.

Artikel 9 Konsultationen

(1) Die ÜNB konsultieren mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO die Interessenträger, einschließlich der ACER, der ENISA und der zuständigen Behörde jedes Mitgliedstaats, zu den Entwürfen von Vorschlägen für die in Artikel 6 Absatz 2 genannten Modalitäten oder Methoden und für die in Artikel 6 Absatz 3 genannten Pläne. Die Konsultation dauert mindestens einen Monat.

(2) Die in Artikel 6 Absatz 2 genannten Vorschläge für Modalitäten oder Methoden, die von den ÜNB in Zusammenarbeit mit der EU-VNBO vorgelegt wurden, werden veröffentlicht und auf Unionsebene einer Konsultation unterzogen. Die von den relevanten ÜNB in Zusammenarbeit mit der EU-VNBO auf regionaler Ebene vorgelegten Vorschläge für Pläne gemäß Artikel 6 Absatz 3 werden mindestens auf regionaler Ebene einer Konsultation unterzogen.

(3) Die ÜNB, unterstützt von ENTSO-E, und die für den Vorschlag für Modalitäten, Methoden oder Pläne zuständige EU-VNBO tragen den in den gemäß Absatz 1 durchgeführten Konsultationen geäußerten Ansichten der Interessenträger, gebührend Rechnung, bevor sie die Vorschläge zur regulatorischen Genehmigung vorlegen. In allen Fällen ist zusammen mit dem Vorschlag eine fundierte Begründung vorzulegen, weshalb die aus der Konsultation hervorgegangenen Stellungnahmen berücksichtigt bzw. nicht berücksichtigt wurden, und rechtzeitig — vor oder gleichzeitig mit dem Vorschlag für Modalitäten oder Methoden — zu veröffentlichen.

Artikel 10 Einbeziehung der Interessenträger

Die ACER organisiert in enger Zusammenarbeit mit ENTSO-E und der EU-VNBO die Einbeziehung der Interessenträger, einschließlich regelmäßiger Treffen mit Interessenträgern, um Probleme zu ermitteln und Verbesserungen im Zusammenhang mit der Durchführung dieser Verordnung vorzuschlagen.

Artikel 11 Kostenerstattung

(1) Die Kosten, die aufgrund der Verpflichtungen aus dieser Verordnung bei ÜNB und VNB anfallen, die der Netzentgeltregulierung unterliegen, einschließlich der Kosten von ENTSO-E und der EU-VNBO, werden von der zuständigen NRB jedes Mitgliedstaats geprüft.

(2) Als angemessen, effizient und verhältnismäßig bewertete Kosten werden durch Netzentgelte oder andere geeignete Mechanismen gedeckt, die von der zuständigen

NRB festgelegt werden.

(3) Auf Verlangen der zuständigen NRB stellen die in Absatz 1 genannten ÜNB und VNB innerhalb einer von der NRB festgelegten angemessenen Frist die erforderlichen Informationen bereit, um die Prüfung der entstandenen Kosten zu erleichtern.

Artikel 12 Überwachung

(1) Die ACER überwacht die Durchführung dieser Verordnung gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2019/943 und Artikel 4 Absatz 2 der Verordnung (EU) 2019/942. Bei der Durchführung der Überwachung kann die ACER mit der ENISA zusammenarbeiten und ENTSO-E und die EU-VNBO um Unterstützung ersuchen. Die ACER unterrichtet die Koordinierungsgruppe „Strom“ und die NIS-Kooperationsgruppe regelmäßig über die Durchführung dieser Verordnung.

(2) Die ACER veröffentlicht nach dem Inkrafttreten dieser Verordnung mindestens alle drei Jahre einen Bericht, um

a) den Stand der Umsetzung der anwendbaren Risikomanagementmaßnahmen im Bereich der Cybersicherheit durch Einrichtungen mit erheblichen Auswirkungen und Einrichtungen mit kritischen Auswirkungen zu überprüfen;

b) zu ermitteln, ob zur Prävention von Risiken für den Elektrizitätssektor zusätzliche Vorschriften über gemeinsame Anforderungen, Planung, Beobachtung, Berichterstattung und Krisenbewältigung erforderlich sein könnten, und

c) Verbesserungsbedarf für die Überarbeitung dieser Verordnung zu bestimmen oder nicht abgedeckte Bereiche und neue Prioritäten zu ermitteln, die sich aufgrund technischer Entwicklungen ergeben können.

(3) Bis zum 13 Juni 2025 kann die ACER in Zusammenarbeit mit der ENISA und nach Konsultation von ENTSO-E und der EU-VNBO auf der Grundlage der gemäß Absatz 5 festgelegten Leistungsindikatoren Leitlinien zu den relevanten Informationen, die der ACER zu Überwachungszwecken zu übermitteln sind, sowie zu dem Verfahren und der Häufigkeit der Einholung der Informationen vorlegen.

(4) Die zuständigen Behörden können Zugang zu den einschlägigen Informationen erhalten, die sich im Besitz der ACER befinden und gemäß diesem Artikel erhoben wurden.

(5) Die ACER legt in Zusammenarbeit mit der ENISA und mit Unterstützung von ENTSO-E und der EU-VNBO in Bezug auf Cybersicherheitsaspekte grenzüberschreitender Stromflüsse unverbindliche Leistungsindikatoren für die Bewertung der be-

trieblichen Zuverlässigkeit vor.

(6) Die in Artikel 2 Absatz 1 dieser Verordnung aufgeführten Einrichtungen übermitteln der ACER die Informationen, die diese zur Wahrnehmung der in Absatz 2 genannten Aufgaben benötigt.

Artikel 13 Benchmarking

(1) Bis zum 13 Juni 2025 erstellt die ACER in Zusammenarbeit mit der ENISA einen unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit. In dem Leitfaden für die NRB werden die Grundsätze des Benchmarkings der durchgeführten Cybersicherheitskontrollen gemäß Absatz 2 erläutert, wobei die Kosten für die Durchführung der Kontrollen und die Wirksamkeit von Prozessen, Produkten, Diensten, Systemen und Lösungen, die zur Durchführung dieser Kontrollen genutzt werden, zu berücksichtigen sind. Die ACER berücksichtigt bei der Erstellung des unverbindlichen Leitfadens für das Benchmarking im Bereich der Cybersicherheit vorhandene Benchmarking-Berichte. Die ACER übermittelt den unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit den NRB zur Information.

(2) Innerhalb von 12 Monaten nach Erstellung des Benchmarking-Leitfadens gemäß Absatz 1 führen die NRB eine Benchmarking-Analyse durch, um zu bewerten, ob die aktuellen Investitionen in die Cybersicherheit

a) Risiken mit Auswirkungen auf grenzüberschreitende Stromflüsse mindern;

b) zu den gewünschten Ergebnissen führen und die Effizienz bei der Entwicklung des Elektrizitätssystems verbessern;

c) effizient sind und in die allgemeine Auftragsvergabe für Vermögenswerte und Dienstleistungen integriert werden.

(3) Bei der Benchmarking-Analyse können die NRB den von der ACER erstellten unverbindlichen Leitfaden für das Benchmarking im Bereich der Cybersicherheit berücksichtigen, wobei sie insbesondere Folgendes bewerten:

a) die durchschnittlichen Ausgaben für die Cybersicherheit zur Minderung von Risiken, die sich auf grenzüberschreitende Stromflüsse auswirken, insbesondere bei Einrichtungen mit erheblichen oder kritischen Auswirkungen;

b) in Zusammenarbeit mit ENTSO-E und der EU-VNBO die Durchschnittspreise für Cybersicherheitsdienste, -systeme und -produkte, die in hohem Maß zur Verbesserung und Aufrechterhaltung der Risikomanagementmaßnahmen im

Bereich der Cybersicherheit in den verschiedenen Netzbetriebsregionen beitragen;

c) das Vorhandensein von Cybersicherheitsdiensten, -systemen und -lösungen, die sich für die Durchführung dieser Verordnung eignen, sowie die Vergleichbarkeit der damit verbundenen Kosten und Funktionen, wobei sie mögliche Maßnahmen ermitteln, die zur Verbesserung der Effizienz der Ausgaben erforderlich sind, insbesondere wenn Investitionen in die Cybersicherheitstechnik erforderlich sein könnten.

(4) Alle Informationen zu Benchmarking-Analysen werden gemäß den Anforderungen dieser Verordnung an die Datenklassifizierung, die Mindest-Cybersicherheitskontrollen und den Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gehandhabt und verarbeitet. Die in den Absätzen 2 und 3 genannte Benchmarking-Analyse wird nicht veröffentlicht.

(5) Unbeschadet der Vertraulichkeitsbestimmungen in Artikel 47 und der Notwendigkeit, die Sicherheit von Einrichtungen zu schützen, die den Bestimmungen dieser Verordnung unterliegen, wird die in den Absätzen 2 und 3 dieses Artikels genannte Benchmarking-Analyse allen NRB, allen zuständigen Behörden, der ACER, der ENISA und der Kommission übermittelt.

Artikel 14 Vereinbarungen mit ÜNB von Drittländern

(1) Innerhalb von 18 Monaten nach dem Inkrafttreten dieser Verordnung bemühen sich die ÜNB einer Netzbetriebsregion, die an ein Drittland angrenzt, um den Abschluss von Vereinbarungen mit ÜNB des benachbarten Drittlands, die mit dem einschlägigen Unionsrecht im Einklang stehen, die Grundlage für die Zusammenarbeit zum Cybersicherheitsschutz bilden und Regelungen für die Zusammenarbeit mit diesen ÜNB im Bereich der Cybersicherheit enthalten.

(2) Die ÜNB unterrichten die zuständige Behörde über die gemäß Absatz 1 geschlossenen Vereinbarungen.

Artikel 15 Gesetzlicher Vertreter

(1) Einrichtungen, die keine Niederlassung in der Union haben, aber Dienstleistungen für Einrichtungen in der Union erbringen und gemäß Artikel 24 Absatz 6 über ihren Status als Einrichtungen mit erheblichen oder kritischen Auswirkungen unterrichtet wurden, benennen innerhalb von drei Monaten nach der Unterrichtung schriftlich ei-

nen Vertreter in der Union und informieren die zuständige Behörde entsprechend.

(2) Dieser Vertreter wird beauftragt, zusätzlich zu oder anstelle der Einrichtung mit erheblichen oder kritischen Auswirkungen als Ansprechpartner zu fungieren, an den sich jede zuständige Behörde und jedes CSIRT in der Union in Bezug auf die Verpflichtungen der Einrichtung aus dieser Verordnung wenden kann. Die Einrichtung mit erheblichen oder kritischen Auswirkungen stattet ihren gesetzlichen Vertreter mit den erforderlichen Befugnissen und ausreichenden Ressourcen aus, um eine effiziente und rechtzeitige Zusammenarbeit mit den jeweils zuständigen Behörden oder CSIRTs zu gewährleisten.

(3) Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Einrichtung ihre Dienste anbietet. Die Einrichtung gilt als der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegend, in dem der Vertreter niedergelassen ist. Einrichtungen mit erheblichen oder kritischen Auswirkungen melden der zuständigen Behörde des Mitgliedstaats, in dem ihr gesetzlicher Vertreter ansässig oder niedergelassen ist, den Namen, die Postanschrift, die E-Mail-Adresse und die Telefonnummer des gesetzlichen Vertreters.

(4) Der benannte gesetzliche Vertreter kann für Verstöße gegen Pflichten aus dieser Verordnung haftbar gemacht werden; dies berührt nicht die Haftung und die rechtlichen Schritte, die gegen die Einrichtung mit erheblichen oder kritischen Auswirkungen eingeleitet werden können.

(5) Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienstleistungen erbringt, gegen die Einrichtung rechtliche Schritte wegen Verstößen gegen Pflichten aus dieser Verordnung einleiten.

(6) Die Benennung eines gesetzlichen Vertreters in der Union gemäß Absatz 1 gilt nicht als Niederlassung in der Union.

Artikel 16 Zusammenarbeit zwischen ENTSO-E und der EU-VNBO

(1) ENTSO-E und die EU-VNBO arbeiten bei der Durchführung der Bewertungen des Cybersicherheitsrisikos gemäß Artikel 19 und Artikel 21 zusammen, insbesondere bei den folgenden Aufgaben:

a) Entwicklung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 18 Absatz 1;

b) Erstellung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23;

c) Entwicklung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor gemäß Kapitel III;

d) Erstellung der Empfehlung für die Cybersicherheit bei der Auftragsvergabe gemäß Artikel 35;

e) Entwicklung der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8;

f) Entwicklung des vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (ECII) gemäß Artikel 48 Absatz 1 Buchstabe a;

g) Erstellung der konsolidierten vorläufigen Liste der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 3;

h) Erstellung der vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Artikel 48 Absatz 4;

i) Erstellung der vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Artikel 48 Absatz 6;

j) Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos gemäß Artikel 19;

k) Durchführung der regionalen Bewertung des Cybersicherheitsrisikos gemäß Artikel 21;

l) Festlegung der regionalen Pläne zur Minderung des Cybersicherheitsrisikos gemäß Artikel 22;

m) Entwicklung von Leitlinien für europäische Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen gemäß Artikel 36;

n) Entwicklung von Leitlinien für die Durchführung dieser Verordnung, in Absprache mit der ACER und der ENISA.

(2) Die Zusammenarbeit zwischen ENTSO-E und der EU-VNBO kann über eine Arbeitsgruppe für Cybersicherheitsrisiken erfolgen.

(3) ENTSO-E und die EU-VNBO unterrichten die ACER, die ENISA, die NIS-Kooperationsgruppe und die Koordinierungsgruppe „Strom“ regelmäßig über die Fortschritte bei der Umsetzung der unionsweiten und regionalen Bewertung des Cy-

bersicherheitsrisikos gemäß Artikel 19 und Artikel 21.

Artikel 17 Zusammenarbeit zwischen der ACER und den zuständigen Behörden

Die ACER überwacht in Zusammenarbeit mit jeder zuständigen Behörde
(1) die Umsetzung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit gemäß Artikel 12 Absatz 2 Buchstabe a und der Berichterstattungspflichten gemäß den Artikeln 27 und 39 sowie
(2) das Verfahren zur Annahme der Modalitäten, Methoden oder Pläne gemäß Artikel 6 Absätze 2 und 3 und deren Umsetzung. Die Zusammenarbeit zwischen der ACER, der ENISA und jeder zuständigen Behörde kann über ein Gremium zur Überwachung von Cybersicherheitsrisiken erfolgen.

Kapitel II – Risikobewertung und Ermittlung der relevanten Cybersicherheitsrisiken

Artikel 18 Methoden zur Bewertung des Cybersicherheitsrisikos

(1) Bis zum 13 März 2025 legen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und nach Konsultation der NIS-Kooperationsgruppe einen Vorschlag für die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten vor.
(2) Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen Folgendes umfassen:

a) eine Liste der zu berücksichtigenden Cyberbedrohungen, einschließlich mindestens der folgenden Bedrohungen der Lieferkette:
   i) schwere und unerwartete Kompromittierung der Lieferkette;
   ii) Nichtverfügbarkeit von IKT-Produkten, -Diensten oder -Prozessen aus der Lieferkette;
   iii) von Akteuren in der Lieferkette ausgelöste Cyberangriffe;
   iv) Weitergabe sensibler Informationen durch die Lieferkette, einschließlich der Nachverfolgung der Lieferkette;

v) Einführung von Schwachstellen oder Hintertüren in IKT-Produkten, -Diensten oder -Prozessen durch Akteure in der Lieferkette;

b) die Kriterien für die Einstufung der Auswirkungen von Cybersicherheitsrisiken als erheblich oder kritisch, wobei festgelegte Schwellenwerte für deren Folgen und Wahrscheinlichkeit zu nutzen sind;

c) einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus Altsystemen, den Kaskadeneffekten von Cyberangriffen und dem Echtzeitcharakter der Netzbetriebssysteme ergeben;

d) einen Ansatz zur Analyse der Cybersicherheitsrisiken, die sich aus der Abhängigkeit von einem einzigen Anbieter von IKT-Produkten, -Diensten oder -Prozessen ergeben.

(3) Die Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf der Ebene der Mitgliedstaaten müssen dieselbe Risiko-Auswirkungs-Matrix umfassen. Mit der Risiko-Auswirkungs-Matrix

a) werden die Folgen von Cyberangriffen anhand folgender Kriterien gemessen:

i) Lastverlust;

ii) Verringerung der Stromerzeugung;

iii) Kapazitätsverlust in der primären Frequenzreserve;

iv) Verlust von Kapazitäten für die Wiederherstellung des Betriebs eines Stromnetzes ohne Rückgriff auf das externe Übertragungsnetz nach einer vollständigen oder teilweisen Abschaltung („Schwarzstart“);

v) voraussichtliche Dauer eines Stromausfalls mit Auswirkungen auf die Kunden in Verbindung mit dem Ausmaß des Ausfalls (nach Zahl der Kunden) und

vi) alle sonstigen quantitativen oder qualitativen Kriterien, die als sinnvolle Indikatoren für die Auswirkungen eines Cyberangriffs auf grenzüberschreitende Stromflüsse dienen könnten;

b) wird die Wahrscheinlichkeit eines Vorfalls als Häufigkeit der Cyberangriffe pro Jahr gemessen.

(4) In den Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene wird beschrieben, wie die ECII-Schwellenwerte für erhebliche und kritische Auswirkungen bestimmt werden. Der ECII muss es den Einrichtungen ermöglichen, im

Rahmen der von ihnen gemäß Artikel 26 Absatz 4 Buchstabe c Ziffer i durchgeführten Folgenabschätzungen die Auswirkungen der Risiken auf ihre Geschäftsprozesse mithilfe der in Absatz 2 Buchstabe b genannten Kriterien abzuschätzen.

(5) ENTSO-E unterrichtet die Koordinierungsgruppe „Strom“ in Abstimmung mit der EU-VNBO über die Vorschläge für die gemäß Absatz 1 zu entwickelnden Methoden zur Bewertung des Cybersicherheitsrisikos.

Artikel 19 Unionsweite Bewertung des Cybersicherheitsrisikos

(1) Innerhalb von neun Monaten nach der Genehmigung der Methoden zur Bewertung des Cybersicherheitsrisikos gemäß Artikel 8 und danach alle drei Jahre führt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe unbeschadet des Artikels 22 der Richtlinie (EU) 2022/2555 eine unionsweite Bewertung des Cybersicherheitsrisikos durch und erstellt einen Entwurf eines Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos. Dabei wenden sie die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden an, um die möglichen Folgen von Cyberangriffen, die sich auf die Betriebssicherheit des Elektrizitätssystems auswirken und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der unionsweiten Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

(2) Der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos muss Folgendes enthalten:

a) die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen;

b) eine Risiko-Auswirkungs-Matrix, die Einrichtungen und die zuständigen Behörden nutzen müssen, um die Cybersicherheitsrisiken zu bewerten, die in der Bewertung des Cybersicherheitsrisikos auf der Ebene der Mitgliedstaaten gemäß Artikel 20 und in der Bewertung des Cybersicherheitsrisikos auf der Ebene von Einrichtungen gemäß Artikel 26 Absatz 2 Buchstabe b ermittelt wurden.

(3) In Bezug auf die unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen muss der Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos Folgendes enthalten:

a) eine Bewertung der möglichen Folgen eines Cyberangriffs anhand der Parameter, die in der gemäß Artikel 18 Absätze 2, 3 und 4 entwickelten und

gemäß Artikel 8 genehmigten Methode zur Bewertung des Cybersicherheitsrisikos festgelegt sind;

b) den ECII und die Schwellenwerte für erhebliche und kritische Auswirkungen, die die zuständigen Behörden gemäß Artikel 24 Absätze 1 und 2 nutzen müssen, um Einrichtungen mit erheblichen oder kritischen Auswirkungen zu ermitteln, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind.

(4) ENTSO-E legt der ACER in Zusammenarbeit mit der EU-VNBO den Entwurf des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos mit den Ergebnissen der unionsweiten Bewertung des Cybersicherheitsrisikos zur Stellungnahme vor. Die ACER gibt innerhalb von drei Monaten nach Eingang eine Stellungnahme zu dem Entwurf des Berichts ab. ENTSO-E und die EU-VNBO tragen der Stellungnahme der ACER bei der Fertigstellung dieses Berichts so weit wie möglich Rechnung.

(5) Innerhalb von drei Monaten nach Eingang der Stellungnahme der ACER übermittelt ENTSO-E in Zusammenarbeit mit der EU-VNBO der ACER, der Kommission, der ENISA und den zuständigen Behörden den endgültigen Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos.

Artikel 20 Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten

(1) Jede zuständige Behörde führt in Bezug auf alle Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat eine Bewertung des Cybersicherheitsrisikos des Mitgliedstaats durch und nutzt dabei die gemäß Artikel 18 entwickelten und gemäß Artikel 8 genehmigten Methoden. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die Risiken von Cyberangriffen ermittelt und analysiert, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören. Bei der Bewertung des Cybersicherheitsrisikos der Mitgliedstaaten werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

(2) Innerhalb von 21 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermittelt jede zuständige Behörde mit Unterstützung des CSIRT und nach Konsultation der für Elektrizität zuständigen CS-NCA dem ENTSO-E und der EU-VNBO einen Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats, der in Bezug auf jeden Geschäftsprozess mit erheblichen oder kritischen

Auswirkungen folgende Informationen enthält:

a) den Stand der Umsetzung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskorntrollen gemäß Artikel 29;

b) eine Liste aller in den letzten drei Jahren gemäß Artikel 38 Absatz 3 gemeldeten Cyberangriffe;

c) eine Zusammenfassung aller in den letzten drei Jahren gemäß Artikel 38 Absatz 6 gemeldeten Informationen zu Cyberbedrohungen;

d) für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung der mit einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten verbundenen Risiken;

e) erforderlichenfalls eine Liste zusätzlicher Einrichtungen, die gemäß Artikel 24 Absätze 1, 2, 3 und 5 als Einrichtungen mit erheblichen oder kritischen Auswirkungen ermittelt wurden.

(3) Der Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats muss dem gemäß Artikel 10 der Verordnung (EU) 2019/941 erstellten Risikovorsorgeplan des Mitgliedstaats Rechnung tragen.

(4) Die Informationen in dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats gemäß Absatz 2 Buchstaben a bis d dürfen nicht mit bestimmten Einrichtungen oder Vermögenswerten verknüpft sein. In dem Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats sind auch die Risiken im Zusammenhang mit den von den zuständigen Behörden der Mitgliedstaaten gemäß Artikel 30 gewährten befristeten Ausnahmen zu bewerten.

(5) ENTSO-E und die EU-VNBO können im Zusammenhang mit den in Unterabsatz 2 Buchstaben a und c genannten Aufgaben die zuständigen Behörden um zusätzliche Informationen ersuchen.

(6) Die zuständigen Behörden stellen sicher, dass die von ihnen bereitgestellten Informationen genau und zutreffend sind.

Artikel 21 Regionale Bewertungen des Cybersicherheitsrisikos

(1) ENTSO-E führt in Zusammenarbeit mit der EU-VNBO und in Absprache mit dem zuständigen regionalen Koordinierungszentrum für jede Netzbetriebsregion eine regionale Bewertung des Cybersicherheitsrisikos durch und nutzt dabei die gemäß Ar-

tikel 19 entwickelten und gemäß Artikel 8 genehmigten Methoden, um die Risiken von Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören, zu ermitteln, zu analysieren und zu bewerten. Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die mit Cyberangriffen verbundenen rechtlichen und finanziellen Schäden sowie Rufschädigungen nicht berücksichtigt.

(2) Innerhalb von 30 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen Bericht über die regionale Bewertung des Cybersicherheitsrisikos.

(3) Der Bericht über die regionale Bewertung des Cybersicherheitsrisikos muss den einschlägigen Informationen Rechnung tragen, die in den Berichten über die unionsweite Bewertung des Cybersicherheitsrisikos und in den Berichten der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos enthalten sind.

(4) Bei der regionalen Bewertung des Cybersicherheitsrisikos werden die gemäß Artikel 6 der Verordnung (EU) 2019/941 bestimmten regionalen Szenarien für Stromversorgungskrisen im Bereich der Cybersicherheit berücksichtigt.

Artikel 22 Regionale Pläne zur Minderung des Cybersicherheitsrisikos

(1) Innerhalb von 36 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6, spätestens jedoch am 13 Juni 2031, und danach alle drei Jahre erstellen die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit den regionalen Koordinierungszentren und der NIS-Kooperationsgruppe für jede Netzbetriebsregion einen regionalen Plan zur Minderung des Cybersicherheitsrisikos.

(2) Die regionalen Pläne zur Minderung des Cybersicherheitsrisikos müssen Folgendes enthalten:

a) die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen, die die Einrichtungen mit erheblichen bzw. kritischen Auswirkungen in der Netzbetriebsregion anwenden müssen;

b) die verbleibenden Cybersicherheitsrisiken in den Netzbetriebsregionen nach Anwendung der unter Buchstabe a genannten Kontrollen.

(3) ENTSO-E legt die regionalen Pläne zur Minderung des Cybersicherheitsrisikos

den relevanten Übertragungsnetzbetreibern, den zuständigen Behörden und der Koordinierungsgruppe „Strom“ vor. Die Koordinierungsgruppe „Strom“ kann Änderungen empfehlen.

(4) Die ÜNB aktualisieren mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe die regionalen Risikominderungspläne alle drei Jahre, soweit aufgrund der Umstände keine häufigere Aktualisierung erforderlich ist.

Artikel 23 Umfassender Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse

(1) Innerhalb von 40 Monaten nach Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre übermitteln die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der NIS-Kooperationsgruppe der Koordinierungsgruppe „Strom“ einen Bericht über die Ergebnisse der Bewertung der Cybersicherheitsrisiken in Bezug auf grenzüberschreitende Stromflüsse (im Folgenden „umfassender Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse“).

(2) Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse stützt sich auf den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos, die Berichte der Mitgliedstaaten über die Bewertung des Cybersicherheitsrisikos und die Berichte über die regionale Bewertung des Cybersicherheitsrisikos und muss folgende Informationen enthalten:

a) die Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 2 Buchstabe a ermittelt wurden, einschließlich der Schätzung der Wahrscheinlichkeit und der Auswirkungen von Cybersicherheitsrisiken, die in den Berichten über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 und Artikel 19 Absatz 3 Buchstabe a bewertet wurden;

b) aktuelle Cyberbedrohungen, insbesondere neu aufkommende Bedrohungen und Risiken für das Elektrizitätssystem;

c) Cyberangriffe im vorangegangenen Zeitraum auf Unionsebene mit einem kritischen Überblick darüber, wie sich diese Cyberangriffe auf grenzüberschreitende Stromflüsse ausgewirkt haben könnten;

d) allgemeiner Stand der Umsetzung der Cybersicherheitsmaßnahmen;

e) Stand der Umsetzung der Informationsflüsse gemäß den Artikeln 37 und 38;

f) Liste der Informationen oder spezifische Kriterien für die Klassifizierung von Informationen gemäß Artikel 46;

g) ermittelte und besonders zu beachtende Risiken, die sich aus einem unsicheren Lieferkettenmanagement ergeben können;

h) Ergebnisse der regionalen und überregionalen Cybersicherheitsübungen gemäß Artikel 44 und dabei insgesamt gewonnene Erfahrungen;

i) eine Analyse der Entwicklung des allgemeinen Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse seit den letzten regionalen Bewertungen des Cybersicherheitsrisikos;

j) alle sonstigen Informationen, die nützlich sein können, um mögliche Verbesserungen dieser Verordnung oder die Notwendigkeit einer Überarbeitung dieser Verordnung oder ihrer Instrumente zu ermitteln, sowie

k) aggregierte und anonymisierte Informationen über die gemäß Artikel 30 Absatz 3 gewährten Ausnahmen.

(3) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können zur Ausarbeitung des umfassenden Berichts über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse beitragen, wobei sie die Vertraulichkeit der Informationen gemäß Artikel 47 wahren müssen. Die ÜNB konsultieren diese Einrichtungen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO frühzeitig.

(4) Der umfassende Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse unterliegt den Bestimmungen des Artikels 46 über den Schutz ausgetauschter Informationen. Unbeschadet des Artikels 10 Absatz 4 und des Artikels 47 Absatz 4 veröffentlichen ENTSO-E und die EU-VNBO eine öffentliche Fassung dieses Berichts, die keine Informationen enthält, die den in Artikel 2 Absatz 1 aufgeführten Einrichtungen schaden können. Die öffentliche Fassung dieses Berichts wird nur mit Zustimmung der NIS-Kooperationsgruppe und der Koordinierungsgruppe „Strom“ veröffentlicht. ENTSO-E ist in Abstimmung mit der EU-VNBO für die Zusammenstellung und Veröffentlichung der öffentlichen Fassung des

Berichts verantwortlich.

Artikel 24 Ermittlung von Einrichtungen mit erheblichen oder kritischen Auswirkungen

(1) Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen, die im Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b enthalten sind, die Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat, die an unionsweiten Prozessen mit erheblichen bzw. kritischen Auswirkungen beteiligt sind. Die zuständigen Behörden können von einer Einrichtung in ihrem Mitgliedstaat Informationen anfordern, um die ECII-Werte für diese Einrichtung zu bestimmen. Liegt der ermittelte ECII einer Einrichtung über dem Schwellenwert für erhebliche oder kritische Auswirkungen, wird die ermittelte Einrichtung in dem in Artikel 20 Absatz 2 genannten Bericht über die Bewertung des Cybersicherheitsrisikos des Mitgliedstaats aufgeführt.

(2) Jede zuständige Behörde ermittelt anhand des ECII und der Schwellenwerte für erhebliche und kritische Auswirkungen aus dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 3 Buchstabe b die nicht in der Union niedergelassenen Einrichtungen mit erheblichen oder kritischen Auswirkungen, soweit sie in der Union tätig sind. Die zuständige Behörde kann von einer nicht in der Union niedergelassenen Einrichtung Informationen anfordern, um die ECII-Werte für die Einrichtung zu bestimmen.

(3) Jede zuständige Behörde kann weitere Einrichtungen in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen einstufen, wenn die folgenden Kriterien erfüllt sind:

a) Die Einrichtung ist Teil einer Gruppe von Einrichtungen, für die ein erhebliches Risiko besteht, dass sie zeitgleich Ziel eines Cyberangriffs sein könnten;

b) der über die Gruppe von Einrichtungen aggregierte ECII liegt über dem Schwellenwert für erhebliche oder kritische Auswirkungen.

(4) Ermittelt eine zuständige Behörde gemäß Absatz 3 zusätzliche Einrichtungen, so gelten alle Prozesse dieser Einrichtungen, deren über die Gruppe aggregierter ECII über dem Schwellenwert für erhebliche Auswirkungen liegt, als Prozesse mit erheblichen Auswirkungen, und alle Prozesse, deren über die Gruppe aggregierter ECII

über den Schwellenwerten für kritische Auswirkungen liegt, gelten als Prozesse mit kritischen Auswirkungen.

(5) Ermittelt eine zuständige Behörde Einrichtungen gemäß Absatz 3 Buchstabe a in mehr als einem Mitgliedstaat, so unterrichtet sie die anderen zuständigen Behörden, ENTSO-E und die EU-VNBO. ENTSO-E übermittelt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO auf der Grundlage der von allen zuständigen Behörden übermittelten Informationen eine Analyse der Aggregierung von Einrichtungen in mehr als einem Mitgliedstaat, die zu einer von verschiedenen Punkten ausgehenden Störung der grenzüberschreitenden Stromflüsse führen und einen Cyberangriff nach sich ziehen können. Wird eine Gruppe von Einrichtungen in mehreren Mitgliedstaaten als Aggregierung ermittelt, deren ECII über dem Schwellenwert für erhebliche oder kritische Auswirkungen liegt, so stufen alle betroffenen zuständigen Behörden die Einrichtungen in dieser Gruppe für ihren jeweiligen Mitgliedstaat auf der Grundlage des aggregierten ECII für die Gruppe der Einrichtungen als Einrichtungen mit erheblichen bzw. kritischen Auswirkungen ein, und die ermittelten Einrichtungen werden in den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos aufgenommen.

(6) Jede zuständige Behörde unterrichtet innerhalb von neun Monaten, nachdem ENTSO-E und die EU-VNBO den Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 übermittelt haben, spätestens jedoch bis zum 13 Juni 2028, die in der Liste aufgeführten Einrichtungen, dass sie in ihrem Mitgliedstaat als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

(7) Wird einer zuständigen Behörde ein Diensteanbieter als Anbieter kritischer IKT-Dienste gemäß Artikel 27 Buchstabe c gemeldet, so teilt sie dies den zuständigen Behörden der Mitgliedstaaten mit, in deren Hoheitsgebiet sich der Sitz oder der Vertreter befindet. Die letztgenannte zuständige Behörde teilt dem Diensteanbieter mit, dass er als Anbieter kritischer Dienste eingestuft wurde.

Artikel 25 Nationale Überprüfungssysteme

(1) Die zuständigen Behörden können ein nationales Überprüfungssystem einrichten, um zu überprüfen, ob die gemäß Artikel 24 Absatz 1 ermittelten Einrichtungen mit kritischen Auswirkungen den nationalen Rechtsrahmen umgesetzt haben, der in der Vergleichsmatrix gemäß Artikel 34 aufgeführt ist. Das nationale Überprüfungssystem

kann sich auf eine von der zuständigen Behörde durchgeführte Inspektion, unabhängige Sicherheitsaudits oder gegenseitige Peer Reviews durch Einrichtungen mit kritischen Auswirkungen in demselben Mitgliedstaat, die von der zuständigen Behörde beaufsichtigt werden, stützen.

(2) Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so stellt sie sicher, dass die Überprüfung nach den folgenden Anforderungen durchgeführt wird:

a) Jede Partei, die die Peer Review, das Audit oder die Inspektion durchführt, muss von der zu überprüfenden Einrichtung mit kritischen Auswirkungen unabhängig sein und darf sich nicht in einem Interessenkonflikt befinden;

b) das Personal, das die Peer Reviews, Audits oder Inspektionen durchführt, muss nachweislich Kenntnisse haben über

   i) die Cybersicherheit im Elektrizitätssektor;

   ii) Cybersicherheitsmanagementsysteme;

   iii) Audit-Grundsätze;

   iv) die Bewertung von Cybersicherheitsrisiken;

   v) den gemeinsamen Rahmen für die Cybersicherheit im Elektrizitätssektor;

   vi) den nationalen Rechts- und Verwaltungsrahmen sowie europäische und internationale Normen, die für die Überprüfung relevant sind;

   vii) die Prozesse mit kritischen Auswirkungen, die Gegenstand der Überprüfung sind;

c) die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, erhält ausreichend Zeit für die Durchführung dieser Tätigkeiten;

d) die Partei, die die Peer Reviews, Audits oder Inspektionen durchführt, ergreift geeignete Maßnahmen, um die bei der Überprüfung erhobenen Informationen im Einklang mit ihrem Vertraulichkeitsgrad zu schützen, und

e) Peer Reviews, Audits oder Inspektionen werden mindestens einmal jährlich durchgeführt und umfassen mindestens alle drei Jahre den gesamten Prüfumfang.

(3) Beschließt eine zuständige Behörde, ein nationales Überprüfungssystem einzurichten, so teilt sie der ACER jährlich mit, wie oft sie Inspektionen im Rahmen dieses

Systems durchgeführt hat.

Artikel 26 Cybersicherheitsrisikomanagement auf Ebene der Einrichtungen

(1) Jede von den zuständigen Behörden gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit erheblichen oder kritischen Auswirkungen führt das Cybersicherheitsrisikomanagement für alle ihre Vermögenswerte in ihren Perimetern mit erheblichen oder kritischen Auswirkungen durch. Jede Einrichtung mit erheblichen oder kritischen Auswirkungen führt alle drei Jahre ein Risikomanagement durch, das die in Absatz 2 genannten Phasen umfasst.

(2) Jede Einrichtung mit erheblichen oder kritischen Auswirkungen stützt ihr Cybersicherheitsrisikomanagement auf einen Ansatz, der auf den Schutz ihrer Netz- und Informationssysteme abzielt und folgende Phasen umfasst:

a) Bestimmung des Kontexts;

b) Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung;

c) Behandlung von Cybersicherheitsrisiken;

d) Akzeptanz von Cybersicherheitsrisiken.

(3) Bei der Bestimmung des Kontexts trifft jede Einrichtung mit erheblichen oder kritischen Auswirkungen folgende Maßnahmen:

a) Festlegung des Umfangs der Bewertung des Cybersicherheitsrisikos, einschließlich der von ENTSO-E und der EU-VNBO ermittelten Prozesse mit erheblichen oder kritischen Auswirkungen sowie anderer Prozesse, die Ziel von Cyberangriffen mit erheblichen oder kritischen Auswirkungen auf grenzüberschreitende Stromflüsse sein können, und

b) Festlegung der Kriterien für die Risikobewertung und die Risikoakzeptanz im Einklang mit der Risiko-Auswirkungs-Matrix, die Einrichtungen und die zuständigen Behörden nach den von ENTSO-E und der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten nutzen müssen, um Cybersicherheitsrisiken zu bewerten.

(4) Bei der Bewertung des Cybersicherheitsrisikos muss jede Einrichtung mit erheblichen oder kritischen Auswirkungen

a) Cybersicherheitsrisiken unter Berücksichtigung folgender Aspekte ermitteln:

i) aller Vermögenswerte, die unionsweite Prozesse mit erheblichen oder kritischen Auswirkungen unterstützen, wobei die möglichen Auswirkungen auf grenzüberschreitende Stromflüsse für den Fall einer Kompromittierung des Vermögenswerts zu bewerten sind;

ii) möglicher Cyberbedrohungen unter Berücksichtigung der Cyberbedrohungen, die im jüngsten umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 ermittelt wurden, sowie Bedrohungen der Lieferkette;

iii) Schwachstellen, einschließlich Schwachstellen in Altsystemen;

iv) möglicher Szenarien von Cyberangriffen, einschließlich Cyberangriffen, die die Betriebssicherheit des Elektrizitätssystems beeinträchtigen und grenzüberschreitende Stromflüsse stören;

v) einschlägiger Risikobeurteilungen und -bewertungen auf Unionsebene, einschließlich koordinierter Risikobewertungen kritischer Lieferketten gemäß Artikel 22 der Richtlinie (EU) 2022/2555, und

vi) bestehender umgesetzter Kontrollen;

b) die Wahrscheinlichkeit und Folgen der unter Buchstabe a genannten Cybersicherheitsrisiken analysieren und das Ausmaß des Cybersicherheitsrisikos anhand der Risiko-Auswirkungs-Matrix bestimmen, die in den von den ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO gemäß Artikel 19 Absatz 2 entwickelten Methoden zur Bewertung des Cybersicherheitsrisikos auf Unionsebene, auf regionaler Ebene und auf Ebene der Mitgliedstaaten genutzt wird, um Cybersicherheitsrisiken zu bewerten;

c) Vermögenswerte nach den möglichen Folgen einer Beeinträchtigung der Cybersicherheit klassifizieren und Perimeter mit erheblichen oder kritischen Auswirkungen wie folgt ermitteln:

i) Durchführung einer Folgenabschätzung für Geschäftsprozesse anhand des ECII für alle Prozesse, die Gegenstand der Bewertung des Cybersicherheitsrisikos sind;

ii) Einstufung eines Prozesses als Prozess mit erheblichen oder kritischen Auswirkungen, wenn sein ECII über dem Schwellenwert für erhebliche bzw. kritische Auswirkungen liegt;

iii) Bestimmung aller Vermögenswerte mit erheblichen oder kritischen Auswirkungen als die Vermögenswerte, die für Prozesse mit erheblichen bzw. kritischen Auswirkungen erforderlich sind;

iv) Bestimmung der Perimeter mit erheblichen oder kritischen Auswirkungen als Perimeter, die alle Vermögenswerte mit erheblichen bzw. kritischen Auswirkungen umfassen, damit der Zugang zu diesen Perimetern kontrolliert werden kann;

d) Cybersicherheitsrisiken durch Priorisierung anhand von Risikobewertungs- und Risikoakzeptanzkriterien gemäß Absatz 3 Buchstabe b beurteilen.

(5) Bei der Behandlung des Cybersicherheitsrisikos erstellt jede Einrichtung mit erheblichen oder kritischen Auswirkungen einen Risikominderungsplan auf Ebene der Einrichtung, wobei sie geeignete Optionen für die Behandlung des Risikos wählt, um die Risiken zu bewältigen und das Restrisiko zu bestimmen.

(6) Bei der Akzeptanz von Cybersicherheitsrisiken entscheidet jede Einrichtung mit erheblichen oder kritischen Auswirkungen auf der Grundlage der in Absatz 3 Buchstabe b festgelegten Risikoakzeptanzkriterien, ob sie das Restrisiko akzeptiert.

(7) Jede Einrichtung mit erheblichen oder kritischen Auswirkungen erfasst die in Absatz 1 genannten Vermögenswerte in einem Vermögensinventar. Dieses Vermögensinventar ist nicht Teil des Berichts über die Risikobewertung.

(8) Die zuständige Behörde kann die im Vermögensinventar enthaltenen Vermögenswerte während der Inspektionen einsehen.

Artikel 27 Berichterstattung über die Risikobewertung auf Ebene der Einrichtung

Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre legt jede Einrichtung mit erheblichen oder kritischen Auswirkungen der zuständigen Behörde einen Bericht vor, der folgende Informationen enthält:

1. eine Liste der für den Risikominderungsplan auf Ebene der Einrichtung gemäß Artikel 26 Absatz 5 ausgewählten Kontrollen mit dem aktuellen Stand der Umsetzung jeder Kontrolle;

2. für jeden unionsweiten Prozess mit erheblichen oder kritischen Auswirkungen eine Schätzung des Risikos einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögens-

werten. Die Schätzung dieses Risikos ist im Einklang mit der Risiko-Auswirkungs-Matrix gemäß Artikel 19 Absatz 2 zu bestimmen;

3. für ihre Prozesse mit kritischen Auswirkungen eine Liste der Anbieter kritischer IKT-Dienste.

Kapitel III – Gemeinsamer Rahmen für die Cybersicherheit im Elektrizitätssektor

Artikel 28 Zusammensetzung, Funktionsweise und Überprüfung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor

(1) Der gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor umfasst die folgenden Kontrollen und Systeme für das Cybersicherheitsmanagement:

a) die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen;

b) die gemäß Artikel 29 entwickelten erweiterten Cybersicherheitskontrollen;

c) die gemäß Artikel 34 entwickelte Vergleichsmatrix, in der die Kontrollen gemäß den Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen und nationaler Rechts- oder Verwaltungsrahmen verglichen werden;

d) das gemäß Artikel 32 eingerichtete Cybersicherheitsmanagementsystem.

(2) Alle Einrichtungen mit erheblichen Auswirkungen wenden die Mindest-Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe a innerhalb ihres Perimeters mit erheblichen Auswirkungen an.

(3) Alle Einrichtungen mit kritischen Auswirkungen wenden die erweiterten Cybersicherheitskontrollen gemäß Absatz 1 Buchstabe b innerhalb ihres Perimeters mit kritischen Auswirkungen an.

(4) Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 wird der in Absatz 1 genannte gemeinsame Rahmen für die Cybersicherheit im Elektrizitätssektor durch die gemäß Artikel 33 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen in der Lieferkette ergänzt.

Artikel 29 Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen

(1) Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen.

(2) Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

(3) Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen müssen überprüft werden können; dazu werden sie entweder im Einklang mit dem Verfahren gemäß Artikel 31 in ein nationales Überprüfungssystem einbezogen oder Sicherheitsaudits durch unabhängige Dritte gemäß den in Artikel 25 Absatz 2 aufgeführten Anforderungen unterzogen.

(4) Die gemäß Absatz 1 entwickelten anfänglichen Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf den Risiken beruhen, die in dem Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 5 ermittelt wurden. Die gemäß Absatz 2 entwickelten geänderten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen müssen auf dem in Artikel 21 Absatz 2 genannten Bericht über die regionale Bewertung des Cybersicherheitsrisikos beruhen.

(5) Die Mindest-Cybersicherheitskontrollen müssen im Einklang mit Artikel 46 Kontrollen zum Schutz der ausgetauschten Informationen umfassen.

(6) Innerhalb von 12 Monaten nach der Genehmigung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 8 Absatz 5 und nach jeder Aktualisierung gemäß Artikel 8 Absatz 10 wenden die in Artikel 2 Absatz 1 genannten Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit erheblichen oder kritischen Auswirkungen eingestuft wurden, bei der Festlegung des Risikominderungsplans auf Ebene der Einrichtung gemäß Artikel 26 Ab-

satz 5 innerhalb der Perimeter mit erheblichen Auswirkungen die Mindest-Cybersicherheitskontrollen und innerhalb der Perimeter mit kritischen Auswirkungen die erweiterten Cybersicherheitskontrollen an.

Artikel 30 Ausnahmen von den Mindest-Cybersicherheitskontrollen und den erweiterten Cybersicherheitskontrollen

(1) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen können bei der jeweils zuständigen Behörde eine Ausnahme von ihrer Verpflichtung zur Anwendung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29 Absatz 6 beantragen. Die zuständige Behörde kann eine solche Ausnahme aus folgenden Gründen gewähren:

a) unter außergewöhnlichen Umständen, wenn die Einrichtung nachweisen kann, dass die Kosten für die Durchführung geeigneter Cybersicherheitskontrollen den Nutzen erheblich übersteigen. Die ACER und ENTSO-E können in Zusammenarbeit mit der EU-VNBO zur Unterstützung der Einrichtungen gemeinsam Leitlinien für die Schätzung der Kosten von Cybersicherheitskontrollen ausarbeiten;

b) bei Vorlage eines Risikobehandlungsplans auf Ebene der Einrichtung, mit dem die Cybersicherheitsrisiken durch alternative Kontrollen auf ein Niveau verringert werden, das nach den in Artikel 26 Absatz 3 Buchstabe b genannten Risikoakzeptanzkriterien akzeptiert werden kann.

(2) Innerhalb von drei Monaten nach Eingang des in Absatz 1 genannten Antrags entscheidet jede zuständige Behörde, ob eine Ausnahme von den Mindest-Cybersicherheitskontrollen und den erweiterten Cybersicherheitskontrollen gewährt wird. Ausnahmen von den Mindest-Cybersicherheitskontrollen oder den erweiterten Cybersicherheitskontrollen werden für höchstens drei Jahre gewährt und können verlängert werden.

(3) Aggregierte und anonymisierte Informationen zu den gewährten Ausnahmen werden dem umfassenden Bericht über die Bewertung des Cybersicherheitsrisikos für grenzüberschreitende Stromflüsse gemäß Artikel 23 als Anhang beigefügt. ENTSO-E und die EU-VNBO aktualisieren die Liste bei Bedarf gemeinsam.

Artikel 31 Überprüfung des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor

(1) Spätestens 24 Monate nach der Annahme der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und der Einrichtung des in Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems muss jede gemäß Artikel 24 Absatz 1 ermittelte Einrichtung mit kritischen Auswirkungen in der Lage sein, auf Verlangen der zuständigen Behörde nachzuweisen, dass sie das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet.

(2) Jede Einrichtung mit kritischen Auswirkungen muss die in Absatz 1 genannte Verpflichtung erfüllen, indem sie sich einem von unabhängigen Dritten durchgeführten Sicherheitsaudit gemäß den Anforderungen aus Artikel 25 Absatz 2 unterzieht oder sich an einem nationalen Überprüfungssystem gemäß Artikel 25 Absatz 1 beteiligt.

(3) Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, erstreckt sich auf alle Vermögenswerte der Einrichtung mit kritischen Auswirkungen innerhalb ihres Perimeters mit kritischen Auswirkungen.

(4) Die Überprüfung, ob eine Einrichtung mit kritischen Auswirkungen das Cybersicherheitsmanagementsystem und die Mindest-Cybersicherheitskontrollen oder die erweiterten Cybersicherheitskontrollen anwendet, wird regelmäßig wiederholt, nämlich spätestens 36 Monate nach Ende der ersten Überprüfung und alle drei Jahre danach.

(5) Jede gemäß Artikel 24 ermittelte Einrichtung mit kritischen Auswirkungen muss die Einhaltung der in Artikel 28 Absatz 1 Buchstaben a, b und c genannten Kontrollen und die Einrichtung des unter Buchstabe d jenes Artikels genannten Cybersicherheitsmanagementsystems nachweisen, indem sie der zuständigen Behörde über das Ergebnis der Überprüfung der Einhaltung Bericht erstattet.

Artikel 32 Cybersicherheitsmanagementsystem

(1) Innerhalb von 24 Monaten, nachdem sie von der zuständigen Behörde darüber unterrichtet wurde, dass sie gemäß Artikel 24 Absatz 6 als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurde, richtet jede Einrichtung mit er-

heblichen oder kritischen Auswirkungen ein Cybersicherheitsmanagementsystem ein, das sie danach alle drei Jahre überprüft, um

a) den Umfang des Cybersicherheitsmanagementsystems unter Berücksichtigung von Schnittstellen und Abhängigkeiten mit anderen Einrichtungen festzulegen;

b) sicherzustellen, dass die gesamte obere Führungsebene über einschlägige rechtliche Verpflichtungen informiert ist und durch rechtzeitige Entscheidungen und rasche Reaktionen aktiv zur Umsetzung des Cybersicherheitsmanagementsystems beiträgt;

c) sicherzustellen, dass die für das Cybersicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;

d) ein Cybersicherheitskonzept festzulegen, das dokumentiert und innerhalb der Einrichtung sowie den von den Sicherheitsrisiken betroffenen Parteien bekannt gegeben wird;

e) Zuständigkeiten für Aufgaben, die für die Cybersicherheit relevant sind, zuzuweisen und bekannt zu geben;

f) das Cybersicherheitsrisikomanagement auf der Ebene der Einrichtungen gemäß Artikel 26 durchzuführen;

g) die für die Umsetzung, Pflege und kontinuierliche Verbesserung des Cybersicherheitsmanagementsystems erforderlichen Ressourcen festzulegen und bereitzustellen, wobei die erforderlichen Kompetenzen und die Sensibilisierung für Cybersicherheitsressourcen zu berücksichtigen sind;

h) die für die Cybersicherheit relevante interne und externe Kommunikation festzulegen;

i) dokumentierte Informationen im Zusammenhang mit dem Cybersicherheitsmanagementsystem zu erstellen, zu aktualisieren und zu kontrollieren;

j) die Ergebnisse und Wirksamkeit des Cybersicherheitsmanagementsystems zu beurteilen;

k) in geplanten Zeitabständen interne Audits durchzuführen, um sicherzustellen, dass das Cybersicherheitsmanagementsystem wirksam umgesetzt und gepflegt wird;

l) die Umsetzung des Cybersicherheitsmanagementsystems in geplanten Zeitabständen zu überprüfen und Abweichungen der Ressourcen und Tätigkeiten von den Konzepten, Verfahren und Leitlinien des Cybersicherheitsmanagementsystems zu kontrollieren und zu beheben.

(2) Der Anwendungsbereich des Cybersicherheitsmanagementsystems der Einrichtung mit erheblichen oder kritischen Auswirkungen umfasst alle Vermögenswerte innerhalb ihres Perimeters mit erheblichen oder kritischen Auswirkungen.

(3) Die zuständigen Behörden regen an, für die Sicherheit von Netz- und Informationssystemen relevante europäische oder internationaler Normen und Spezifikationen anzuwenden, ohne dabei die Nutzung einer bestimmten Technologie vorzuschreiben oder zu begünstigen.

Artikel 33 Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette

(1) Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO einen Vorschlag für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette, mit denen die in den unionsweiten Bewertungen des Cybersicherheitsrisikos ermittelten Risiken für die Lieferketten gemindert werden, um die gemäß Artikel 29 entwickelten Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen zu ergänzen. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette werden zusammen mit den Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette erstrecken sich auf den gesamten Lebenszyklus aller IKT- Produkte, -Dienste und -Prozesse einer Einrichtung mit erheblichen oder kritischen Auswirkungen innerhalb ihrer Perimeter mit erheblichen oder kritischen Auswirkungen. Bei der Entwicklung des Vorschlags für Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen in der Lieferkette wird die NIS-Kooperationsgruppe konsultiert.

(2) Die Mindest-Cybersicherheitskontrollen in der Lieferkette bestehen aus Kontrollen für Einrichtungen mit erheblichen oder kritischen Auswirkungen, die

a) auf Cybersicherheitsspezifikationen bezogene Empfehlungen für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen enthalten und mindestens Folgendes abdecken:

i) Zuverlässigkeitsüberprüfungen der Mitarbeiter des Anbieters, die an der Lieferkette beteiligt sind und sich mit sensiblen Informationen befassen oder Zugang zu Vermögenswerten mit erheblichen oder kritischen Auswirkungen der Einrichtung haben. Die Zuverlässigkeitsüberprüfung kann eine Überprüfung der Identität und des Hintergrunds von Mitarbeitern oder Auftragnehmern einer Einrichtung im Einklang mit den nationalen Rechtsvorschriften und Verfahren sowie dem einschlägigen und geltenden Unionsrecht umfassen, einschließlich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates[18]. Zuverlässigkeitsüberprüfungen müssen verhältnismäßig und strikt auf das Notwendige beschränkt sein. Sie werden ausschließlich zum Zweck der Bewertung eines potenziellen Sicherheitsrisikos für die betreffende Einrichtung durchgeführt. Sie müssen in einem angemessenen Verhältnis zu den Geschäftserfordernissen, der Klassifizierung der einzusehenden Informationen und den wahrgenommenen Risiken stehen und können von der Einrichtung selbst, einem externen Unternehmen, das ein Screening durchführt, oder durch staatliches Clearing vorgenommen werden;

ii) die Prozesse für eine sichere und kontrollierte Gestaltung, Entwicklung und Herstellung von IKT-Produkten, -Diensten und -Prozessen, die Förderung der Gestaltung und Entwicklung von IKT-Produkten, -Diensten und -Prozessen, die geeignete technische Maßnahmen zur Gewährleistung der Cybersicherheit umfassen;

iii) die Gestaltung von Netz- und Informationssystemen, in denen Geräte selbst dann nicht als vertrauenswürdig gelten, wenn sie sich in einem

[18] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

sicheren Perimeter befinden, eine Überprüfung aller eingegangenen Anfragen erfordern und das Prinzip der minimalen Berechtigung angewandt wird;

iv) den Zugang des Anbieters zu den Vermögenswerten der Einrichtung;

v) die vertraglichen Verpflichtungen des Anbieters zum Schutz sensibler Informationen der Einrichtung und zur Beschränkung des Zugangs zu diesen Informationen;

vi) die zugrunde liegenden Spezifikationen für die Cybersicherheit bei der Auftragsvergabe an Unterauftragnehmer des Anbieters;

vii) die Rückverfolgbarkeit der Anwendung der Cybersicherheitsspezifikationen von der Entwicklung über die Produktion bis zur Bereitstellung von IKT-Produkten, -Diensten oder -Prozessen;

viii) die Unterstützung von Sicherheitsaktualisierungen während der gesamten Lebensdauer von IKT-Produkten, -Diensten oder -Prozessen;

ix) das Recht auf Prüfung der Cybersicherheit in den Konzeptions-, Entwicklungs- und Produktionsprozessen des Anbieters sowie

x) die Bewertung des Risikoprofils des Anbieters;

b) diese Einrichtungen dazu verpflichten, die unter Buchstabe a genannten Empfehlungen für die Auftragsvergabe zu berücksichtigen, wenn sie Verträge mit Anbietern, Kooperationspartnern und anderen Parteien in der Lieferkette schließen, sowohl in Bezug auf normale Lieferungen von IKT-Produkten, -Diensten und -Prozessen als auch in Bezug auf ungeplante Ereignisse und Umstände wie die Kündigung und den Übergang von Verträgen im Falle von Fahrlässigkeit des Vertragspartners;

c) diese Einrichtungen dazu verpflichten, die Ergebnisse einschlägiger koordinierter Sicherheitsrisikobewertungen kritischer Lieferketten gemäß Artikel 22 Absatz 1 der Richtlinie (EU) 2022/2555 zu berücksichtigen;

d) Kriterien für die Auswahl von Anbietern und die Auftragsvergabe an Anbieter enthalten, die die unter Buchstabe a genannten Cybersicherheitsspezifikationen erfüllen können und über ein Maß an Cybersicherheit verfügen, das den Cybersicherheitsrisiken des vom Anbieter bereitgestellten IKT-Produkts, -Dienstes oder -Prozesses angemessen ist;

e) Kriterien für die Diversifizierung der Bezugsquellen für IKT-Produkte, -Dienste und -Prozesse und zur Verringerung des Risikos eines Anbieter-Lock-ins enthalten;

f) Kriterien für die regelmäßige Überwachung, Überprüfung oder Prüfung der Cybersicherheitsspezifikationen für interne Betriebsprozesse des Anbieters während des gesamten Lebenszyklus jedes IKT-Produkts, -Dienstes und -Prozesses enthalten.

(3) Für die Cybersicherheitsspezifikationen in der in Absatz 2 Buchstabe a genannten Empfehlung zur Cybersicherheit bei der Auftragsvergabe wenden Einrichtungen mit erheblichen oder kritischen Auswirkungen im Einklang mit Artikel 35 Absatz 4 die Grundsätze der Auftragsvergabe aus der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates[19] an oder legen ihre eigenen Spezifikationen auf der Grundlage der Ergebnisse der Bewertung des Cybersicherheitsrisikos auf der Ebene der Einrichtung fest.

(4) Die erweiterten Cybersicherheitskontrollen in der Lieferkette müssen Kontrollen für Einrichtungen mit kritischen Auswirkungen umfassen, um bei der Auftragsvergabe zu überprüfen, ob IKT-Produkte, -Dienste und -Prozesse, die als Vermögenswerte mit kritischen Auswirkungen verwendet werden sollen, den Cybersicherheitsspezifikationen entsprechen. Das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess wird entweder durch ein europäisches Schema für die Cybersicherheitszertifizierung gemäß Artikel 31 oder mit von der Einrichtung ausgewählten und organisierten Überprüfungsmaßnahmen überprüft. Die Überprüfungsmaßnahmen müssen ausreichend gründlich und umfassend sein, um zu gewährleisten, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess genutzt werden kann, um die in der Risikobewertung auf Ebene der Einrichtung ermittelten Risiken zu mindern. Die Einrichtung mit kritischen Auswirkungen dokumentiert die Maßnahmen zur Verringerung der ermittelten Risiken.

(5) Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für die Beschaffung relevanter IKT-Produkte, -Dienste und -Prozesse. Die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersi-

[19] Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

cherheitskontrollen in der Lieferkette gelten für Einrichtungen, die gemäß Artikel 24 als Einrichtungen mit kritischen oder erheblichen Auswirkungen ermittelt wurden, bei der Auftragsvergabe ab sechs Monaten nach der Annahme oder Aktualisierung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen gemäß Artikel 29.

(6) Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO der zuständigen Behörde eine Änderung der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen in der Lieferkette vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Artikel 34 Vergleichsmatrix für Cybersicherheitskontrollen im Elektrizitätssektor anhand von Normen

(1) Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des Berichts über die unionsweite Bewertung des Cybersicherheitsrisikos gemäß Artikel 19 Absatz 4 erarbeiten die ÜNB mit Unterstützung von ENTSO-E sowie in Zusammenarbeit mit der EU-VNBO und in Absprache mit der ENISA einen Vorschlag für eine Matrix, mit der die Kontrollen gemäß Artikel 28 Absatz 1 Buchstaben a und b anhand ausgewählter europäischer und internationaler Normen sowie einschlägiger technischer Spezifikationen verglichen werden (im Folgenden „Vergleichsmatrix“). ENTSO-E und die EU-VNBO dokumentieren die Gleichwertigkeit der verschiedenen Kontrollen mit den in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen.

(2) Die zuständigen Behörden können ENTSO-E und der EU-VNBO einen Vergleich der in Artikel 28 Absatz 1 Buchstaben a und b genannten Kontrollen mit dem entsprechenden nationalen Rechts- und Verwaltungsrahmen, einschließlich der einschlägigen nationalen Normen der Mitgliedstaaten gemäß Artikel 25 der Richtlinie (EU) 2022/2555, übermitteln. Stellt die zuständige Behörde eines Mitgliedstaats einen solchen Vergleich bereit, so integrieren ENTSO-E und die EU-VNBO diesen nationalen Vergleich in die Vergleichsmatrix.

(3) Innerhalb von sechs Monaten nach Erstellung jedes Berichts über die regionale Bewertung des Cybersicherheitsrisikos gemäß Artikel 21 Absatz 2 schlagen die ÜNB mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sowie in

Absprache mit der ENISA der zuständigen Behörde eine Änderung der Vergleichsmatrix vor. Der Vorschlag wird im Einklang mit Artikel 8 Absatz 10 vorgelegt und muss den in der regionalen Risikobewertung ermittelten Risiken Rechnung tragen.

Kapitel IV – Empfehlungen für die Cybersicherheit bei der Auftragsvergabe

Artikel 35 Empfehlungen für die Cybersicherheit bei der Auftragsvergabe

(1) Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO in einem Arbeitsprogramm, das jedes Mal bei der Annahme eines Berichts über die regionale Bewertung des Cybersicherheitsrisikos erstellt und aktualisiert wird, eine Reihe von unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe, die Einrichtungen mit erheblichen oder kritischen Auswirkungen als Grundlage für die Beschaffung von IKT-Produkten, -Diensten und -Prozessen in den Perimetern mit erheblichen oder kritischen Auswirkungen nutzen können. Dieses Arbeitsprogramm umfasst

a) eine Beschreibung und Klassifizierung der Arten von IKT-Produkten, -Diensten und -Prozessen, die von Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Perimeter mit erheblichen oder kritischen Auswirkungen verwendet werden;

b) eine Liste der Arten von IKT-Produkten, -Diensten und -Prozessen, für die eine Reihe unverbindlicher Cybersicherheitsempfehlungen auf der Grundlage der einschlägigen Berichte über die regionale Bewertung des Cybersicherheitsrisikos und der Prioritäten von Einrichtungen mit erheblichen oder kritischen Auswirkungen zu erstellen sind.

(2) ENTSO-E übermittelt der ACER in Zusammenarbeit mit der EU-VNBO innerhalb von sechs Monaten nach Annahme oder Aktualisierung des Berichts über die regionale Bewertung des Cybersicherheitsrisikos eine Zusammenfassung dieses Arbeitsprogramms.

(3) Die ÜNB bemühen sich mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicherzustellen, dass die auf der Grundlage der einschlägigen regionalen Bewertung des Cybersicherheitsrisikos entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe in allen Netzbetriebsregionen ähnlich oder vergleichbar sind. Die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe müssen mindestens die in Artikel 33 Absatz 2 Buchstabe a genann-

ten Spezifikationen umfassen. Soweit möglich, werden die Spezifikationen aus europäischen und internationalen Normen ausgewählt.

(4) Die ÜNB stellen mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO sicher, dass die Empfehlungen für die Cybersicherheit bei der Auftragsvergabe

a) den Grundsätzen der Auftragsvergabe aus der Richtlinie 2014/24/EU entsprechen und

b) mit den neuesten verfügbaren europäischen Schemata für die Cybersicherheitszertifizierung, die für das IKT-Produkt, den IKT-Dienst oder den IKT-Prozess relevant sind, vereinbar sind und diesen Rechnung tragen.

Artikel 36 Leitlinien für die Nutzung europäischer Schemata für die Cybersicherheitszertifizierung bei der Beschaffung von IKT-Produkten, -Diensten und -Prozessen

(1) Unbeschadet des Rahmens für die Schaffung europäischer Schemata für die Cybersicherheitszertifizierung gemäß Artikel 46 der Verordnung (EU) 2019/881 können die gemäß Artikel 35 entwickelten unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe sektorspezifische Leitlinien für die Verwendung europäischer Schemata für die Cybersicherheitszertifizierung umfassen, wenn für eine von Einrichtungen mit kritischen Auswirkungen verwendete Art von IKT-Produkten, -Diensten oder -Prozessen ein geeignetes Schema zur Verfügung steht.

(2) Die ÜNB arbeiten mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO eng mit der ENISA zusammen, um die sektorspezifischen Leitlinien bereitzustellen, die in den unverbindlichen Empfehlungen für die Cybersicherheit bei der Auftragsvergabe gemäß Absatz 1 enthalten sind.

Kapitel V – Informationsflüsse, Cyberangriffe und Krisenmanagement

Artikel 37 Vorschriften für den Informationsaustausch

(1) Erhält eine zuständige Behörde Informationen über einen meldepflichtigen Cyberangriff,

a) bewertet sie den Grad der Vertraulichkeit dieser Informationen und unterrichtet die Einrichtung unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Eingang der Informationen, über das Ergebnis ihrer Bewertung;

b) versucht sie, andere ähnliche Cyberangriffe in der Union zu ermitteln, die anderen zuständigen Behörden gemeldet wurden, um die zu dem meldepflichtigen Cyberangriff eingegangenen Informationen mit Informationen zu vergleichen, die zu anderen Cyberangriffen bereitgestellt wurden, und um vorhandene Informationen zu ergänzen sowie die Reaktion im Bereich der Cybersicherheit zu stärken und zu koordinieren;

c) ist sie für die Entfernung von Geschäftsgeheimnissen und die Anonymisierung der Informationen im Einklang mit den einschlägigen nationalen Vorschriften und Unionsvorschriften verantwortlich;

d) übermittelt sie die Informationen unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen über einen meldepflichtigen Cyberangriff, den nationalen zentralen Anlaufstellen, den CSIRTs und allen gemäß Artikel 4 benannten zuständigen Behörden anderer Mitgliedstaten und stellt diesen Behörden oder Stellen regelmäßig aktualisierte Informationen zur Verfügung;

e) übermittelt sie die Informationen über den Cyberangriff nach Anonymisierung und Entfernung von Geschäftsgeheimnissen gemäß Absatz 1 Buchstabe c unverzüglich, spätestens jedoch 24 Stunden nach Eingang der Informationen gemäß Absatz 1 Buchstabe a, den Einrichtungen mit kritischen oder erheblichen Auswirkungen in ihrem Mitgliedstaat und stellt regelmäßig aktualisierte Informationen bereit, um den Einrichtungen einen wirksamen Schutz zu ermöglichen;

f) kann sie die meldende Einrichtung mit erheblichen oder kritischen Auswirkungen auffordern, die meldepflichtigen Informationen über Cyberangriffe auf sichere Weise an andere möglicherweise betroffene Einrichtungen weiterzuleiten, um den Elektrizitätssektor für die Lage zu sensibilisieren und zu verhindern, dass ein Risiko eintritt, das dort zu einem grenzüberschreitenden Cybersicherheitsvorfall eskalieren könnte;

g) übermittelt sie der ENISA nach Anonymisierung und Entfernung von Geschäftsgeheimnissen einen zusammenfassenden Bericht mit den Informationen zu dem Cyberangriff.

(2) Erhält ein CSIRT Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

a) teilt es diese der ENISA unverzüglich über einen geeigneten Kanal für den sicheren Informationsaustausch mit, sofern in anderen Rechtsvorschriften der Union nichts anderes bestimmt ist;

b) unterstützt es die betroffene Einrichtung dabei, vom Hersteller oder Anbieter eine wirksame, koordinierte und rasche Behandlung der aktiv ausgenutzten Schwachstelle ohne Patch oder wirksame und effiziente Abhilfemaßnahmen zu erhalten;

c) tauscht es die verfügbaren Informationen mit dem Verkäufer aus und fordert den Hersteller oder Anbieter auf, möglichst eine Liste der CSIRTs in den Mitgliedstaaten vorzulegen, die von der aktiv ausgenutzten Schwachstelle ohne Patch betroffen sind und informiert werden müssen;

d) tauscht es verfügbare Informationen nach dem Grundsatz „Kenntnis nur, wenn nötig“ mit den unter obigem Buchstaben genannten CSIRTs aus;

e) stellt es Informationen über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch bereit.

(3) Erhält eine zuständige Behörde Kenntnis von einer aktiv ausgenutzten Schwachstelle ohne Patch, so

a) informiert sie in Abstimmung mit den CSIRTs in ihrem Mitgliedstaat über etwaige vorhandene Abhilfestrategien und -maßnahmen in Bezug auf die aktiv ausgenutzte Schwachstelle ohne Patch;

b) übermittelt sie die Informationen an ein CSIRT in dem Mitgliedstaat, in dem die aktiv ausgenutzte Schwachstelle ohne Patch gemeldet wurde.

(4) Erhält die zuständige Behörde Kenntnis von einer Schwachstelle ohne Patch, in Bezug auf die keine Beweise für eine aktive Ausnutzung vorliegen, stimmt sie sich unverzüglich mit dem CSIRT im Hinblick auf eine koordinierte Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 ab.

(5) Erhält ein CSIRT gemäß Artikel 38 Absatz 6 von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen in Bezug auf Cyberbedrohungen, so leitet es diese oder andere Informationen, die für die Verhütung, Erkennung, Behandlung oder Minderung des damit verbundenen Risikos von Bedeutung sind, an die Einrichtungen mit kritischen oder erheblichen Auswirkungen in seinem Mitgliedstaat und gegebenenfalls an alle betroffenen CSIRTs und seine nationa-

le zentralen Anlaufstelle unverzüglich, spätestens jedoch vier Stunden nach Eingang der Informationen, weiter.

(6) Erhält eine zuständige Behörde von einer oder mehreren Einrichtungen mit erheblichen oder kritischen Auswirkungen Informationen über Cyberbedrohungen, so leitet sie diese Informationen für die Zwecke des Absatzes 5 an das CSIRT weiter.

(7) Die zuständigen Behörden können die Zuständigkeiten nach den Absätzen 3 und 4 in Bezug auf eine oder mehrere Einrichtungen mit erheblichen oder kritischen Auswirkungen, die in mehr als einem Mitgliedstaat tätig sind, ganz oder teilweise an eine andere zuständige Behörde in einem dieser Mitgliedstaaten delegieren, sofern sich die betroffenen zuständigen Behörden darauf geeinigt haben.

(8) Die ÜNB entwickeln mit Unterstützung von ENTSO-E und in Zusammenarbeit mit der EU-VNBO bis zum 13 Juni 2025 eine Klassifizierungsmethode für Cyberangriffe. Die ÜNB können mit Unterstützung von ENTSO-E und der EU-VNBO die zuständigen Behörden ersuchen, die ENISA und ihre für Cybersicherheit zuständigen Behörden zur Unterstützung bei der Entwicklung einer solchen Klassifizierungsskala zu konsultieren. Die Methode muss fünf Stufen für die Schwere eines Cyberangriffs enthalten, wobei „erheblich“ und „kritisch“ die höchsten Stufen darstellen. Die Klassifizierung muss sich auf die Bewertung der folgenden Parameter stützen:

a) die potenziellen Auswirkungen unter Berücksichtigung der gemäß Artikel 26 Absatz 4 Buchstabe c ermittelten exponierten Vermögenswerte und Perimeter und

b) die Schwere des Cyberangriffs.

(9) Bis zum 13 Juni 2026 führt ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Machbarkeitsstudie hinsichtlich der Möglichkeit durch, ein gemeinsames Instrument zu entwickeln, das es allen Einrichtungen ermöglicht, Informationen mit den zuständigen nationalen Behörden auszutauschen, und prüft die damit verbundenen finanziellen Kosten.

(10) In der Machbarkeitsstudie wird die Möglichkeit geprüft, ein solches gemeinsames Instrument

a) zu nutzen, um Einrichtungen mit kritischen oder erheblichen Auswirkungen durch einschlägige sicherheitsrelevante Informationen für den Betrieb grenzüberschreitender Stromflüsse zu unterstützen, z. B. durch echtzeitnahe Berichterstattung über Cyberangriffe, Frühwarnungen im Zusammenhang mit

Cybersicherheitsfragen und nicht offengelegten Schwachstellen von Geräten, die im Elektrizitätssystem eingesetzt werden;

b) in einem geeigneten und äußerst vertrauenswürdigen Umfeld zu pflegen;

c) zu nutzen, um Daten bei Einrichtungen mit kritischen oder erheblichen Auswirkungen zu erheben und die Entfernung vertraulicher Informationen und die Anonymisierung der Daten zu unterstützen und diese unverzüglich an Einrichtungen mit kritischen oder erheblichen Auswirkungen weiterzuleiten.

(11) In Zusammenarbeit mit der EU-VNBO

a) konsultiert ENTSO-E bei der Machbarkeitsstudie die ENISA und die NIS-Kooperationsgruppe, die nationalen zentralen Anlaufstellen und die Vertreter der wichtigsten Interessenträger;

b) legt ENTSO-E die Ergebnisse der Machbarkeitsstudie der ACER und der NIS-Kooperationsgruppe vor.

(12) ENTSO-E kann in Zusammenarbeit mit der EU-VNBO Initiativen analysieren und unterstützen, die von Einrichtungen mit kritischen oder erheblichen Auswirkungen vorgeschlagen werden, um solche Instrumente für den Informationsaustausch zu bewerten und zu testen.

Artikel 38 Aufgaben von Einrichtungen mit erheblichen oder kritischen Auswirkungen beim Informationsaustausch

(1) Jede Einrichtung mit erheblichen oder kritischen Auswirkungen

a) richtet für alle Vermögenswerte innerhalb ihres gemäß Artikel 26 Absatz 4 Buchstabe c bestimmten Cybersicherheitsperimeters mindestens die CSOC-Kapazitäten ein, um

i) sicherzustellen, dass die einschlägigen Netz- und Informationssysteme und -anwendungen Sicherheitsprotokolle für die Sicherheitsüberwachung umfassen, damit Anomalien erkannt und Informationen über Cyberangriffe erhoben werden können;

ii) die Sicherheitsüberwachung durchzuführen, einschließlich der Erkennung eines Eindringens und der Bewertung von Schwachstellen von Netz- und Informationssystemen;

iii) zu analysieren und erforderlichenfalls im Rahmen ihrer Zuständigkeit und Kapazitäten alle für den Schutz der Einrichtung erforderlichen Maßnahmen zu ergreifen;

iv) sich an der in diesem Artikel beschriebenen Erhebung und Weitergabe von Informationen zu beteiligen;

b) ist berechtigt, sich diese Kapazitäten gemäß Buchstabe a ganz oder teilweise über MSSP zu beschaffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen bleiben für die MSSP verantwortlich und überwachen deren Bemühungen;

c) benennt für den Informationsaustausch eine zentrale Anlaufstelle auf Ebene der Einrichtung.

(2) Die ENISA kann im Rahmen der in Artikel 6 Absatz 2 der Verordnung (EU) 2019/881 festgelegten Aufgabe unverbindliche Leitlinien für die Einrichtung solcher Kapazitäten oder die Vergabe von Unteraufträgen an MSSP für die Erbringung des Dienstes herausgeben.

(3) Jede Einrichtung mit kritischen oder erheblichen Auswirkungen teilt ihren CSIRTs und der für sie zuständigen Behörde relevante Informationen im Zusammenhang mit einem meldepflichtigen Cyberangriff unverzüglich, spätestens jedoch vier Stunden, nachdem ihr bekannt wurde, dass der Sicherheitsvorfall meldepflichtig ist, mit.

(4) Informationen im Zusammenhang mit einem Cyberangriff gelten als meldepflichtig, wenn der Cyberangriff bei der Bewertung durch die betroffene Einrichtung nach der Klassifizierungsmethode für Cyberangriffe gemäß Artikel 37 Absatz 8 als „erheblich“ bis „kritisch“ eingestuft wird. Die gemäß Absatz 1 Buchstabe c benannte zentrale Anlaufstelle auf Ebene der Einrichtung teilt die Einstufung des Sicherheitsvorfalls mit.

(5) Übermitteln Einrichtungen mit kritischen oder erheblichen Auswirkungen relevante Informationen zu aktiv ausgenutzten Schwachstellen ohne Patch an ein CSIRT, so kann dieses diese Informationen an die für das CSIRT zuständige Behörde weiterleiten. Je nach Sensibilität der gemeldeten Informationen kann das CSIRT die Informationen aus triftigen cybersicherheitsbezogenen Gründen zurückhalten oder zeitverzögert übermitteln.

(6) Jede Einrichtung mit kritischen oder erheblichen Auswirkungen stellt ihren CSIRTs unverzüglich alle Informationen im Zusammenhang mit einer meldepflichtigen Cyberbedrohung bereit, die grenzüberschreitende Auswirkungen haben könnte.

Informationen im Zusammenhang mit einer Cyberbedrohung gelten als meldepflichtig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

a) Sie umfassen relevante Informationen für die Verhütung, Erkennung, Behandlung oder Minderung der Auswirkungen des Risikos durch andere Einrichtungen mit kritischen oder erheblichen Auswirkungen;

b) die ermittelten, im Zusammenhang mit einem Angriff genutzten Vorgehensweisen, Taktiken und Verfahren sind mit Informationen wie kompromittierten URL-Adressen oder IP-Adressen, Hashs oder anderen Attributen verbunden, die für die Kontextualisierung und Zuordnung des Angriffs nützlich sind;

c) eine Cyberbedrohung kann weiter bewertet und mit zusätzlichen Informationen verknüpft werden, die von Dienstanbietern oder Dritten, die nicht dieser Verordnung unterliegen, bereitgestellt werden.

(7) Jede Einrichtung mit kritischen oder erheblichen Auswirkungen gibt beim Austausch von Informationen gemäß diesem Artikel an,

a) dass die Informationen gemäß dieser Verordnung übermittelt werden;

b) ob die Informationen Folgendes betreffen:

   i) einen meldepflichtigen Cyberangriff gemäß Absatz 3;

   ii) nicht öffentlich bekannte aktiv ausgenutzte Schwachstellen ohne Patch gemäß Absatz 4;

   iii) eine meldepflichtige Cyberbedrohung gemäß Absatz 5;

c) im Falle eines meldepflichtigen Cyberangriffs, welchen Grad der Cyberangriff nach der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe aufweist und welche Informationen zu dieser Einstufung geführt haben, einschließlich mindestens der Kritikalität des Cyberangriffs.

(8) Meldet eine Einrichtung mit kritischen oder erheblichen Auswirkungen einen erheblichen Sicherheitsvorfall gemäß Artikel 23 der Richtlinie (EU) 2022/2555 und enthält die Meldung des Sicherheitsvorfalls nach dem genannten Artikel einschlägige Informationen gemäß Absatz 3 des vorliegenden Artikels, so gilt die Meldung der Einrichtung nach Artikel 23 Absatz 1 der genannten Richtlinie auch als Meldung von Informationen gemäß Absatz 3 des vorliegenden Artikels.

(9) Jede Einrichtung mit kritischen oder erheblichen Auswirkungen erstattet der für sie zuständigen Behörde oder dem CSIRT Bericht, wobei sie klar angibt, welche Informationen nur an die zuständige Behörde oder das CSIRT übermittelt werden dür-

fen, wenn der Informationsaustausch die Quelle eines Cyberangriffs sein könnte. Jede Einrichtung mit kritischen oder erheblichen Auswirkungen hat das Recht, dem zuständigen CSIRT eine nichtvertrauliche Fassung der Informationen zur Verfügung zu stellen.

Artikel 39 Erkennung von Cyberangriffen und Umgang mit den damit zusammenhängenden Informationen

(1) Einrichtungen mit erheblichen oder kritischen Auswirkungen entwickeln mit der erforderlichen Unterstützung der jeweils zuständigen Behörde, von ENTSO-E und der EU-VNBO die erforderlichen Kapazitäten für den Umgang mit entdeckten Cyberangriffen. Einrichtungen mit kritischen oder erheblichen Auswirkungen können von dem CSIRT unterstützt werden, das in ihrem jeweiligen Mitgliedstaat im Rahmen der den CSIRTs gemäß Artikel 11 Absatz 5 Buchstabe a der Richtlinie (EU) 2022/2555 übertragenen Aufgabe benannt wurde. Einrichtungen mit kritischen oder erheblichen Auswirkungen setzen wirksame Verfahren zur Ermittlung, Klassifizierung und Bewältigung von Cyberangriffen ein, die sich auf grenzüberschreitende Stromflüsse auswirken oder auswirken könnten, um deren Auswirkungen möglichst gering zu halten.

(2) Hat ein Cyberangriff Auswirkungen auf grenzüberschreitende Stromflüsse, so arbeiten die zentralen Anlaufstellen auf Ebene der betroffenen Einrichtungen mit kritischen oder erheblichen Auswirkungen zusammen, um Informationen untereinander auszutauschen, wobei sie von der zuständigen Behörde des Mitgliedstaats, in dem der Cyberangriff zuerst gemeldet wurde, koordiniert werden.

(3) Einrichtungen mit kritischen oder erheblichen Auswirkungen

a) stellen sicher, dass ihre eigene zentrale Anlaufstelle auf Ebene der Einrichtung nach dem Grundsatz „Kenntnis nur, wenn nötig“ Zugang zu den Informationen hat, die sie von der nationalen zentralen Anlaufstelle über ihre zuständige Behörde erhalten hat;

b) übermitteln, sofern dies nicht bereits gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2022/2555 geschehen ist, der zuständigen Behörde des Mitgliedstaats, in dem sie niedergelassen sind, und der nationalen zentralen Anlaufstelle eine Liste ihrer für die Cybersicherheit zuständigen zentralen Anlaufstellen,

   i) von denen die zuständige Behörde und die nationale zentrale Anlaufstelle Informationen über meldepflichtige Cyberangriffe erhalten könnte;

ii) an die die zuständigen Behörden und die nationalen zentralen Anlaufstellen gegebenenfalls Informationen übermitteln müssen;

c) richten auf der Grundlage der beobachtbaren Entwicklung des Cyberangriffs innerhalb der Perimeter mit kritischen oder erheblichen Auswirkungen Verfahren zur Bewältigung von Cyberangriffen ein, einschließlich Rollen und Zuständigkeiten, Aufgaben und Reaktionen;

d) testen mindestens einmal jährlich alle Verfahren zur Bewältigung von Cyberangriffen, wobei sie mindestens ein Szenario testen, das sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirkt. Dieser jährliche Test kann von Einrichtungen mit kritischen oder erheblichen Auswirkungen während der regelmäßigen Übungen gemäß Artikel 43 durchgeführt werden. Jede Live-Reaktionsmaßnahme auf einen Cyberangriff mit einer Folge, die gemäß der in Artikel 37 Absatz 8 genannten Klassifizierungsmethode für Cyberangriffe mindestens in die Stufe 2 eingestuft wird und der eine Cybersicherheitsursache zugrunde liegt, kann als jährlicher Test des Plans für die Reaktion auf Cyberangriffe betrachtet werden.

(4) Die in Absatz 1 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

Artikel 40 Krisenmanagement

(1) Stellt die zuständige Behörde fest, dass eine Stromversorgungskrise im Zusammenhang mit einem Cyberangriff steht, der Auswirkungen auf mehr als einen Mitgliedstaat hat, setzen die zuständigen Behörden der betroffenen Mitgliedstaaten, die CS-NCA, die RP-NCA und die NIS-Behörden für das Cyberkrisenmanagement der betroffenen Mitgliedstaaten gemeinsam eine Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen ein.

(2) Die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen

a) koordiniert eine effiziente Einholung aller relevanten Cybersicherheitsinformationen und deren weitere Übermittlung an die am Krisenmanagementprozess beteiligten Einrichtungen;

b) organisiert die Kommunikation zwischen allen von der Krise betroffenen Einrichtungen und den zuständigen Behörden, um Überschneidungen zu verringern und die Effizienz der Analysen und technischen Reaktionen zur Bewäl-

tigung zeitgleich auftretender Stromversorgungskrisen, denen eine Cybersicherheitsursache zugrunde liegt, zu erhöhen;

c) stellt in Zusammenarbeit mit den zuständigen CSIRTs das erforderliche Fachwissen bereit, einschließlich operativer Beratung bei der Umsetzung möglicher Abhilfemaßnahmen für die von dem Sicherheitsvorfall betroffenen Einrichtungen;

d) unterrichtet die Kommission und die Koordinierungsgruppe „Strom“ im Einklang mit den in Artikel 46 festgelegten Schutzprinzipien über den Stand des Sicherheitsvorfalls und aktualisiert diese Informationen regelmäßig;

e) holt Rat bei den zuständigen Behörden, Agenturen oder Einrichtungen ein, die zur Bewältigung der Stromversorgungskrise beitragen könnten.

(3) Gilt der Cyberangriff als Cybersicherheitsvorfall großen Ausmaßes oder wird dies erwartet, unterrichtet die Ad-hoc- Koordinierungsgruppe für grenzüberschreitende Krisen unverzüglich die nationalen Behörden für das Cyberkrisenmanagement gemäß Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2555 in den von dem Sicherheitsvorfall betroffenen Mitgliedstaaten sowie die Kommission und das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe). In einer solchen Situation unterstützt die Ad-hoc-Koordinierungsgruppe für grenzüberschreitende Krisen das EU-CyCLONe in Bezug auf sektorale Besonderheiten.

(4) Einrichtungen mit kritischen oder erheblichen Auswirkungen müssen Kapazitäten, interne Leitlinien, Vorsorgepläne und Personal, das an der Aufdeckung und Eindämmung grenzüberschreitender Krisen mitwirkt, vorsehen und darüber verfügen. Die von einer zeitgleich auftretenden Stromversorgungskrise betroffene Einrichtung mit kritischen oder erheblichen Auswirkungen untersucht die zugrunde liegende Ursache dieser Krise in Zusammenarbeit mit der für sie zuständigen Behörde, um festzustellen, inwieweit die Krise mit einem Cyberangriff in Verbindung steht.

(5) Die in Absatz 4 genannten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

Artikel 41 Cybersicherheitskrisenmanagement- und -reaktionspläne

(1) Innerhalb von 24 Monaten nach der Übermittlung des Berichts über die unionsweite Risikobewertung an die ACER entwickelt diese in enger Zusammenarbeit mit der ENISA, ENTSO-E, der EU-VNBO, den CS-NCA, den zuständigen Behörden, den

RP-NCA, den NRB und den nationalen NIS-Behörden für das Cyberkrisenmanagement einen unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor.

(2) Innerhalb von 12 Monaten nach der Ausarbeitung des unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplans für den Elektrizitätssektor gemäß Absatz 1 durch die ACER erstellt jede zuständige Behörde einen nationalen Cybersicherheitskrisenmanagement- und -reaktionsplan für grenzüberschreitende Stromflüsse unter Berücksichtigung des unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplans für den Elektrizitätssektor und des gemäß Artikel 10 der Verordnung (EU) 2019/941 erstellten nationalen Risikovorsorgeplans. Dieser Plan muss mit dem Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 im Einklang stehen. Die zuständige Behörde stimmt sich mit den Einrichtungen mit kritischen oder erheblichen Auswirkungen sowie mit der RP-NCA in ihrem Mitgliedstaat ab.

(3) Der gemäß Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 erforderliche nationale Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gilt als nationaler Plan für das Cybersicherheitskrisenmanagement im Sinne dieses Artikels, wenn er Bestimmungen für das Krisenmanagement und die Krisenreaktion in Bezug auf grenzüberschreitende Stromflüsse enthält.

(4) Die in den Absätzen 1 und 2 aufgeführten Aufgaben können von den Mitgliedstaaten gemäß Artikel 37 Absatz 2 der Verordnung (EU) 2019/943 auch an die regionalen Koordinierungszentren delegiert werden.

(5) Einrichtungen mit kritischen oder erheblichen Auswirkungen stellen sicher, dass ihre Krisenmanagementprozesse im Bereich der Cybersicherheit

a) kompatible Verfahren für die grenzüberschreitende Bewältigung von Cybersicherheitsvorfällen gemäß Artikel 6 Nummer 8 der Richtlinie (EU) 2022/2555 umfassen, die förmlich in ihren Krisenmanagementpläne enthalten sind;

b) Teil der allgemeinen Krisenmanagementmaßnahmen sind.

(6) Innerhalb von 12 Monaten nach der Unterrichtung der Einrichtungen mit erheblichen oder kritischen Auswirkungen gemäß Artikel 24 Absatz 6 und danach alle drei Jahre erstellen Einrichtungen mit kritischen oder erheblichen Auswirkungen auf Ebene der Einrichtung einen Krisenmanagementplan für Cybersicherheitskrisen, der in ihre allgemeinen Krisenmanagementpläne aufgenommen wird. Dieser Plan muss mindestens Folgendes umfassen:

a) Regeln für die Erklärung einer Krise gemäß Artikel 14 Absätze 2 und 3 der Verordnung (EU) 2019/941;

b) klare Aufgaben und Zuständigkeiten für das Krisenmanagement, einschließlich der Rolle anderer relevanter Einrichtungen mit kritischen oder erheblichen Auswirkungen;

c) aktuelle Kontaktinformationen sowie Regeln für die Kommunikation und den Informationsaustausch während einer Krisensituation, einschließlich der Verbindung zu den CSIRTs.

(7) Die Maßnahmen für das Krisenmanagement gemäß Artikel 21 Absatz 2 Buchstabe c der Richtlinie (EU) 2022/2555 gelten als Krisenmanagementplan auf Ebene der Einrichtung für den Elektrizitätssektor im Sinne dieses Artikels, wenn sie alle in Absatz 6 aufgeführten Anforderungen erfüllen.

(8) Die Krisenmanagementpläne werden in den Cybersicherheitsübungen gemäß den Artikeln 43, 44 und 45 getestet.

(9) In Bezug auf Prozesse mit kritischen oder erheblichen Auswirkungen nehmen Einrichtungen mit kritischen oder erheblichen Auswirkungen ihre Krisenmanagementpläne auf Ebene der Einrichtung in ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) auf. Die Krisenmanagementpläne auf Ebene der Einrichtung müssen Folgendes umfassen:

a) Prozesse, die von der Verfügbarkeit, Integrität und Zuverlässigkeit von IT-Diensten abhängen;

b) alle Standorte für die Aufrechterhaltung des Geschäftsbetriebs, einschließlich der Standorte für Hardware und Software;

c) alle internen Aufgaben und Zuständigkeiten im Zusammenhang mit den Verfahren zur Aufrechterhaltung des Geschäftsbetriebs.

(10) Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihre Krisenmanagementpläne auf Ebene der Einrichtung mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

(11) Die ACER aktualisiert den gemäß Absatz 1 erstellten unionsweiten Cybersicherheitskrisenmanagement- und -reaktionsplan für den Elektrizitätssektor mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.

(12) Jede zuständige Behörde aktualisiert den gemäß Absatz 2 erstellten nationalen Cybersicherheitskrisenmanagement- und -reaktionsplan für grenzüberschreitende

Stromflüsse mindestens alle drei Jahre sowie immer dann, wenn dies erforderlich ist.
(13) Einrichtungen mit kritischen oder erheblichen Auswirkungen testen ihre Pläne zur Aufrechterhaltung des Geschäftsbetriebs mindestens einmal alle drei Jahre oder nach größeren Änderungen in einem Prozess mit kritischen Auswirkungen. Die Ergebnisse der Tests der Pläne zur Aufrechterhaltung des Geschäftsbetriebs werden dokumentiert. Einrichtungen mit kritischen oder erheblichen Auswirkungen können den Test ihres Plans zur Aufrechterhaltung des Geschäftsbetriebs in die Cybersicherheitsübungen einbeziehen.
(14) Einrichtungen mit kritischen oder erheblichen Auswirkungen aktualisieren ihren Plan zur Aufrechterhaltung des Geschäftsbetriebs immer bei Bedarf und mindestens einmal alle drei Jahre unter Berücksichtigung der Ergebnisse des Tests.
(15) Werden bei einem Test Mängel im Plan zur Aufrechterhaltung des Geschäftsbetriebs festgestellt, behebt die Einrichtung mit kritischen oder erheblichen Auswirkungen diese Mängel innerhalb von 180 Kalendertagen nach dem Test und führt einen neuen Test durch, um nachzuweisen, dass die Korrekturmaßnahmen wirksam sind.
(16) Kann eine Einrichtung mit kritischen oder erheblichen Auswirkungen die Mängel nicht innerhalb von 180 Kalendertagen beheben, nimmt sie die Gründe in den Bericht auf, der der für sie zuständigen Behörde gemäß Artikel 27 vorzulegen ist.

Artikel 42 Cybersicherheits-Frühwarnkapazitäten für den Elektrizitätssektor

(1) Die zuständigen Behörden arbeiten mit der ENISA zusammen, um im Rahmen der Unterstützung für die Mitgliedstaaten gemäß Artikel 6 Absätze 2 und 7 der Verordnung (EU) 2019/881 Frühwarnkapazitäten für die Cybersicherheit im Elektrizitätsbereich (Electricity Cybersecurity Early Alert Capabilities, ECEAC) zu entwickeln.
(2) Die ECEAC müssen es der ENISA bei der Wahrnehmung der in Artikel 7 Absatz 7 der Verordnung (EU) 2019/881 aufgeführten Aufgaben ermöglichen,

a) freiwillig ausgetauschte Informationen einzuholen bei:
   i) CSIRTs, zuständigen Behörden;
   ii) den in Artikel 2 der vorliegenden Verordnung aufgeführten Einrichtungen;
   iii) jeder anderen Einrichtung, die relevante Informationen auf freiwilliger Basis weitergeben möchte;
b) die eingeholten Informationen zu bewerten und zu klassifizieren;

c) die Informationen zu bewerten, zu denen die ENISA Zugang hat, um Risikobedingungen für die Cybersicherheit und relevante Indikatoren für Aspekte grenzüberschreitender Stromflüsse zu ermitteln;

d) Bedingungen und Indikatoren zu ermitteln, die häufig mit Cyberangriffen im Elektrizitätssektor korrelieren;

e) anhand der Bewertung und Ermittlung von Risikofaktoren festzulegen, ob weitere Analysen vorzunehmen und Präventivmaßnahmen zu ergreifen sind;

f) die zuständigen Behörden über die ermittelten Risiken und empfohlene Präventionsmaßnahmen für die betreffenden Einrichtungen zu unterrichten;

g) alle in Artikel 2 aufgeführten relevanten Einrichtungen über die Ergebnisse der gemäß den Buchstaben b, c und d dieses Absatzes bewerteten Informationen zu unterrichten;

h) die einschlägigen Informationen regelmäßig in den gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 erstellten EU-Cybersicherheitslagebericht aufnehmen;

i) soweit möglich, aus den erhobenen Informationen anwendbare Daten abzuleiten, die darauf hindeuten, dass ein potenzieller Sicherheitsverstoß oder Cyberangriff („Kompromittierungsindikatoren“) vorliegt.

(3) Die CSIRTs leiten die von der ENISA bereitgestellten Informationen im Rahmen ihrer in Artikel 11 Absatz 3 Buchstabe b der Richtlinie (EU) 2022/2555 festgelegten Aufgaben unverzüglich an die betreffenden Einrichtungen weiter.

(4) Die ACER überwacht die Wirksamkeit der ECEAC. Die ENISA unterstützt die ACER durch Bereitstellung aller erforderlichen Informationen gemäß Artikel 6 Absatz 2 und Artikel 7 Absatz 1 der Verordnung (EU) 2019/881. Die Analyse dieser Überwachungstätigkeit ist Teil der Überwachung gemäß Artikel 12 der vorliegenden Verordnung.

Kapitel VI – Rahmen für Cybersicherheitsübungen im Elektrizitätssektor

Artikel 43 Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten

(1) Bis zum 31. Dezember des Jahres nach der Unterrichtung der Einrichtungen mit kritischen Auswirkungen und danach alle drei Jahre führt jede Einrichtung mit kritischen Auswirkungen eine Cybersicherheitsübung durch, die ein oder mehrere Sze-

narien mit Cyberangriffen umfasst, die sich direkt oder indirekt auf grenzüberschreitende Stromflüsse auswirken und mit den gemäß den Artikeln 20 und 27 bei den Cybersicherheitsrisikobewertungen auf Ebene der Mitgliedstaaten und Einrichtungen ermittelten Risiken im Zusammenhang stehen.

(2) Abweichend von Absatz 1 kann die RP-NCA nach Konsultation der zuständigen Behörde und der gemäß Artikel 9 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörde für das Cyberkrisenmanagement beschließen, anstelle der Cybersicherheitsübung auf Ebene der Einrichtung eine Cybersicherheitsübung gemäß Absatz 1 auf Ebene des Mitgliedstaats durchzuführen. In diesem Zusammenhang unterrichtet die zuständige Behörde

a) alle Einrichtungen mit kritischen Auswirkungen ihres Mitgliedstaats, die NRB, die CSIRTs und die CS-NCA bis spätestens 30. Juni des Jahres, das der Cybersicherheitsübung auf Ebene der Einrichtungen vorausgeht;

b) jede Einrichtung, die an der Cybersicherheitsübung auf Ebene des Mitgliedstaats teilnehmen muss, spätestens sechs Monate vor der Übung.

(3) Die RP-NCA organisiert mit technischer Unterstützung ihrer CSIRTs die in Absatz 2 beschriebene Cybersicherheitsübung auf Ebene des Mitgliedstaats getrennt oder zusammen mit einer anderen Cybersicherheitsübung in diesem Mitgliedstaat. Um diese Übungen zusammenfassen zu können, kann die RP-NCA die in Absatz 1 genannte Cybersicherheitsübung auf Ebene des Mitgliedstaats um ein Jahr verschieben.

(4) Die Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten müssen mit den nationalen Rahmen für das Cybersicherheitskrisenmanagement gemäß Artikel 9 Absatz 4 Buchstabe d der Richtlinie (EU) 2022/2555 im Einklang stehen.

(5) Bis zum 31 Dezember 2026 und danach alle drei Jahre stellt ENTSO-E in Zusammenarbeit mit der EU-VNBO ein Muster für das Übungsszenario für die Durchführung der in Absatz 1 genannten Cybersicherheitsübungen auf Ebene der Einrichtungen und der Mitgliedstaaten bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheitsrisikos auf Ebene der Einrichtungen und der Mitgliedstaaten Rechnung tragen und zentrale Leistungskriterien enthalten. ENTSO-E und die EU-VNBO beziehen die ACER und die ENISA bei der Entwicklung dieses Musters ein.

Artikel 44 Regionale oder überregionale Cybersicherheitsübungen

(1) Bis zum 31 Dezember 2029 und danach alle drei Jahre organisiert ENTSO-E in Zusammenarbeit mit der EU-VNBO in jeder Netzbetriebsregion eine regionale Cybersicherheitsübung. An der regionalen Cybersicherheitsübung nehmen die Einrichtungen mit kritischen Auswirkungen teil. ENTSO-E kann in Zusammenarbeit mit der EU-VNBO innerhalb desselben Zeitrahmens anstelle einer regionalen Cybersicherheitsübung eine überregionale Cybersicherheitsübung in mehr als einer Netzbetriebsregion organisieren. Bei der Übung sollten andere vorhandene Risikobewertungen und Szenarien für die Cybersicherheit, die auf Unionsebene entwickelt wurden, berücksichtigt werden.

(2) Die ENISA unterstützt ENTSO-E und die EU-VNBO bei der Vorbereitung und Organisation der Cybersicherheitsübung auf regionaler oder überregionaler Ebene.

(3) ENTSO-E unterrichtet in Abstimmung mit der EU-VNBO die Einrichtungen mit kritischen Auswirkungen, die an der regionalen oder überregionalen Cybersicherheitsübung teilnehmen müssen, sechs Monate vor der Übung.

(4) Der Organisator einer regelmäßigen Cybersicherheitsübung auf Unionsebene gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 oder einer obligatorischen Cybersicherheitsübung in Bezug auf den Elektrizitätssektor innerhalb desselben geografischen Perimeters kann ENTSO-E und die EU-VNBO zur Teilnahme einladen. In diesen Fällen gilt die Verpflichtung nach Absatz 1 nicht, sofern alle Einrichtungen mit kritischen Auswirkungen in der Netzbetriebsregion an derselben Übung teilnehmen.

(5) Nehmen ENTSO-E und die EU-VNBO an einer Cybersicherheitsübung gemäß Absatz 4 teil, so können sie die in Absatz 1 genannte regionale oder überregionale Cybersicherheitsübung um ein Jahr verschieben.

(6) Bis zum 31 Dezember 2027 und danach alle drei Jahre stellt ENTSO-E in Abstimmung mit der EU-VNBO ein Muster für die Durchführung der regionalen und überregionalen Cybersicherheitsübungen bereit. Das Muster muss den Ergebnissen der jüngsten Bewertung des Cybersicherheitsrisikos auf regionaler Ebene Rechnung tragen und zentrale Leistungskriterien enthalten. In Bezug auf die Organisation und Durchführung der regionalen und überregionalen Cybersicherheitsübungen konsultiert ENTSO-E die Kommission und kann den Rat der ACER, der ENISA und der Gemeinsamen Forschungsstelle einholen.

Artikel 45 Ergebnisse von Cybersicherheitsübungen auf regionaler oder überregionaler Ebene oder auf der Ebene von Einrichtungen oder Mitgliedstaaten

(1) Auf Ersuchen einer Einrichtung mit kritischen Auswirkungen nehmen die Anbieter kritischer Dienste an den in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen teil, wenn sie Dienste für die Einrichtung mit kritischen Auswirkungen in dem Bereich erbringen, der dem Anwendungsbereich der betreffenden Cybersicherheitsübung entspricht.

(2) Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen analysieren und beenden die einschlägigen Cybersicherheitsübungen mit einem an alle Teilnehmer gerichteten Bericht, in dem die gewonnenen Erkenntnisse zusammengefasst werden, wobei sie bei der ENISA gemäß Artikel 7 Absatz 5 der Verordnung (EU) 2019/881 Rat einholen können. Der Bericht muss Folgendes enthalten:

a) die Übungsszenarien, Sitzungsberichte, wichtigsten Standpunkte, Erfolge und Erkenntnisse auf allen Ebenen der Elektrizitätswertschöpfungskette;

b) die Angabe, ob die wichtigsten Leistungskriterien erfüllt wurden;

c) eine Liste von Empfehlungen für Einrichtungen, die an der einschlägigen Cybersicherheitsübung teilnehmen, in

Bezug auf eine Korrektur, Anpassung oder Änderung von Cybersicherheitskrisenprozessen, -verfahren, zugehörigen Governance-Modellen und etwaigen bestehenden vertraglichen Verpflichtungen mit Anbietern kritischer Dienste.

(3) Auf Ersuchen des CSIRTs-Netzes, der NIS-Kooperationsgruppe oder des EU-CyCLONe leiten die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen die Ergebnisse der einschlägigen Cybersicherheitsübung weiter. Die Organisatoren teilen jeder an den Übungen teilnehmenden Einrichtung die in Absatz 2 Buchstaben a und b dieses Artikels genannten Informationen mit. Die Organisatoren übermitteln die Liste der in Absatz 2 Buchstabe c genannten Empfehlungen ausschließlich an die Einrichtungen, an die sich die Empfehlungen richten.

(4) Die Organisatoren der in Artikel 43 Absätze 1 und 2 und in Artikel 44 Absatz 1 genannten Cybersicherheitsübungen treffen mit den an den Übungen teilnehmenden Einrichtungen regelmäßig Folgemaßnahmen in Bezug auf die Umsetzung der Empfehlungen gemäß Absatz 2 Buchstabe c des vorliegenden Artikels.

Kapitel VII – Schutz von Informationen

Artikel 46 Grundsätze für den Schutz ausgetauschter Informationen

(1) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen nur nach dem Grundsatz „Kenntnis nur, wenn nötig“ und im Einklang mit den einschlägigen Vorschriften der Union und der Mitgliedstaaten über die Informationssicherheit zugänglich sind.

(2) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass die im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen während des gesamten Lebenszyklus dieser Informationen entsprechend behandelt und nachverfolgt werden und dass sie am Ende ihres Lebenszyklus erst dann freigegeben werden, wenn sie anonymisiert wurden.

(3) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass alle erforderlichen Schutzmaßnahmen organisatorischer und technischer Art getroffen werden, um die Vertraulichkeit, Integrität, Verfügbarkeit und Nichtabstreitbarkeit der im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen, unabhängig von den dabei genutzten Mitteln, zu wahren und zu schützen. Die Schutzmaßnahmen müssen

a) verhältnismäßig sein;

b) Cybersicherheitsrisiken im Zusammenhang mit bekannten früheren und sich abzeichnenden Bedrohungen Rechnung tragen, denen die Informationen im Zusammenhang mit dieser Verordnung ausgesetzt sein könnten;

c) soweit möglich auf nationalen, europäischen oder internationalen Normen und bewährten Verfahren beruhen;

d) dokumentiert werden.

(4) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass jede Person, der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen gewährt wird, über die auf Ebene der Einrichtungen geltenden Sicherheitsvorschriften sowie über die für den Schutz von Informationen relevanten Maßnahmen und Verfahren unterrichtet wird. Die Einrichtungen stellen sicher, dass die betroffene Person die Zuständigkeit anerkennt, die Informationen nach den in der Unterrichtung erteilten Anweisungen zu schützen.

(5) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen stellen sicher, dass der Zugang zu den im Rahmen dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen auf Personen beschränkt wird,

a) die aufgrund ihrer Funktionen, und beschränkt auf die Ausführung der ihnen übertragenen Aufgaben, zum Zugang zu diesen Informationen berechtigt sind;

b) in Bezug auf die die Einrichtung ethische Grundsätze und Integritätsgrundsätze prüfen konnte und für die es keine Hinweise auf ein negatives Ergebnis einer Zuverlässigkeitsüberprüfung gibt, mit der die Zuverlässigkeit der Person im Einklang mit bewährten Verfahren und den Standardsicherheitsanforderungen der Einrichtung und erforderlichenfalls mit den nationalen Gesetzen und Vorschriften bewertet wurde.

(6) Die in Artikel 2 Absatz 1 aufgeführten Einrichtungen bedürfen der schriftlichen Zustimmung der natürlichen oder juristischen Person, die die Informationen ursprünglich erstellt oder bereitgestellt hat, bevor sie diese Informationen an Dritte weitergeben, die nicht in den Anwendungsbereich dieser Verordnung fallen.

(7) Eine in Artikel 2 Absatz 1 aufgeführte Einrichtung kann der Ansicht sein, dass diese Informationen ohne Einhaltung der Absätze 1 und 4 des vorliegenden Artikels weitergegeben werden müssen, um eine zeitgleich auftretende Stromversorgungskrise mit einer zugrunde liegenden Cybersicherheitsursache oder eine grenzüberschreitende Krise innerhalb der Union in einem anderen Sektor zu verhindern. In diesem Fall

a) konsultiert sie die zuständige Behörde und kann von ihr zur Weitergabe dieser Informationen ermächtigt werden;

b) anonymisiert sie diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren;

c) schützt sie die Identität des Urhebers und der Einrichtungen, die diese Informationen im Rahmen dieser Verordnung verarbeitet haben.

(8) Abweichend von Absatz 6 des vorliegenden Artikels können die zuständigen Behörden Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder übermittelt werden, einem nicht in Artikel 2 Absatz 1 aufgeführten

Dritten bereitstellen, ohne dass der Urheber der Informationen schriftlich zugestimmt hat, müssen diesen jedoch so bald wie möglich davon in Kenntnis setzen. Bevor die betreffende zuständige Behörde Informationen, die im Rahmen dieser Verordnung bereitgestellt, empfangen, ausgetauscht oder übermittelt wurden, einem nicht in Artikel 2 Absatz 1 aufgeführten Dritten offenlegt, muss sie in angemessenem Umfang sicherstellen, dass der betreffende Dritte Kenntnis von den geltenden Sicherheitsvorschriften hat, und hinreichende Gewähr dafür erhalten, dass der betreffende Dritte die empfangenen Informationen gemäß den Absätzen 1 bis 5 des vorliegenden Artikels schützen kann. Die zuständige Behörde anonymisiert diese Informationen, ohne dass die Elemente verloren gehen, die erforderlich sind, um die Öffentlichkeit über ein unmittelbares und ernstes Risiko für grenzüberschreitende Stromflüsse und mögliche Abhilfemaßnahmen zu informieren, und schützt die Identität des Urhebers der Informationen. In diesem Fall schützt der nicht in Artikel 2 Absatz 1 aufgeführte Dritte die empfangenen Informationen gemäß den auf Ebene der Einrichtung bereits geltenden Bestimmungen oder, wenn dies nicht möglich ist, nach den Bestimmungen und Anweisungen der jeweils zuständigen Behörde.

(9) Dieser Artikel gilt nicht für Einrichtungen, die nicht in Artikel 2 Absatz 1 aufgeführt sind, wenn sie Informationen gemäß Absatz 6 des vorliegenden Artikels erhalten. In diesem Fall ist Absatz 7 anzuwenden, oder die zuständige Behörde kann dieser Einrichtung schriftliche Bestimmungen bereitstellen, die in Fällen anzuwenden sind, in denen Informationen gemäß dieser Verordnung eingehen.

Artikel 47 Vertraulichkeit von Informationen

(1) Alle gemäß dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen unterliegen dem Berufsgeheimnis gemäß den Absätzen 2 bis 5 dieses Artikels sowie den Anforderungen aus Artikel 65 der Verordnung (EU) 2019/943. Alle von den in Artikel 2 dieser Verordnung aufgeführten Einrichtungen für die Zwecke der Durchführung dieser Verordnung bereitgestellten, empfangenen, ausgetauschten oder übermittelten Informationen werden unter Berücksichtigung des vom Urheber angewandten Vertraulichkeitsgrads der Informationen geschützt.

(2) Die in Artikel 2 aufgeführten Einrichtungen unterliegen der Verpflichtung zur Wahrung des Berufsgeheimnisses.

(3) Die CS-NCAs, die NRB, die RP-NCA und die CSIRTs tauschen alle für die Wahr-

nehmung ihrer Aufgaben erforderlichen Informationen aus.

(4) Alle von den in Artikel 2 Absatz 1 aufgeführten Einrichtungen für die Zwecke der Durchführung von Artikel 23 empfangenen, ausgetauschten oder übermittelten Informationen werden anonymisiert und aggregiert.

(5) Informationen, die eine dieser Verordnung unterliegende Einrichtung oder Behörde im Rahmen der Erfüllung ihrer Pflichten erhält, dürfen an keine andere Einrichtung oder Behörde weitergegeben werden; davon unberührt bleiben Fälle, die unter das nationale Recht, andere Bestimmungen dieser Verordnung oder andere einschlägige Unionsvorschriften fallen.

(6) Unbeschadet des nationalen Rechts und des Unionsrechts dürfen Behörden, Einrichtungen oder natürliche Personen, die Informationen gemäß dieser Verordnung erhalten, diese für keinen anderen Zweck als für die Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung verwenden.

(7) Die ACER gibt nach Konsultation der ENISA, aller zuständigen Behörden, von ENTSO-E und der EU-VNBO bis zum 13 Juni 2025 Leitlinien für alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen zu Mechanismen für den Austausch von Informationen und insbesondere zu den geplanten Kommunikationsflüssen und Methoden zur Anonymisierung und Aggregierung von Informationen für die Zwecke der Durchführung des vorliegenden Artikels heraus.

(8) Nach nationalem Recht oder Unionsrecht vertrauliche Informationen werden nur dann mit der Kommission und anderen zuständigen Behörden ausgetauscht, wenn ein solcher Austausch für die Anwendung dieser Verordnung erforderlich ist. Die auszutauschenden Informationen werden auf den für den Zweck dieses Informationsaustauschs erforderlichen und verhältnismäßigen Umfang beschränkt. Beim Informationsaustausch wird die Vertraulichkeit der Informationen gewahrt und die Sicherheit sowie die geschäftlichen Interessen von Einrichtungen mit kritischen oder erheblichen Auswirkungen werden geschützt.

Kapitel VIII - Schlussbestimmungen

Artikel 48 Übergangsbestimmungen

(1) Bis zur Genehmigung der Modalitäten oder Methoden gemäß Artikel 6 Absatz 2 oder der Pläne gemäß Artikel 6 Absatz 3 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unverbindliche Leitlinien zu folgenden Themen:

a) einem vorläufigen Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor (im Folgenden „ECII“) gemäß Absatz 2;

b) einer vorläufigen Liste der unionsweiten Prozesse mit erheblichen oder kritischen Auswirkungen gemäß Absatz 4 sowie

c) einer vorläufigen Liste europäischer und internationaler Normen und Kontrollen gemäß Absatz 6, die nach nationalen Rechtsvorschriften erforderlich und für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

(2) Bis zum 13 Oktober 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine Empfehlung für einen vorläufigen ECII. ENTSO-E teilt den zuständigen Behörden in Zusammenarbeit mit der EU-VNBO den empfohlenen vorläufigen ECII mit.

(3) Vier Monate nach Erhalt des empfohlenen vorläufigen ECII oder bis spätestens 13 Februar 2025 ermitteln die zuständigen Behörden auf der Grundlage des empfohlenen ECII Einrichtungen, die als Einrichtungen mit erheblichen oder kritischen Auswirkungen in ihrem Mitgliedstaat in Betracht kommen, und erstellen eine vorläufige Liste von Einrichtungen mit erheblichen oder kritischen Auswirkungen. Die in der vorläufigen Liste aufgeführten Einrichtungen mit erheblichen oder kritischen Auswirkungen können ihren in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip freiwillig nachkommen. Bis zum 13 März 2025 teilen die zuständigen Behörden den in der vorläufigen Liste aufgeführten Einrichtungen mit, dass sie als Einrichtung mit erheblichen oder kritischen Auswirkungen eingestuft wurden.

(4) Bis zum 13 Dezember 2024 erarbeitet ENTSO-E in Zusammenarbeit mit der EU-VNBO eine vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen. Die gemäß Absatz 3 unterrichteten Einrichtungen, die freiwillig beschließen, ihre in dieser Verordnung festgelegten Verpflichtungen nach dem Vorsorgeprinzip zu erfüllen, nutzen die vorläufige Liste von unionsweiten Prozessen mit erheblichen oder kritischen Auswirkungen, um vorläufige Perimeter mit erheblichen oder kritischen Auswirkungen zu bestimmen und um zu ermitteln, welche Vermögenswerte in die erste Bewertung des Cybersicherheitsrisikos auf Ebene der Einrichtung einzubeziehen sind.

(5) Bis zum 13 September 2024 übermittelt jede gemäß Artikel 4 Absatz 1 zuständige Behörde ENTSO-E und der EU-VNBO eine Liste ihrer nationalen Rechtsvorschriften, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

(6) Bis zum 13 Juni 2025 erstellt ENTSO-E in Zusammenarbeit mit der EU-VNBO unter Berücksichtigung der von den zuständigen Behörden bereitgestellten Informationen eine vorläufige Liste der nach nationalem Recht vorgeschriebenen europäischen und internationalen Normen und Kontrollen, die für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse relevant sind.

(7) Die vorläufige Liste der europäischen und internationalen Normen und Kontrollen muss Folgendes enthalten:

a) europäische und internationale Normen und nationale Rechtsvorschriften, die Leitlinien für Methoden für das

Risikomanagement im Bereich der Cybersicherheit auf Ebene der Einrichtungen enthalten, und

b) Cybersicherheitskontrollen, die denjenigen gleichwertig sind, die voraussichtlich Teil der Mindest-Cybersicherheitskontrollen und der erweiterten Cybersicherheitskontrollen sein werden.

(8) ENTSO-E und die EU-VNBO berücksichtigen bei der Fertigstellung der vorläufigen Liste von Normen die Stellungnahmen der ENISA und der ACER. ENTSO-E und die EU-VNBO veröffentlichen die vorläufige Liste der europäischen und internationalen Normen und Kontrollen auf ihren Websites.

(9) ENTSO-E und die EU-VNBO konsultieren die ENISA und die ACER zu den gemäß Absatz 1 erstellten Vorschlägen für unverbindliche Leitlinien.

(10) Bis die Mindest-Cybersicherheitskontrollen und die erweiterten Cybersicherheitskontrollen gemäß Artikel 29 entwickelt und gemäß Artikel 8 angenommen sind, bemühen sich alle in Artikel 2 Absatz 1 aufgeführten Einrichtungen, die gemäß Absatz 1 des vorliegenden Artikels erstellten unverbindlichen Leitlinien nach und nach anzuwenden.

Artikel 49 Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.