NISTify ENERGY

E-LEARNING COURSE

Einführung in die Umsetzung der NCCS-Verordnung

NIS2U GmbH

1.0.0 – 04/12/2025

Contents

Chapter 1

Einleitung

Der NCCS (Network Code on Cybersecurity), wie er in der DELEGIERTEN VERORDNUNG (EU) 2024/1366 DER KOMMISSION [1] festgelegt ist, zielt darauf ab, ein einheitliches Cybersicherheitsrahmenwerk innerhalb des europäischen Elektrizitätssektors zu schaffen, um die Sicherheit grenzüberschreitender Stromflüsse zu gewährleisten. Diese Verordnung legt einen Netzkodex fest, der **branchenspezifische Regeln für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse** festlegt, darunter Vorschriften zu gemeinsamen Mindestanforderungen, Planung, Überwachung, Berichterstattung und Krisenmanagement.

Der Network Code on Cybersecurity NCCS wurde am 24. Mai 2024 offiziell angenommen.

Die Verordnung trat unmittelbar nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Ziel dieses Materials ist es, den Akteuren des Elektrizitätssektors das Verständnis und die wirksame Anwendung der NCCS-Cybersicherheitsverordnung zu erleichtern.

1.1 Grundbegriffe des NCCS

Vor Beginn des Kursmaterials empfiehlt es sich, sich mit den Grundbegriffen vertraut zu machen. Diese Konzepte können in diesem Abschnitt nachgelesen werden und sind auch in den entsprechenden Teilen des Materials durch Klicken auf den jeweiligen Begriff zugänglich.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

1.1.1 A

TERM

Akkreditierung

Bestätigung durch eine nationale Akkreditierungsstelle, dass eine Konformitätsbewertungsstelle die in harmonisierten Normen festgelegten Anforderungen und, gegebenenfalls, zusätzliche Anforderungen, einschließlich solcher in relevanten sektoralen Akkreditierungssystemen, erfüllt, um eine spezielle Konformitätsbewertungstätigkeit durchzuführen.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008R0765

TERM

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Anbieter von verwalteten Sicherheitsdiensten

Bezeichnet einen Anbieter verwalteter Dienste, der Tätigkeiten im Zusammenhang mit dem Management von Cybersicherheitsrisiken durchführt oder dabei unterstützt.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Anbieter von verwalteten Diensten

Eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt. RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Ansprechpartner auf Organisationsebene (SPOC)

Bezeichnet den Ansprechpartner auf Organisationsebene, wie in Artikel 38 Absatz 1 Buchstabe c [a] benannt.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L_202401366&qid=1737539416885#art_38
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Assurance Level

Bezeichnet eine Vertrauensgrundlage dafür, dass ein IKT-Produkt, ein IKT-Dienst oder ein IKT-Prozess die Sicherheitsanforderungen eines bestimmten europäischen Cybersicherheitszertifizierungsschemas erfüllt; gibt das Niveau an, auf dem das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess bewertet wurde, misst jedoch nicht die tatsächliche Sicherheit des Produkts, Dienstes oder Prozesses.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

1.1.2 B

TERM

Behörden, die für das Management von Cyberkrisen zuständig sind

Bezeichnet Behörden, die gemäß Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2555 für das Management groß angelegter Cybersicherheitsvorfälle und -krisen (Cyberkrisenmanagement) benannt oder eingerichtet wurden. Die Mitgliedstaaten stellen sicher, dass diese Behörden über angemessene Ressourcen verfügen, um ihre Aufgaben wirksam und effizient wahrzunehmen, und dass Kohärenz mit bestehenden nationalen Krisenmanagementrahmen gewährleistet ist.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Beinahe-Vorfall

Ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist;

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

1.1.3 C

TERM

CER-Richtlinie

Am 14. Dezember 2022 hat die Europäische Union die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen angenommen und die Richtlinie 2008/114/EG des Rates aufgehoben.

RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557

TERM

Cyberangriff

Ein böswilliger IKT-bezogenen Vorfall, der auf den Versuch eines Angreifers zurückgeht, einen Vermögenswert zu zerstören, freizulegen, zu verändern, zu deaktivieren, zu entwenden oder auf unberechtigte Weise auf diesen Vermögenswert zuzugreifen oder ihn auf un-

berechtigte Weise zu nutzen.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Cyberbedrohung

Bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

TERM

Cybersicherheit

Bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

TERM

Cybersicherheitsmaßnahme

Bezeichnet Maßnahmen oder Verfahren, die durchgeführt werden, um Cybersicherheitsrisiken zu vermeiden, zu erkennen, entgegenzuwirken oder zu minimieren.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Cybersicherheitsoperationszentrum, Betriebszentrum für Cybersicherheit (CSOC)

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

1.1.4 E

TERM

Einrichtung mit erheblichen Auswirkungen

Bezeichnet eine Einrichtung, die einen Prozess mit erheblichen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 [a] ermittelt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Einrichtung mit kritischen Auswirkungen

Bezeichnet eine Einrichtung, die einen Prozess mit kritischen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 [a] bestimmt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Erhebliche Cyberbedrohung

Eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Erheblicher Cybersicherheitsvorfall großen Ausmaßes

Bezeichnet einen Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Europäisches Cybersicherheitszertifizierungsschema

Bezeichnet ein umfassendes Regelwerk aus Vorschriften, technischen Anforderungen, Normen und Verfahren, das auf Unionsebene festgelegt wird und für die Zertifizierung oder Konformitätsbewertung bestimmter IKT-Produkte, IKT-Dienstleistungen oder IKT-Prozesse gilt.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

1.1.5 F

TERM

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

1.1.6 G

TERM

Grenzüberschreitender Stromfluss

Bezeichnet das physikalische Durchströmen einer Menge elektrischer Energie durch ein Übertragungsnetz eines Mitgliedstaats aufgrund der Auswirkungen der Tätigkeit von Erzeugern oder Kunden oder beiden außerhalb dieses Mitgliedstaats auf dessen Übertragungsnetz.

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02019R0943-20240716

1.1.7 I

TERM

Initiator

Bezeichnet eine Organisation, die ein Ereignis des Informationsaustauschs, der Informationsweitergabe oder der Informationsspeicherung einleitet.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

IKT

Informations- und Kommunikationstechnologie.

TERM

IKT-Dienstleistung

Bezeichnet einen Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

TERM

IKT-Prozess

Bezeichnet jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

TERM

IKT-Produkt

Bezeichnet ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

TERM

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. DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

IKT-Altsystem

Bezeichnet ein Produkt, das das Ende seines Lebenszyklus (Ende seiner Lebensdauer) erreicht hat, aus technologischen oder wirtschaftlichen Gründen nicht für Upgrades oder Fehlerbehebungen in Frage kommt oder nicht mehr von seinem Anbieter oder einem IKT-Drittdienstleister unterstützt wird, das allerdings weiterhin genutzt wird und die Funktionen des Finanzunternehmens unterstützt.

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554

TERM

Interessenträger

Bezeichnet jede Partei, die ein Interesse am Erfolg und an der kontinuierlichen Funktionsweise einer Organisation oder eines Prozesses hat, wie z. B. Mitarbeitende, Direktoren, Anteilseigner, Regulierungsbehörden, Verbände, Lieferanten und Kunden.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

1.1.8 K

TERM

Konformitätsbewertung

Bezeichnet das Verfahren zur Bewertung, ob spezifische Anforderungen an ein Produkt, ein Verfahren, eine Dienstleistung, ein System, eine Person oder eine Stelle erfüllt sind.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02008R0765-20210716

TERM

Konformitätsbewertungsstelle

Eine Stelle, die Konformitätsbewertungstätigkeiten einschließlich Kalibrierungen, Prüfungen, Zertifizierungen und Inspektionen durchführt.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02008R0765-20210716

1.1.9 M

TERM

Mitgliedstaat

Bezeichnet ein Land, das Mitglied der Europäischen Union ist und das EU-Recht einhält.

1.1.10 N

TERM

Nationale Akkreditierungsstelle

Die einzige Stelle in einem Mitgliedstaat, die im Auftrag dieses Staates Akkreditierungen durchführt.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02008R0765-20210716

TERM

Nationale zentrale Anlaufstelle

Bezeichnet die von jedem Mitgliedstaat gemäß Artikel 8 Absatz 3 der RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a] benannte oder eingerichtete Anlaufstelle.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Netz- und Informationssystem

Bezeichnet:

Artikel 6 Nummer 1: . ein elektronisches Kommunikationsnetz gemäß Artikel 2 Nummer 1 der Richtlinie (EU) 2018/1972; . ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, von denen eines oder mehrere aufgrund eines Programms eine automatische Verarbeitung digitaler Daten durchführen; oder . digitale Daten, die von den unter den Buchstaben a und b genannten Elementen gespeichert, verarbeitet, abgerufen oder übertragen werden, zum Zweck ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Wartung;

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Normen

Bezeichnet eine von einer anerkannten Normungsorganisation angenommene technische Spezifikation zur wiederholten oder kontinuierlichen Anwendung, deren Einhaltung nicht verbindlich ist. VERORDNUNG (EU) Nr. 1025/2012 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012R1025

1.1.11 O

TERM

Organisation

Bezeichnet eine natürliche oder juristische Person, die nach dem nationalen Recht ihres Sitzstaates gegründet und als solche anerkannt ist und in eigenem Namen Rechte ausüben und Verpflichtungen eingehen kann.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

OT (Operational Technology)

OT ist die Kombination aus Produktionsautomatisierung, Maschine-zu-Maschine-Kommunikation und Datenerfassung.

1.1.12 P

TERM

Perimeter mit erheblichen Auswirkungen

Bezeichnet einen von einer der in Artikel 2 Absatz 1 [a] 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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_2
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Perimeter mit kritischer Auswirkung

Bezeichnet einen von einer in Artikel 2 Absatz 1 [a] genannten Stelle definierten Perimeter, der alle Anlagen mit kritischer Auswirkung umfasst, auf die der Zugang kontrolliert werden kann und der den Geltungsbereich definiert, in dem fortgeschrittene Cybersicherheitsmaß-

nahmen gelten.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [b]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_2
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Prozess mit kritischer Auswirkungen

Bezeichnet einen Geschäftsprozess, der von einer Stelle durchgeführt wird, für den die Indizes zur Bewertung der Auswirkungen auf die Cybersicherheit im Elektrizitätsbereich über dem Schwellenwert für kritische Auswirkungen liegen.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

1.1.13 R

TERM

Risiko

Das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen

Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Risikoauswirkungsmatrix

Bezeichnet eine Matrix, die bei der Risikobewertung genutzt wird, um für jedes bewertete Risiko die mit ihm verbundenen Auswirkungen zu bestimmen.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

1.1.14 S

TERM

Schwachstelle

Eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Schwachstellenmanagement im Bereich der Cybersicherheit

Im Bereich der Cybersicherheit“ bezeichnet die Praxis, Schwachstellen zu ermitteln und zu beheben.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Selbstbewertung der Konformität

Bezeichnet eine Maßnahme eines Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Bewertung, ob diese IKT- Produkte, -Dienste oder -Prozesse die Anforderungen, die in einem spezifischen europäischen Schema für die Cybersicherheitszertifizierung festgelegt sind, erfüllen.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881

TERM

Sicherheit von Netz- und Informationssystemen

Die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Spezifikationen für die Auftragsvergabe

Bezeichnet die von Einrichtungen für die Beschaffung neuer oder aktualisierter IKT-Produkte, -Prozesse oder -Dienste festgelegten Spezifikationen.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Stromversorgungskrise

Eine bestehende oder drohende Situation, die durch eine im Sinne der Vorgaben der Mitgliedstaaten und der Beschreibung in ihren Risikovorsorgeplänen erhebliche Stromknappheit oder durch die Unmöglichkeit, Kunden mit Strom zu versorgen, gekennzeichnet ist.

VERORDNUNG (EU) 2019/941 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0941

TERM

Systembetriebsregion

Bezeichnet die Systembetriebsregionen gemäß Anhang I des ACER-Beschlusses 05-2022 über die Definition von Systembetriebsregionen, die gemäß Artikel 36 der Verordnung (EU) 2019/943 eingerichtet wurden.

1.1.15 T

TERM

Technische Spezifikation

Bezeichnet ein Dokument, das technische Anforderungen vorschreibt, die von einem Produkt, einem Prozess, einer Dienstleistung oder einem System erfüllt werden müssen, und das eine oder mehrere der folgenden Festlegungen enthält.

VERORDNUNG (EU) Nr. 1025/2012 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012R1025

1.1.16 U

TERM

Unionsweiter Prozess mit kritischer Auswirkung

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Unionsweiter Prozess mit hoher Auswirkung

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

1.1.17 V

TERM

Vertreter

Eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines DNS-Diensteanbieters, einer Einrichtung, die Domänennamen-Registrierungsdienste erbringt, eines TLD-Namenregisters, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen, eines Anbieters verwalteter Dienste, eines Anbieters verwalteter Sicherheitsdienste oder eines Anbieters von einem Online-Marktplatz, von einer Online-Suchmaschine oder von einer Plattform für Dienste sozialer Netzwerke, der bzw. die nicht in der Union niedergelassen ist, zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT — statt an die Einrichtung — hinsichtlich der Pflichten dieser Einrichtung gemäß dieser Richtlinie wenden kann.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Vermögenswerte

Eine Software oder Hardware in den Netzwerk- und Informationssystemen, die das Finanzunternehmen nutzt.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

TERM

Vermögenswert mit erheblichen Auswirkungen

Bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit erheblichen Auswirkungen erforderlich ist. DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Vermögenswert mit kritischen Auswirkungen

Bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit kritischen Auswirkungen erforderlich ist. DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

TERM

Vorfall

Bezeichnet ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übertragenen oder verarbeiteten Daten oder von über Netz- und Infor-

mationssysteme angebotenen oder zugänglichen Diensten beeinträchtigt.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

TERM

Vorfallbehandlung

Bezeichnet alle Maßnahmen und Verfahren, die darauf abzielen, Vorfälle zu verhindern, zu erkennen, zu analysieren, einzudämmen oder auf sie zu reagieren und sich davon zu erholen.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

1.1.18 Z

TERM

Zuordnungsmatrix

Erarbeitet gemäß Artikel 34 der DELEGIERTEN VERORDNUNG (EU) 2024/1366 DER KOMMISSION [a], zur Zuordnung der in den Buchstaben a und b genannten Kontrollen zu ausgewählten europäischen und internationalen Normen sowie nationalen gesetzlichen oder regulatorischen Rahmenwerken.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_34

1.2 Beteiligte Akteure im Zusammenhang mit der NCCS

Im Laufe des Kurses werden Sie auf verschiedene Akteure stoßen, die an der Umsetzung der NCCS-Verordnung beteiligt sind. Es ist ratsam, sich vor Beginn mit diesen Akteuren vertraut zu machen.

1.2.1 A

TERM

Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)

Eine spezialisierte Agentur der Europäischen Union, die für die Förderung der Integration und des effizienten Funktionierens der EU-Energiemärkte zuständig ist.

https://www.acer.europa.eu/ [a]

VERORDNUNG (EU) 2019/942 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [b]

[a] https://www.acer.europa.eu/
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942

TERM

Agentur der Europäischen Union für Cybersicherheit (ENISA)

ENISA ist die Cybersicherheitsagentur der EU und unterstützt die Mitgliedstaaten bei der Abwehr von Cyberbedrohungen.

1.2.2 B

TERM

Benannter Strommarktbetreiber (NEMO)

Ein Marktteilnehmer, der von der zuständigen Behörde eines Mitgliedstaats benannt wurde, um an der Kopplung des einheitlichen Day-Ahead-Markts oder des einheitlichen Intraday-Markts teilzunehmen.

1.2.3 C

TERM

Computer-Notfallteams (CSIRT)

Eine Organisation, die für das Management von Sicherheitsvorfällen in Netz- und Informationssystemen zuständig ist. RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

TERM

Cybersicherheit zuständigen Behörden (CS NCA)

Die nationale zuständige Behörde für Cybersicherheit in einem bestimmten Mitgliedstaat.

1.2.4 D

TERM

DG CONNECT (Generaldirektion Kommunikationsnetze, Inhalte und Technologien der Europäischen Kommission)

Die Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CONNECT) entwickelt und implementiert die politischen Maßnahmen der Europäischen Kommission.

TERM

DG ENER (Generaldirektion Energie der Europäischen Kommission)

Die Generaldirektion Energie der Europäischen Kommission ist für die Energiepolitik der EU verantwortlich.

1.2.5 E

TERM

EU-VNBO (EU DSO)

Europäische Organisation der Verteilnetzbetreiber

Die EU-VNBO wurde von der Europäischen Union gegründet, um die Koordinierung und Entwicklung der Stromverteilungsnetze zu fördern. Sie spielt eine zentrale Rolle bei der Integration der Energiemärkte, der Einbindung erneuerbarer Energiequellen und der Unterstützung der Energiewende.

Die Aktivitäten der EU-VNBO werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

https://eudsoentity.eu/ [a]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [b]

[a] https://eudsoentity.eu/
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

TERM

Europäische Kommission (EK)

Die Europäische Kommission ist das Exekutivorgan der Europäischen Union und verantwortlich für die Umsetzung der EU-Rechtsvorschriften, die Entwicklung von Politiken und die Verwaltung des Haushalts.

TERM

Elektrizitätskoordinierungsgruppe (EKG)

Ziel der Elektrizitätskoordinierungsgruppe ist es, Informationen über strompolitische Maßnahmen mit grenzüberschreitenden Auswirkungen auszutauschen und zu koordinieren und die Zusammenarbeit durch Wissens- und Erfahrungsaustausch zu erleichtern.

KOMMISSIONSENTSCHEIDUNG 2012/C 353/02 [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)

1.2.6 K

TERM

Kooperationsgruppe für Netz- und Informationssysteme (NIS CG)

Kooperationsgruppe für Cybersicherheit

Die Kooperationsgruppe für Netz- und Informationssicherheit (NIS CG) koordiniert die Cybersicherheitszusammenarbeit in der EU. Die Aufgaben der NIS-Kooperationsgruppe sind in Artikel 11 der NIS-Richtlinie festgelegt.

DURCHFÜHRUNGSBESCHLUSS (EU) 2017/179 DER KOMMISSION [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32017D0179

1.2.7 N

TERM

Nationale zuständige Behörde (NCA)

Eine nationale zuständige Behörde ist eine offizielle Stelle oder Organisation, die durch Rechtsvorschriften befugt ist, einen bestimmten Sektor oder Bereich zu regeln, zu überwachen und zu kontrollieren. Diese Behörden stellen die Einhaltung nationaler und gegebenenfalls internationaler Gesetze und Standards sicher.

TERM

Nationale Regulierungsbehörden (NRB)

Eine offizielle staatliche oder unabhängige Organisation, die für die Regulierung, Überwachung

und Kontrolle bestimmter Bereiche innerhalb eines Landes oder einer Region zuständig ist.

1.2.8 R

TERM

Risikovorsorge zuständigen Behörden (RP-NCA)

Die RP-NCA ist für die Entwicklung und Umsetzung von Risikovorsorgeplänen zuständig.

TERM

Regionale Koordinierungszentren (RCC)

Regionale Koordinierungszentren (RCC) haben eine beratende Rolle bei der Entwicklung regionaler Cybersicherheitsrisikobewertungen und -minderungspläne und koordinieren die Zusammenarbeit der Mitgliedstaaten im Bereich der Cybersicherheit.

Eingerichtet gemäß Artikel 35 der Verordnung (EU) 2019/943.

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

1.2.9 S

TERM

Systembetreiber

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Übertragungs- oder Verteilernetzes verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

1.2.10 Ü

TERM

Übertragungsnetzbetreiber (ÜNB)

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung des Übertragungsnetzes in einem bestimmten Gebiet sowie dessen Verbindung mit anderen Netzen und die langfristige Fähigkeit zur Deckung eines angemessenen Bedarfs an Stromübertragung verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

1.2.11 V

TERM

Verteilnetzbetreiber (DSO)

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Verteilernetzes in einem bestimmten Gebiet sowie für die langfristige Fähigkeit zur Deckung gerechtfertigter Stromverteilungsanforderungen verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944

TERM

Verband Europäischer Übertragungsnetzbetreiber (ENTSO-E)

Gemeinsame Organisation der europäischen Übertragungsnetzbetreiber. Sie spielt eine zentrale Rolle bei der Integration des europäischen Strommarktes und der Sicherstellung der Stabilität des Stromsystems.

Die Aktivitäten von ENTSO-E werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

https://www.entsoe.eu/ [a]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [b]

[a] https://www.entsoe.eu/
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

Chapter 2

Allgemeine Einführung

Der Netzkodex zur Cybersicherheit [1] ist eine entscheidende Verordnung zur Gewährleistung der Cybersicherheit grenzüberschreitender Stromflüsse innerhalb der Europäischen Union. Ziel dieses Kapitels ist es, einen Überblick über die Verordnung Cybersicherheit, ihre Notwendigkeit und ihren Hintergrund zu geben. Sie erfahren, warum diese Verordnung im Elektrizitätssektor von entscheidender Bedeutung ist, welche Organisationen unter ihren Anwendungsbereich fallen und welche Behörden für ihre Umsetzung verantwortlich sind.

2.1 Warum ist die Verordnung zur Cybersicherheit notwendig?

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

NOTE

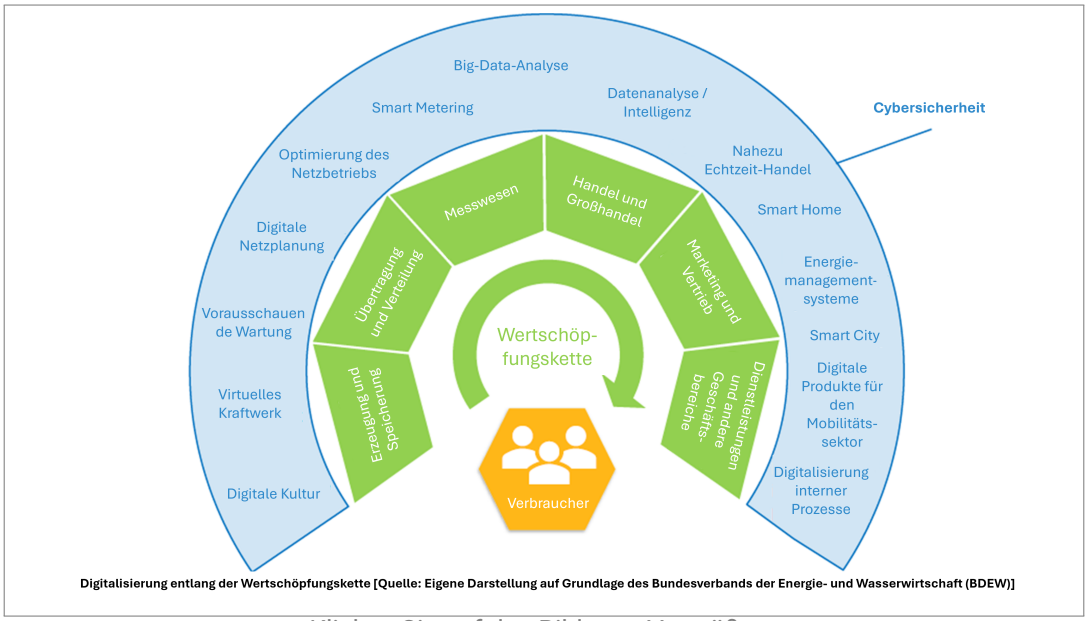
Die Untertitel des Videos wurden mit KI-gestützten Werkzeugen generiert, daher können Fehler enthalten sein.

Die NCCS ist von grundlegender Bedeutung für die europäischen Bürgerinnen und Bürger sowie für Unternehmen.

Dafür gibt es mehrere Gründe:

- Elektrizität ist lebenswichtig für die europäischen Bürger und Unternehmen.
- Der Elektrizitätssektor in der Union befindet sich in einem **tiefgreifenden Wandel**, gekennzeichnet durch zunehmend dezentralisierte Märkte mit einer größeren Anzahl von Akteuren, einem höheren Anteil an Energie aus erneuerbaren Quellen sowie stärker digitalisierten und vernetzten Systemen.
- Das **integrierte europäische Stromnetz** ist einzigartig, da es den nahtlosen Stromtransfer über mehrere Länder hinweg ermöglicht und so die Energiesicherheit, Effizienz und Integration erneuerbarer Energien verbessert. Eine Netzkarte der EU finden Sie hier: Grid Map [2]
- Europa verfolgt das klare Ziel eines **vollständig integrierten Binnenmarkts für Energie**, der einen diskriminierungsfreien Zugang sowohl für bestehende als auch neue Marktteilnehmer gewährleistet und den grenzüberschreitenden Energiehandel erleichtert.
- **Digitalisierung** und Cybersicherheit sind entscheidend für die Erbringung grundlegender Dienste und daher von strategischer Bedeutung für kritische Energieinfrastrukturen.
- **Digitalisierung bringt erhebliche Risiken** mit sich, da eine zunehmende Angriffsfläche für Cyberangriffe und Vorfälle im Bereich Cybersicherheit die Versorgungssicherheit und den Datenschutz von Verbraucherinnen und Verbrauchern gefährden kann. Die Digitalisierung des Energiesektors hat ihren Preis: erhöhte Anfälligkeit gegenüber Cybervorfällen und Angriffen. Allgegenwärtige Konnektivität und Datenerfassung verstärken den bereits bestehenden Bedarf an Datensicherheit — sei es für Kunden, Systeme oder Vermögenswerte. Viele Energieanlagen sind seit Jahrzehnten in Betrieb, in Zeiten, in denen keine vernetzte Kommunikation vorgesehen war, nur rein überwachend agiert wurde oder zumindest spezifisch für den jeweiligen Anwendungszweck entwickelt wurden.

[2] https://www.entsoe.eu/data/map/



Digitalisierung entlang der Wertschöpfungskette [Quelle: Eigene Darstellung auf Grundlage des Bundesverbands der Energie- und Wasserwirtschaft (BDEW)]

Klicken Sie auf das Bild zum Vergrößern

GOOD TO KNOW

Die NCCS ergänzt und erweitert die Richtlinie NIS 2 um sektorspezifische Anforderungen an die Cybersicherheit und bietet präzisere Anweisungen und Verfahren.

Ziel der NCCS ist es, einen **umfassenden und einheitlichen Rahmen zur Cybersicherheit** für den europäischen **Stromsektor** zu schaffen, der für die **Sicherheit und Zuverlässigkeit** der OT- und IT-Systeme im digitalen Zeitalter unerlässlich ist. Dadurch wird die Sicherheit der **grenzüberschreitenden Stromversorgung** gewährleistet.

Diese Verordnung wurde in enger Zusammenarbeit mit ACER, ENISA, dem Verband ENTSO für Strom, der EU-VNBO-Organisation und anderen Interessenträgern ausgearbeitet, um ausgewogene, wirksame und verhältnismäßige Regeln auf transparente und partizipative Weise zu erlassen.

2.2 Rechtsvorschriften

?**Netzkodex zur Cybersicherheit (NCCS)**

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 Netzkodexes mit sektorspezifischen Vorschriften für die Cybersicherheit grenzüberschreitender Stromflüsse [a]

Am 13. Juni 2024 trat die Verordnung der Kommission zur Schaffung eines europäischen Rahmens für die Cybersicherheit grenzüberschreitender Stromflüsse in Kraft.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366

?**Rechtsvorschrift zur Cybersicherheit**

- RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein erlebliches 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) [3]

?**Rechtsvorschrift zur Resilienz kritischer Einrichtungen**

- 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 [4]

?**Weitere relevante Rechtsvorschriften**

- VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt [5]
- VERORDNUNG (EU) 2019/941 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 5. Juni 2019 über die Gewährleistung der Versorgungssicherheit im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG [6]
- VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019 über ENISA (die Agentur der Europäischen Union für Cybersicherheit) und über Zertifizierungsanforderungen für die Cybersicherheit der Informations- und Kommunikationstechnologie sowie zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Cybersicherheitsgesetz) [7]
- VERORDNUNG (EU) Nr. 1025/2012 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. Oktober 2012 über die europäische Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates und 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 sowie zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates [8]

[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0943
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0941
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012R1025

- VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 9. Juli 2008 über Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates [9]
- VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die digitale operationelle Resilienz des Finanzsektors 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 [10]

2.3 Welche Aspekte der Cybersicherheit deckt die NCCS ab?

Die NCCS ist eine umfassende Verordnung, die mehrere Aspekte der Cybersicherheit im Elektrizitätssektor abdeckt. Zu den wichtigsten Bereichen gehören:

1. Risikobewertung im Bereich Cybersicherheit

Die Risikobewertung ist eine der zentralen Säulen der NCCS. Das Cybersicherheits-Risikomanagement im Rahmen der NCCS-Verordnung erfordert ein strukturiertes Verfahren, das unter anderem die Identifizierung von Risiken umfasst, die sich aus Cyberangriffen auf grenzüberschreitende Stromflüsse ergeben, sowie die zugehörigen betrieblichen Prozesse und deren Geltungsbereiche, einschließlich geeigneter Sicherheitskontrollen und Authentifizierungsmechanismen. **Die Risikobewertung erfolgt regelmäßig auf EU-, regionaler, nationaler und Organisationsebene.** Der in verschiedenen Bestimmungen dargelegte risikobasierte Ansatz dient der Identifizierung von Prozessen, unterstützenden Vermögenswerten und deren betreibenden Organisationen, die Auswirkungen auf grenzüberschreitende Stromflüsse haben. Je nachdem, in welchem Maße potenzielle Cyberangriffe die Tätigkeiten dieser Organisationen in Bezug auf grenzüberschreitende Stromflüsse beeinträchtigen, können sie als Organisationen mit erheblicher Auswirkung oder kritischer Auswirkung eingestuft werden. Die Mitgliedstaaten sind dafür verantwortlich, Organisationen zu identifizieren, die die Qualifikationskriterien für Organisationen mit erheblicher und kritischer Auswirkung erfüllen, durch die zuständige Behörde gemäß der NCCS-Verordnung.

Die Risikobewertungen im Bereich Cybersicherheit auf EU-, nationaler, regionaler und Organisationsebene können gemäß der NCCS-Verordnung auf Risiken beschränkt sein, die sich aus Cyberangriffen im Sinne der VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [11] ergeben. Dementsprechend können Risiken im Zusammenhang mit physischen Angriffen, Naturkatastrophen und Betriebsunterbrechungen durch Anlagen- oder Personalausfälle ausgeschlossen sein.

Die Bestimmungen der NCCS-Verordnung berühren nicht das Unionsrecht, das spezifische Vorschriften über die Zertifizierung von Informations- und Kommunikationstechnologieprodukten, -diensten und -prozessen enthält, insbesondere im Hinblick auf den Rahmen zur Einrichtung europäischer Cybersicherheitszertifizierungsregelungen, wie in der VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [12] festgelegt.

[9] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008R0765
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2554
[12] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019R0881

2. Gemeinsamer Rahmen für die Cybersicherheit im Strombereich

Zur Minderung von Cybersicherheitsrisiken ist es erforderlich, ein detailliertes Regelwerk für das Vorgehen und die Zusammenarbeit relevanter Akteure zu schaffen, deren Tätigkeiten mit Aspekten der Cybersicherheit grenzüberschreitender Stromflüsse zusammenhängen, um die Systemsicherheit zu gewährleisten. Diese organisatorischen und technischen Vorschriften sollen sicherstellen, dass die meisten Vorfälle mit Ursachen im Bereich Cybersicherheit auf operativer Ebene wirksam behandelt werden können. Es muss festgelegt werden, welche Maßnahmen diese Akteure ergreifen sollen, um solche Krisen zu vermeiden, und welche Maßnahmen möglich sind, falls die Systembetriebsregeln allein nicht mehr ausreichen. **Daher ist es notwendig, einen gemeinsamen Regelungsrahmen festzulegen, um gleichzeitige Stromkrisen mit Ursachen im Bereich Cybersicherheit zu verhindern, sich darauf vorzubereiten und sie zu bewältigen.** Dies erhöht die Transparenz in der Vorbereitungsphase und während einer gleichzeitigen Stromkrise und gewährleistet, dass Maßnahmen in koordinierter und wirksamer Weise gemeinsam mit den zuständigen Cybersicherheitsbehörden der Mitgliedstaaten ergriffen werden.

3. Informationsaustausch

Da die Ausnutzung von Schwachstellen in Netz- und Informationssystemen zu erheblichen Störungen der Energieversorgung und schweren wirtschaftlichen Schäden für Verbraucher führen kann, müssen diese Schwachstellen schnell erkannt und beseitigt werden, um Risiken zu minimieren. Zur wirksamen Umsetzung der NCCS-Verordnung müssen relevante Organisationen und zuständige Behörden in geeigneten praktischen und Testaktivitäten zusammenarbeiten. Dazu gehört der Austausch von Informationen über Cyberbedrohungen, Cyberangriffe, Schwachstellen, Vermögenswerte sowie Methoden, Taktiken, Techniken und Verfahren, über die Vorbereitung auf Krisenfälle im Bereich Cybersicherheit und über andere Übungen. **Die Verordnung legt den Umfang meldepflichtiger Cyberangriffe, Bedrohungen und Schwachstellen sowie die Regeln für den Informationsaustausch und Vertraulichkeitspflichten fest.**

4. Sicherheit der Lieferkette

Jüngste Cyberangriffe zeigen, dass Organisationen zunehmend Ziel von Angriffen auf die Lieferkette werden. Solche Angriffe betreffen nicht nur einzelne Organisationen innerhalb des Anwendungsbereichs, sondern können auch kaskadierende Effekte auf andere Organisationen im Stromnetz haben, mit denen sie verbunden sind.

Auf Grundlage der Verordnung werden Mindestanforderungen und fortgeschrittene Cybersicherheitskontrollen sowie Beschaffungsempfehlungen für die Akteure der Lieferkette formuliert.

2.4 Was ist der Hintergrund der NCCS-Verordnung?

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [13] legt Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in der Union fest. VERORDNUNG (EU) 2019/941 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [14] ergänzt die RICHTLINIE

[13] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0941

(EU) 2022/2555 [15] dahingehend, dass Cybersicherheitsvorfälle im Elektrizitätssektor ordnungsgemäß als Risiko identifiziert und Maßnahmen zu deren Bewältigung in die Risikovorsorgepläne aufgenommen werden. VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [16] ergänzt sowohl die Richtlinie (EU) 2022/2555 [17] als auch die Verordnung (EU) 2019/941 [18], indem sie spezifische Vorschriften für den Elektrizitätssektor auf Unionsebene festlegt. Darüber hinaus ergänzt diese delegierte Verordnung die Bestimmungen der Richtlinie (EU) 2022/2555 [19] in Bezug auf den Elektrizitätssektor, soweit es um grenzüberschreitende Stromflüsse geht.

Zentrale Maßnahmen der Kommission sind unter anderem der Aufbau eines umfassenden Rechtsrahmens auf Grundlage der EU-Cybersicherheitsstrategie (JOIN/2013/01) [20], der Richtlinie (EU) 2022/2555 [21] sowie des Cybersicherheitspakets (JOIN/2017/450 final) [22] vom September 2017, das auch das Cybersicherheitsgesetz enthält.

- Die NCCS ist am 13. Juni 2024 in Kraft getreten.
- Ein delegierter Rechtsakt der Europäischen Kommission ist **unmittelbar anwendbar und rechtsverbindlich in allen Mitgliedstaaten der EU.**
- Die NCCS legt **sektorspezifische Vorschriften** für **Cybersicherheitsaspekte** grenzüberschreitender Stromflüsse fest.
- Die NCCS **ergänzt andere europäische Rechtsvorschriften zur Cybersicherheit** (Richtlinie (EU) 2022/2555 [23]), soweit grenzüberschreitende Stromflüsse betroffen sind.

GOOD TO KNOW

- Die NCCS **ist in allen Mitgliedstaaten der EU unmittelbar anwendbar und rechtsverbindlich.**
- Die NCCS ist am 13. Juni 2024 in Kraft getreten.

2.5 Identifizierungsmethode der Organisationen

Ziel der NCCS-Verordnung ist es, die Cybersicherheit des europäischen Stromsystems in einem einheitlichen Rahmen zu stärken. Um eine wirksame Umsetzung zu gewährleisten, ist es notwendig, genau zu definieren, welche **Organisationen** den Anforderungen der Verordnung unterliegen.

[15] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0943
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[18] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0941
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[20] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52013JC0001
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[22] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=JOIN:2017:450:FIN
[23] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

Die Identifizierung der Organisationen erfolgt durch die zuständigen Behörden auf der Grundlage von Artikel 24 der NCCS [24] und Artikel 48 der NCCS [25].

Identifizierungskriterien:

1. Ihr ECII-Wert (Index für die Auswirkungen auf die Cybersicherheit) übersteigt die Schwellenwerte für erlebliche oder kritische Auswirkungen.

Vorläufige ECII-Werte sind hier verfügbar:

Vorläufige ECII-Werte laut ENTSO-E [26].

2. Sie nehmen an mit erheblichen Auswirkungen und mit kritischen Auswirkungen Prozessen auf EU-Ebene teil.

Die vorläufige Liste der Prozesse ist hier verfügbar:

Vorläufige Prozessliste laut ENTSO-E [27].

Identifizierung zusätzlicher Organisationen

1. Organisationen, die nicht in der Union niedergelassen sind, aber Dienstleistungen für in der Union tätige Organisationen erbringen

Die **zuständige Behörde** kann **Einrichtung mit erheblichen Auswirkungen** und **Einrichtung mit kritischen Auswirkungen** identifizieren, die nicht in der EU niedergelassen sind, sofern sie innerhalb der Union tätig sind. Die **zuständige Behörde** kann von diesen Organisationen Informationen anfordern, um ihre ECII-Werte zu bestimmen. Organisationen, die nicht in der Union niedergelassen sind, aber Dienstleistungen für Organisationen innerhalb der Union erbringen und benachrichtigt wurden, dass sie als erheblich relevant oder kritisch relevant eingestuft werden, müssen innerhalb von drei Monaten nach Eingang der Benachrichtigung schriftlich einen Vertreter in der Union benennen und die benachrichtigende zuständige Behörde entsprechend informieren, wie in Artikel 15 der NCCS festgelegt.

2. Gruppe von Organisationen

Die zuständige Behörde eines jeden **Mitgliedstaats** kann zusätzliche Organisationen als **Einrichtung mit erheblichen Auswirkungen** oder **Einrichtung mit kritischen Auswirkungen** identifizieren, wenn die folgenden Kriterien erfüllt sind:

a. Die Organisation ist Teil einer Gruppe von Organisationen, die einem erheblichen Risiko einer gleichzeitigen Betroffenheit durch einen **Cyberangriff** ausgesetzt sind.

b. Der aggregierte ECII-Wert der Gruppe übersteigt die Schwellenwerte für erhebliche Auswirkung oder kritische Auswirkung.

[24] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_24
[25] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_48
[26] https://www.entsoe.eu/network_codes/nccs/
[27] https://www.entsoe.eu/network_codes/nccs/

2.6 Welche Organisationen fallen unter den Anwendungsbereich der NCCS?

Organisationen werden als **„erheblich"** oder **„kritisch"** eingestuft, basierend auf dem **potenziellen Schweregrad eines Cyberangriffs auf ihre Prozesse und die damit verbundenen Vermögenswerte** sowie der **Auswirkung auf grenzüberschreitende Stromflüsse** (Artikel 24 der NCCS [28]).

Die folgenden Organisationen fallen unter den Anwendungsbereich von Artikel 2 Absatz 1 der NCCS [29]:

Klicken Sie auf das Bild zum Vergrößern

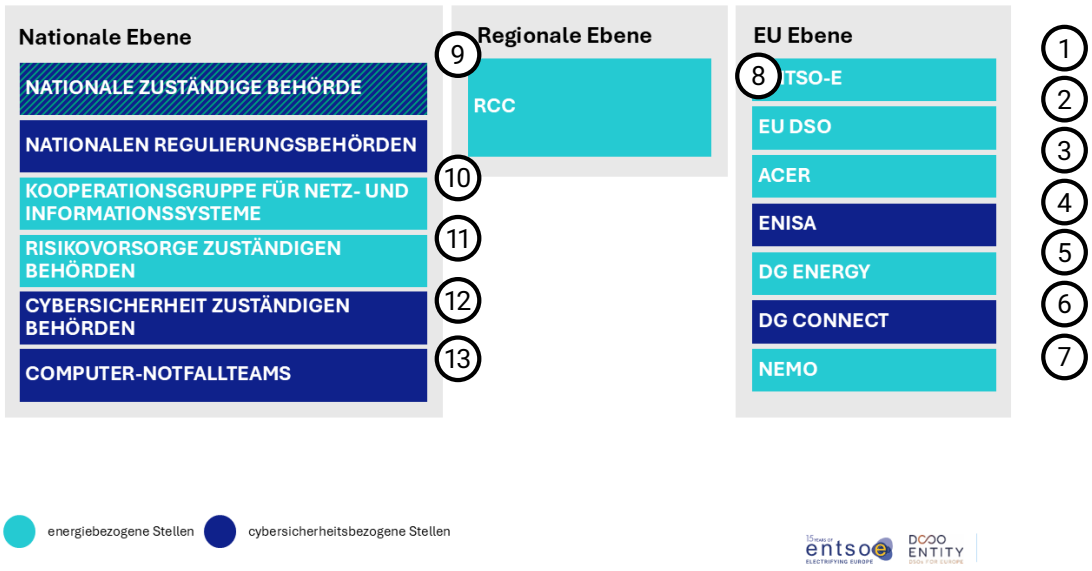
GOOD TO KNOW

- Die Identifizierung erfolgt anhand definierter Schwellenwerte (ECII). Die zuständige Behörde kann auch die Teilnahme an EU-weiten Prozessen mit erleblicher oder kritischer Auswirkung bewerten.
- Die zuständige Behörde stuft Organisationen in die Kategorien erheblcih und kritisch ein.

[28] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_24
[29] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_2

2.7 Wer ist für die Steuerung der NCCS verantwortlich?

> Die Steuerung des NCCS involviert mehrere Interessengruppen.



1

ENTSO-E (Verband Europäischer Übertragungsnetzbetreiber)

ENTSO-E [30] ist der Zusammenschluss der europäischen Übertragungsnetzbetreiber. Im Rahmen der NCCS ist ENTSO-E verantwortlich für die Durchführung der EU-weiten Cybersicherheits-Risikobewertung (Artikel 19 der NCCS [31]) sowie für die Erstellung regionaler Risikobewertungsberichte (Artikel 21 der NCCS [32]). Diese regionalen Bewertungen berücksichtigen regionale Krisenszenarien gemäß Artikel 6 der Verordnung (EU) 2019/941 [33]. ENTSO-E organisiert in Zusammenarbeit mit der EU-VNBO regionale Cybersicherheitsübungen in allen Systembetriebsregionen (Artikel 44 der NCCS [34]).

2

EU-VNBO (Europäische Organisation der Verteilnetzbetreiber)

[30] https://www.entsoe.eu/
[31] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_19
[32] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_21
[33] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_6
[34] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_44

EU-VNBO [35] vertritt die europäischen Verteilnetzbetreiber. Gemäß NCCS arbeitet die EU-VNBO mit ENTSO-E bei der Durchführung der EU-weiten Risikobewertung (Artikel 19 [36]) sowie bei regionalen Berichten (Artikel 21 [37]) zusammen.

Beide organisieren gemeinsam regionale Übungen (Artikel 44 [38]).

3

ACER (Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden)

ACER [39] unterstützt die Regulierung des Energiemarktes. Gemäß NCCS gibt ACER Stellungnahmen zur Methodik der Risikobewertung ab (Artikel 8 [40]), überwacht die Umsetzung (Artikel 12 [41]), und legt Berichtspflichten (Artikel 27 [42], Artikel 39 [43]) sowie Leistungsindikatoren fest (Artikel 13 [44]). ACER koordiniert zudem die Annahme und Umsetzung von Begriffen, Methoden und Plänen (Artikel 6 [45]) und erstellt einen unionsweiten Krisenmanagementplan für den Stromsektor (Artikel 41 [46]).

4

ENISA (Agentur der Europäischen Union für Cybersicherheit)

ENISA [47] berät zu Cybersicherheit. Im Rahmen der NCCS konsultiert ENISA ACER und ENTSO-E zur Risikobewertungsmethodik (Artikel 6 [48]), bewertet Cybersicherheitsübungen (Artikel 43 [49]), und betreibt das Europäische Zentrum für den Informationsaustausch zur Cybersicherheit (ECEAC) (Artikel 42 [50]).

5

DG ENER (Generaldirektion Energie der Europäischen Kommission)

Die GD ENER [51] ist zuständig für die Energiepolitik der EU.

6

[35] https://eudsoentity.eu/
[36] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_19
[37] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_21
[38] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_44
[39] https://www.acer.europa.eu/
[40] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_8
[41] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_12
[42] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_27
[43] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_39
[44] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_13
[45] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_6
[46] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_41
[47] https://www.enisa.europa.eu/
[48] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_6
[49] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_43
[50] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366#art_42
[51] https://commission.europa.eu/about/departments-and-executive-agencies/energy_de

DG CONNECT (Generaldirektion Kommunikationsnetze, Inhalte und Technologien der Europäischen Kommission)

Die GD CONNECT [52] ist zuständig für die digitalen Politiken der EU.

7

NEMO

Benannte Strommarktbetreiber (Nominated Electricity Market Operators).

8

Regionale Koordinierungszentren (RCC)

Diese Zentren beraten bei der Entwicklung regionaler Risikobewertungen und Pläne sowie bei der Koordinierung zwischen Mitgliedstaaten.

9

Nationale zuständige Behörden (NCA)

Sie sind zuständig für die Umsetzung der NCCS in den Mitgliedstaaten. Sie identifizieren relevante Organisationen (Artikel 24 [53]), genehmigen Methoden (Artikel 6 [54]), erteilen Ausnahmen (Artikel 30 [55]), führen Bewertungen durch (Artikel 20 [56]), überprüfen die Einhaltung (Artikel 25 [57]), und koordinieren den Informationsaustausch zu Cyberangriffen.

10

Nationalen Regulierungsbehörden (NRB)

Sie sind verantwortlich für die Regulierung der Energiemärkte. Gemäß NCCS bestimmen sie u.a. die Mechanismen zur Kostenanerkennung (Artikel 11 [58]) und führen Leistungsevaluierungen durch (Artikel 13 [59]).

11

Nationale Behörden für die Risikovorsorge (RP NCA)

Sie sind zuständig für die Planung und Umsetzung von Risikovorsorgemaßnahmen, insbeson-

[52] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_de
[53] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_24
[54] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_6
[55] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_30
[56] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_20
[57] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_25
[58] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_11
[59] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_13

dere bei Risikobewertungen und dem Umgang mit Cyberangriffen.

12

Nationale Cybersicherheitsbehörden (CS NCA)

Sie sind verantwortlich für die nationale Cybersicherheitsstrategie und deren Umsetzung.

13

Computer Security Incident Response Teams (CSIRT)

Sie sind zuständig für die Bewältigung von Cybersicherheitsvorfällen. Sie unterstützen erheblich- und kritisch relevante Organisationen, tauschen Bedrohungsinformationen aus und nehmen an Übungen teil.

2.7.1 Zentrale Regulierungsbehörden

Die Mitgliedstaaten spielen eine Schlüsselrolle bei der Umsetzung der NCCS. Zur wirksamen Durchsetzung der Anforderungen der NCCS benennt jeder **Mitgliedstaat** eine zuständige Behörde, die für die Umsetzung der Verordnung verantwortlich ist (Artikel 4 der NCCS [60]).

> **Nationale zuständige Behörde**

Führt folgende Aufgaben aus:

- Eine nationale Regierungs- oder Regulierungsbehörde, die für die Erfüllung der ihr gemäß Artikel 4 der NCCS [61] übertragenen Aufgaben zuständig ist.
- Wird von jedem Mitgliedstaat **spätestens sechs Monate nach Inkrafttreten** der Verordnung benannt (Artikel 4 Absatz 1 [62]).
- **Koordiniert und arbeitet zusammen** mit den zuständigen Cybersicherheitsbehörden, den NRB, RP NCA, CSIRT und anderen durch den jeweiligen Mitgliedstaat bestimmten Behörden, um eine effektive Umsetzung der NCCS sicherzustellen und Doppelarbeit zu vermeiden (Artikel 5 [63]).
- **Kann Aufgaben** an andere nationale Behörden delegieren (Artikel 4 Absatz 3 [64]).

[60] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_4
[61] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_4
[62] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[63] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_5
[64] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4

- **Identifiziert erheblich- und kritisch relevante Organisationen** (Artikel 24 Absatz 2 [65]).
- **Genehmigt entwickelte Bedingungen und Methoden** (Artikel 6 Absatz 2 [66]).
- **Führt Cybersicherheits-Risikobewertungen durch** (Artikel 20 Absatz 1 [67]).
- **Erteilt Ausnahmen von Mindest- und fortgeschrittenen Sicherheitskontrollen** (Artikel 30 Absatz 1 [68]).
- **Kann Inspektionen** von Organisationen mit kritischer Auswirkung gemäß nationalem Recht durchführen, um deren Konformität mit der NCCS zu überprüfen (Artikel 25 [69]).

Nationale Regulierungsbehörde

Führt folgende Aufgaben aus:

- **Setzt die NCCS um** gemäß Artikel 59 Absatz 1 Buchstabe e) der RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [70].
- **Bewertet Kosten**, die Übertragungsnetzbetreiber (ÜNB) und Verteilnetzbetreiber (VNB) tragen, gemäß Artikel 11 der Richtlinie (EU) 2019/944 [71].
- **Führt Bewertung und Analyse** innerhalb von 12 Monaten nach Entwicklung der Leitlinien zur Leistungsevaluierung durch, gemäß Artikel 13 Absatz 2 der Richtlinie (EU) 2019/944 [72].

---

[65] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[66] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_6
[67] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_20
[68] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_30
[69] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25
[70] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0944#art_59
[71] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0944#art_11
[72] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0944#art_13

Chapter 3

Übergangsbestimmungen der NCCS

In diesem Kapitel erfahren Sie mehr über die wichtigsten Übergangsbestimmungen der NCCS.

Artikel 48 der NCCS-Verordnung [1] enthält Übergangsbestimmungen, die eine verstärkte Anwendung von Leitlinien zur Cybersicherheit im Elektrizitätssektor sicherstellen, bis endgültige Bedingungen und Methoden ausgearbeitet und angenommen werden.

Nach dem Vorsorgeprinzip können **Einrichtung mit erheblichen Auswirkungenn** und **Einrichtung mit kritischen Auswirkungen** während der **Übergangszeit** (bis zum 13. Juni 2028, abhängig von der EU-weiten Annahme relevanter Methoden) freiwillig den in der NCCS-Verordnung festgelegten Verpflichtungen nachkommen, noch bevor sie gemäß Artikel 24 der NCCS [2] endgültig identifiziert werden.

Darüber hinaus schreibt Artikel 48 Absatz 10 der NCCS [3] vor, dass alle identifizierten Organisationen bis zur Annahme der Mindest- und erweiterten Sicherheitskontrollen gemäß Artikel 29 der NCCS [4] schrittweise die gemäß Artikel 48 Absatz 1 [5] entwickelten Leitlinien umsetzen sollen.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48

Thema	Erarbeitet von	Zeitplan
Entwicklung vorläufiger ECII-Werte (Artikel 48 Absatz 2 der NCCS [6]) Die vorläufigen ECII-Werte unterstützen die zuständigen Behörden bei der Identifizierung der Einrichtung mit erheblichen oder mit kritischen Auswirkungen.	ENTSO-E, EU-VNBO	13. Oktober 2024
Zusammenstellung der Liste Prozesse mit erheblichen Auswirkungen und Prozess mit kritischer Auswirkung (Artikel 48 Absatz 4 der NCCS [7]) Ergänzend zu den ECII-Werten liefern diese Prozesse zusätzliche Orientierung für die Identifizierung.	ENTSO-E, EU-VNBO	13. Dezember 2024
Zusammenstellung der vorläufigen Liste Einrichtung mit erheblichen oder mit kritischen Auswirkungen und Benachrichtigung der Organisationen (Artikel 48 Absatz 3 der NCCS [8])	Zuständige Behörde	Identifizierung benannter Organisationen: 13. Februar 2025 Benachrichtigung der Organisationen: 13. März 2025
Entwicklung einer **vorläufigen Liste europäischer und internationaler Normen und Kontrollen**, die gemäß nationalen Vorschriften für die Cybersicherheit grenzüberschreitender Stromflüsse relevant sind (Artikel 48 der NCCS [9])	ENTSO-E, EU-VNBO	13. Juni 2025

Das **ENTSO-E** (Zusammenschluss der europäischer Übertragungsnetzbetreiber) hat in Zusammenarbeit mit dem **EU VNBO** (Europäische Organisation der Verteilnetzbetreiber) eine **vorläufige Liste von Prozessen mit hoher und kritischer Auswirkung** auf Unionsebene erstellt.

[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_48

Die vorläufige Liste der Prozesse ist unter den folgenden Links abrufbar:

> FILE 1
>
> Vorläufige Liste von Prozessen mit hoher und kritischer Auswirkung auf Unionsebene
>
> **files/Provisional list of Union-wide high-impact and critical-impact processes.pdf**

Das **unterstützende methodische Dokument** liefert zusätzliche Informationen und Begründungen zu den aufgeführten Prozessen.

> FILE 2
>
> Unterstützendes Dokument zur vorläufigen Liste von Prozessen mit hoher und kritischer Auswirkung
>
> **files/Supporting document Provisional list of Union-wide high-impact and critical-impact processes.pdf**

Im Rahmen des NCCS hat **ENTSO-E** in Zusammenarbeit mit dem **EU VNBO** einen **vorläufigen Elektrizitäts-Cybersicherheits-Auswirkungsindex ECII sowie Schwellenwerte für die Kategorien hohe und kritische Auswirkung** entwickelt.

Der vorläufige Elektrizitäts-Cybersicherheits-Auswirkungsindex (ECII) ist unter den folgenden Links abrufbar:

> FILE 3
>
> Vorläufiger Elektrizitäts-Cybersicherheits-Auswirkungsindex (ECII)
>
> **files/Provisional ECII.pdf**

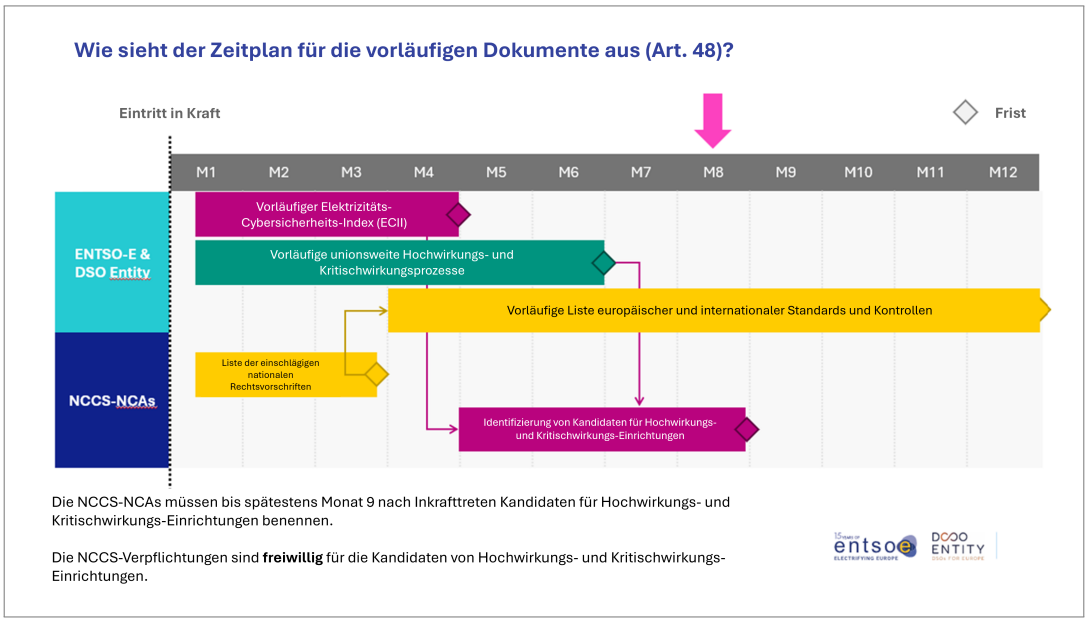
Das **unterstützende methodische Dokument** liefert zusätzliche Informationen und Begründungen zum ECII.

> FILE 4
>
> Unterstützendes Dokument zum vorläufigen Elektrizitäts-Cybersicherheits-Auswirkungsindex (ECII)
>
> **files/Supporting document provisional ECII.pdf**

GOOD TO KNOW

- Die zuständigen Behörden werden die in der vorläufigen Liste benannten Einrichtungen **spätestens bis zum 13. März 2025** benachrichtigen und darüber informieren, dass sie als Einrichtungen mit hoher oder kritischer Auswirkung eingestuft wurden.
- Einrichtungen, die in der vorläufigen Liste als solche mit hoher oder kritischer Auswirkung aufgeführt sind, können auf freiwilliger Basis den in dieser Verordnung festgelegten Verpflichtungen gemäß dem Vorsorgeprinzip nachkommen.

Hier ist der vorläufige Zeitplan einsehbar:



Chapter 4

Vergleich von NCCS und NIS2

Dieser Teil soll den Anwendungsbereich und die Anwendung der beiden Verordnungen RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES, NIS-2-Richtlinie [1] und DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION zur Ergänzung der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates durch einen Netzkodex über sektorspezifische Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse, NCCS-Verordnung [2] klären.

Die NIS-2-Richtlinie und der Netzkodex für Cybersicherheit (NCCS) sind beides wichtige Verordnungen in der EU, aber sie dienen unterschiedlichen Zwecken und haben unterschiedliche Geltungsbereiche: NIS-2-Richtlinie:* Dies ist eine aktualisierte Version der ursprünglichen NIS-Richtlinie (NIS 1), die 2016 eingeführt wurde. NIS 2 zielt darauf ab, die Sicherheit und Widerstandsfähigkeit kritischer Infrastrukturen und digitaler Dienste in der EU zu verbessern. Sie gilt für ein breiteres Spektrum von Sektoren, darunter wesentliche Dienste wie Energie, Verkehr, Banken, Gesundheit und Anbieter digitaler Dienste. Mit der NIS 2 werden strengere Sicherheitsanforderungen, Meldepflichten für Zwischenfälle und ein umfassenderer Ansatz für das Management von Cybersicherheitsrisiken eingeführt.

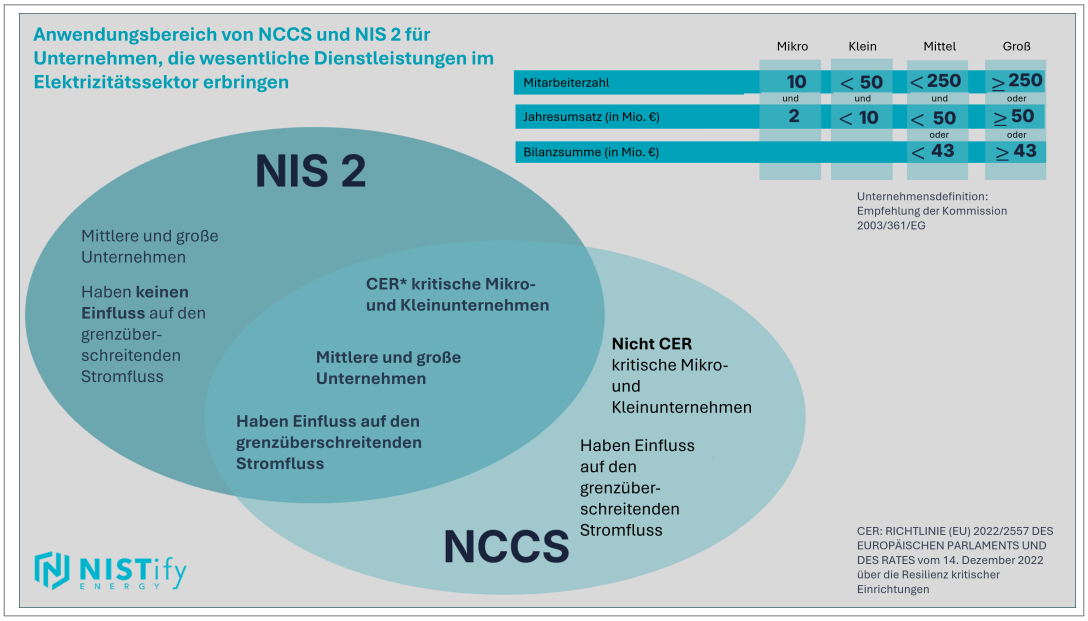
NIS-2-Richtlinie: Dies ist eine aktualisierte Version der ursprünglichen NIS-Richtlinie (NIS 1), die 2016 eingeführt wurde. NIS 2 zielt darauf ab, die Sicherheit und Widerstandsfähigkeit kritischer Infrastrukturen und digitaler Dienste in der EU zu verbessern. Sie gilt für ein breiteres Spektrum von Sektoren, darunter wesentliche Dienste wie Energie, Verkehr, Banken, Gesundheit und Anbieter digitaler Dienste. Mit der NIS 2 werden strengere Sicherheitsanforderungen, Meldepflichten für Zwischenfälle und ein umfassenderer Ansatz für das Management von Cybersicherheitsrisiken eingeführt.

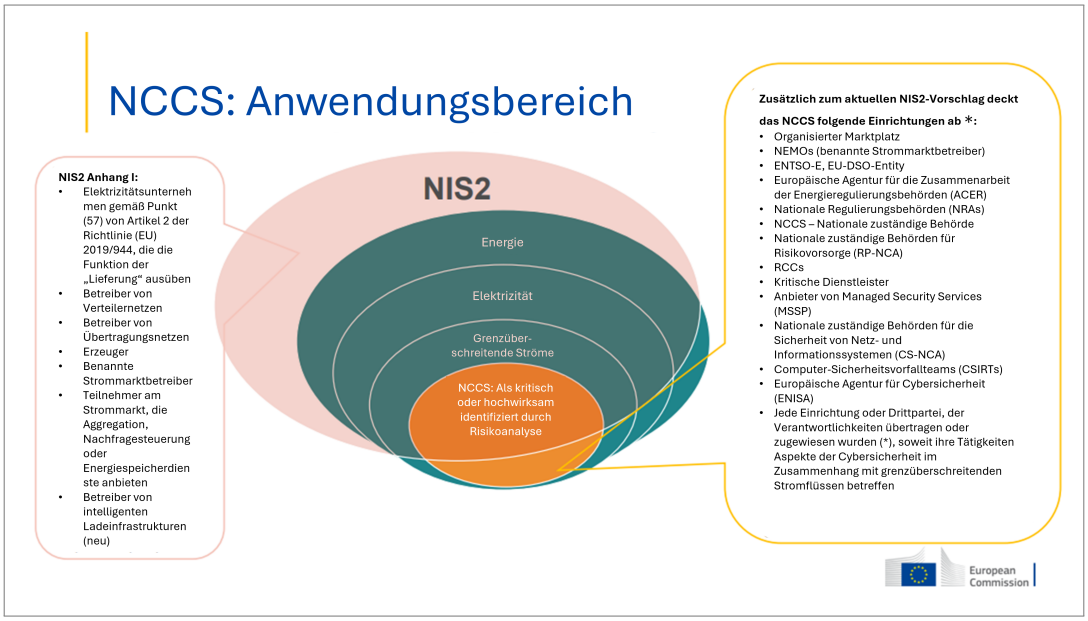
Netzkodex für Cybersicherheit: Der Netzkodex für Cybersicherheit konzentriert sich speziell auf die Cybersicherheit der grenzüberschreitenden Stromflüsse innerhalb der EU. Er legt einheitliche Cybersicherheitsstandards für den Elektrizitätssektor fest, einschließlich Regeln für die Risikobewertung, Mindestsicherheitsanforderungen, Zertifizierung von Produkten und Dienstleistungen, kontinuierliche Überwachung, Berichterstattung und Krisenmanagement.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366

4.1 Anwendungsbereich von NCCS und NIS 2

Wie im folgenden Diagramm zu sehen ist, haben NIS 2 und NCCS unterschiedliche, aber sich überschneidende Einflussbereiche, insbesondere wenn es um die Größe der Unternehmen und ihre Auswirkungen auf den grenzüberschreitenden Stromfluss geht. Das Verständnis dieser Unterschiede ist für Unternehmen entscheidend, um die Einhaltung der Vorschriften zu gewährleisten und die Widerstandsfähigkeit kritischer Infrastrukturen zu verbessern.





4.2 NCCS und NIS 2 Anforderungen

> Erkunden Sie die spezifischen Anforderungen und Unterschiede zwischen NIS 2 und NCCS in Schlüsselbereichen.

Betroffene IT-/OT-Geräte

NIS 2

Die NIS 2 deckt **alle IT- und OT-Systeme innerhalb einer Organisation** ab und gewährleistet so einen umfassenden Ansatz für die Cybersicherheit in allen Bereichen. Dieser breite Geltungsbereich soll die allgemeine Cybersicherheitshygiene fördern, auch für kleinere oder weniger kritische Systeme.

NCSS

Im Gegensatz dazu konzentriert sich der NCCS auf Systeme in kritischen oder besonders relevanten Bereichen, basierend auf ihrer Rolle in hochwirksamen und sicherheitskritischen Prozessen – also jene Systeme, deren Kompromittierung erhebliche Auswirkungen auf den Betrieb haben oder sogar andere Regionen oder Sektoren betreffen könnte. Der Fokus liegt hierbei auf dem Schutz der wesentlichsten Komponenten, bei denen die höchsten Risiken bestehen.

NIS 2	NCCS
Alle Systeme	Systeme innerhalb von kritischen und/oder hochgefährdeten Bereichen (physisch, logisch)

Risikoanalyse und Risikomanagement

NIS 2

Während die NIS-2-Richtlinie eine gewisse Flexibilität bei der Umsetzung zulässt, verpflichtet sie Organisationen, die als „wesentliche“ oder „wichtige Einrichtungen“ eingestuft sind, zur Einführung von Risikomanagementpraktiken. Diese Organisationen sind verpflichtet, Maßnahmen zum Management von Cybersicherheitsrisiken zu ergreifen, um identifizierte Risiken zu adressieren. Die Flexibilität besteht darin, dass diese Einrichtungen ihren Risikomanagementansatz an ihre spezifischen Ressourcen, Risikoniveaus und betrieblichen Anforderungen anpassen können.

NCCS

Der NCCS geht noch einen Schritt weiter, indem sie einen strukturierten und kooperativen Ansatz für das Risikomanagement betont. Sie schreibt einen detaillierten Risikobewertungsprozess vor, der sich über vier Ebenen erstreckt: EU-weit, regional, auf Ebene der Mitgliedstaaten und auf Ebene einzelner Einrichtungen. Dieser Ansatz gewährleistet ein harmonisiertes Verständnis von Cybersicherheitsrisiken und ermöglicht koordinierte Maßnahmen zur Risikominderung.

NIS 2	NCCS
Erforderlich	Erforderlich

Informationsaustausch zwischen den Betroffenen

NIS 2

In der NIS 2 wird der **Informationsaustausch gefördert**, aber auf freiwilliger Basis, so dass die Unternehmen selbst entscheiden können, wie viele Informationen sie weitergeben möchten, je nach Komfort und Prioritäten. Dieser flexible Ansatz kann einen offenen, organischen Informationsaustausch fördern.

NCCS

Der NCCS hingegen **verlangt den Informationsaustausch**. Organisationen sind verpflichtet, Vorfälle zu melden und relevante Daten auszutauschen, wodurch sichergestellt wird, dass wichtige

Bedrohungsinformationen schnell und einheitlich zwischen allen betroffenen Parteien ausgetauscht werden. Dies ist eine wesentliche Voraussetzung für eine koordinierte, rechtzeitige Reaktion auf potenzielle Bedrohungen, insbesondere in Hochrisikobereichen.

NIS 2	NCCS
Freiwillig und auf Vereinbarungsbasis	Es besteht eine Verpflichtung zur Zusammenarbeit (was, wann, mit wem)

CSOC erstellen

NIS 2

Die NIS 2 **verlangt** von Organisationen nicht, dass sie ein CSOC einrichten, sondern lässt ihnen die **Flexibilität**, je nach Größe, Bedarf und Ressourcen andere Sicherheitsmaßnahmen zu wählen. Dieser Ansatz eignet sich gut für **kleinere oder weniger kritische** Einrichtungen, die möglicherweise nicht die Kapazität für ein eigenes CSOC haben.

NCCS

Der NCCS impliziert oder **verlangt jedoch ein CSOC für kritische und hochgefährdete Systeme**, da er anerkennt, dass Echtzeitüberwachung und schnelle Reaktion für Hochrisikoumgebungen notwendig sind. Es wird erwartet, dass Organisationen, die kritische Infrastrukturen verwalten, über ein CSOC oder eine gleichwertige Fähigkeit verfügen, um eine kontinuierliche Überwachung aufrechtzuerhalten.

NIS 2	NCCS
Nicht erforderlich	Erforderlich

Identifizierung und Meldung von Vorfällen

NIS 2

Die NIS 2 schreibt vor, dass **wichtige Sicherheitsvorfälle**, die IT/OT-Systeme betreffen, **unverzüglich** gemeldet werden müssen, im Allgemeinen innerhalb von 24 Stunden. Bei Bedrohungen und Beinahe-Cyber-Vorfällen wird die **Meldung gefördert, bleibt aber freiwillig**, so dass die Unternehmen je nach Schweregrad und Kontext entscheiden können. Unternehmen sind für die interne Untersuchung von Vorfällen verantwortlich, während grenzüberschreitende Auswirkungen je nach Bedarf an die Computer-Notfallteams (CSIRT) weitergeleitet werden. Dieser Ansatz bietet Flexibilität und stellt gleichzeitig sicher, dass wichtige Vorfälle zeitnah gemeldet werden.

NCCS

Der NCCS setzt **strengere Anforderungen für die Meldung** durch, insbesondere für Vorfälle, die grenzüberschreitende Energiesysteme betreffen könnten. Bedeutende Vorfälle müssen **innerhalb eines kürzeren Zeitfensters** (innerhalb von 4 Stunden) gemeldet werden, um den potenziell größeren Auswirkungen Rechnung zu tragen. Darüber hinaus schreibt der NCCS die Untersuchung von Zwischenfällen unter Beteiligung der zuständigen Behörde und mit Unterstützung von CSOC vor. Dieser umfassende Ansatz soll eine rasche, koordinierte Reaktion auf kritische Zwischenfälle ermöglichen, insbesondere auf solche mit Auswirkungen über die Landesgrenzen hinaus.

NIS 2	NCCS
* Bedeutende Sicherheitsvorfälle im Zusammenhang mit IT/OT-Systemen müssen sofort (innerhalb von 24 Stunden) gemeldet werden, während Bedrohungen und Cyber-nahe Vorfälle den Computer-Notfallteams (CSIRT) auf freiwilliger Basis gemeldet werden müssen (Aktualisierung innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats). * Organisationen untersuchen Vorfälle intern; grenzüberschreitende Auswirkungen werden von Computer-Notfallteams (CSIRT) untersucht.	*Bedeutende Sicherheitsvorfälle im Zusammenhang mit IT/OT-Systemen - oder mit grenzüberschreitenden Auswirkungen auf die Energie - müssen unverzüglich (innerhalb von 4 Stunden) der zuständigen Behörde und dem CSIRT gemeldet werden, einschließlich Bedrohungen und Beinahe-Cyber-Vorfälle. * Alle anderen bedeutenden Sicherheitsvorfälle müssen gemäß den NIS-2-Standards gemeldet werden. * Auf der Grundlage der vom CSOC bereitgestellten Informationen untersucht die Organisation die Vorfälle mit Unterstützung der zuständigen Behörde.

Sicherheit der Lieferkette

NIS 2

In der NIS 2 wird die Sicherheit der Lieferkette als **zwingendes Element des Cybersecurity-Risikomanagements** aufgenommen. Organisationen müssen die Sicherheitsrisikobewertung von kritischen Lieferketten auf EU-Ebene berücksichtigen. Zusätzlich kann die Kommission Verordnungen erlassen, die technische und methodische Anforderungen für das Cybersecurity-Risikomanagement festlegen, falls dies auf sektoraler Ebene erforderlich ist. Ein Zertifikat für einen Lieferanten oder das gelieferte Produkt oder die Dienstleistung kann verlangt werden, um die Einhaltung der Sicherheitsstandards zu gewährleisten.

NCCS

Der NCCS bietet **ausführlichere Leitlinien zur Sicherheit der Lieferkette** mit definierten Risikobewertungs- und Kontrollkriterien. Es ist **vorgeschrieben, die Sicherheitsrisikobewertung** von kritischen Lieferketten auf EU-Ebene zu berücksichtigen, und es werden spezifische Empfehlungen für die Beschaffung gegeben. Für Einrichtungen mit erheblichen/kritischen Auswirkungen wird die Verantwortung dafür übernommen, dass die Lieferanten die Cybersicherheitsanforderungen erfüllen, einschließlich der Festlegung von Auswahlkriterien und vertraglichen Verpflichtungen. Anbieter kri-

tischer IKT-Dienstleistungen müssen ebenfalls benachrichtigt werden und die NCCS-Bestimmungen für Organisationen mit kritischer oder erheblicher Auswirkung einhalten.

NIS 2	NCCS
* Obligatorisches Element des Cybersecurity-Risikomanagements * Die Berücksichtigung der Sicherheitsrisikobewertung kritischer Lieferketten auf EU-Ebene ist obligatorisch. * Die Kommission kann Verordnungen erlassen, die die technischen und methodischen Anforderungen an das Cybersecurity-Risikomanagement regeln, gegebenenfalls auf sektoraler Ebene. * Ein Zertifikat für einen Lieferanten oder ein geliefertes Produkt oder eine Dienstleistung kann verlangt werden.	* Es wurden detaillierte Kriterien für die Risikobewertung und -kontrolle festgelegt. * Die Berücksichtigung der Sicherheitsrisikobewertung kritischer Lieferketten auf EU-Ebene ist obligatorisch. * Empfehlungen für die Auftragsvergabe sind definiert. * Die für die Umsetzung der Cybersicherheitsanforderungen durch den Lieferanten verantwortliche Stelle (Auswahlkriterien, vertragliche Anforderungen) * Kritische IKT-Dienstleister müssen benachrichtigt werden und unterliegen den NCCS-Bestimmungen in Bezug auf Organisationen mit kritischen Auswirkungen oder erheblichen Auswirkungen.

Einrichtung eines nationalen Überwachungs- und Kontrollsystems (NIS 2 und NCCS-konform)

NIS 2

Gemäß NIS 2 muss ein **nationales Aufsichtskontrollsystem** eingerichtet werden, wobei die Prüfungen im Bezugsjahr 2025 beginnen und **alle zwei Jahre** durchgeführt werden müssen. Dieser Rahmen gewährleistet eine regelmäßige Aufsicht, enthält jedoch keine sektorspezifischen Anforderungen an die Prüfer, sondern erlaubt allgemeinere Prüfungsansätze.

NCCS

Der NCCS verfolgt einen intensiveren Ansatz, insbesondere für Unternehmen mit kritischen Auswirkungen. Audits sind **jährlich** vorgeschrieben, wobei ab dem Referenzjahr 2026 alle drei Jahre ein **umfassendes Audit** stattfindet. Für die Prüfer gelten sektorspezifische Anforderungen, die sicherstellen, dass der Prüfprozess auf die Bedürfnisse der kritischen Infrastruktursektoren zugeschnitten ist und dass Unternehmen mit erheblicher Auswirkung eine spezielle Aufsicht erhalten.

NIS 2	NCCS
* * Audit alle 2 Jahre	* Erfordert Unternehmen mit kritischen Auswirkungen * Jährliches Audit, vollständiges Audit alle 3 Jahre * Sektorspezifische Anforderungen gelten für den Prüfer

Managementsystem für Cybersicherheit, Überprüfung der Konformität der durchgeführten Kontrollen

NIS 2

Die NIS 2 schreibt nicht ausdrücklich ein Cybersicherheitsmanagementsystem vor, so dass die Organisationen ihren Ansatz für die Kontrolle und Überprüfung der Cybersicherheit entsprechend ihren Bedürfnissen und Ressourcen flexibel wählen können.

NCCS

Der NCCS **verlangt** jedoch, dass alle kritischen Wermögenswerte innerhalb des kritischen Bereichs über ein Cybersicherheitsmanagementsystem verfügen. Für diese Anlagen sind alle drei Jahre verpflichtende Audits und Überprüfungen vorgeschrieben, wobei zwei Überprüfungsmethoden zulässig sind: Sicherheitsaudits durch unabhängige Dritte oder interne Überprüfungen, die bestimmte Anforderungen erfüllen und einen einheitlichen Standard für die Einhaltung der Cybersicherheitsvorschriften gewährleisten.

NIS 2	NCCS
* Erfordert kein Cybersicherheitsmanagementsystem	* Erfordert alle Vermögenswerte von Organisationen mit kritischer Auswirkung innerhalb des kritischen Bereichs * Obligatorisches Audit und Überprüfung alle 3 Jahre * Zwei Möglichkeiten: Sicherheitsaudits durch unabhängige Dritte, die die Anforderungen des vorhergehenden Punktes erfüllen, oder der vorhergehende Punkt

Verfahren zum Management von Cyberangriffen testen

NIS 2

Die NIS 2 **verlangt** von den Organisationen nicht, dass sie ihre Verfahren zum Management von Cyberangriffen unabhängig testen. Stattdessen wird diese Verantwortung in der Regel den Behörden auf EU- und nationaler Ebene zugewiesen, die die Aufsicht übernehmen, ohne spezifische Testverpflichtungen für einzelne Organisationen durchzusetzen.

NCCS

Der NCCS verlangt jedoch, dass Organisationen mit kritischen Auswirkungen **mindestens einmal im Jahr** umfassende Tests ihrer Verfahren zur Reaktion auf Cyberangriffe durchführen. Diese Tests können auch Teil von umfassenderen organisationsweiten Cybersicherheitsübungen sein. Die Testanforderung muss bis zum 31. Dezember 2025 vollständig umgesetzt werden, wobei

sich einige Organisationen schrittweise dazu verpflichten. Dadurch wird sichergestellt, dass die Organisationen ihre Reaktionsfähigkeit aktiv bewerten und verbessern.

NIS 2	NCCS
Erfordert keine Prüfung von Verfahren zum Management von Cyberangriffen	* Umfassende Verfahren zur Reaktion auf Cyberangriffe, die mindestens einmal jährlich getestet werden. Sie kann auch als Teil einer organisationsweiten Cybersicherheitsübung durchgeführt werden.

Krisenmanagement

NIS 2

Im Rahmen der NIS 2 werden die Zuständigkeiten für das Krisenmanagement in erster Linie von **Behörden auf EU- und nationaler Ebene** wahrgenommen und nicht einzelnen Organisationen auferlegt. Dieser Ansatz auf hoher Ebene ermöglicht eine zentralisierte Koordinierung bei größeren Zwischenfällen.

NCCS

Der NCCS legt einen stärkeren Fokus auf die aktive Beteiligung am Krisenmanagement durch Organisationen mit kritischer Auswirkung. Sie verpflichtet diese Organisationen dazu, in Abstimmung mit den zuständigen Behörden zu handeln, um eine koordinierte Reaktion auf groß angelegte Cybervorfälle sicherzustellen. Diese Anforderung fördert die Krisenvorsorge und stärkt gemeinsame Maßnahmen zur Krisenbewältigung.

NIS 2	NCCS
Aufgabe der Behörde für Krisenmanagement	Akive Teilnahme

Durchführung von Cyberangriffsübungen

NIS 2

Für die NIS 2 ist die Durchführung von Cyberangriffsübungen **nur auf EU- und nationaler Ebene** vorgeschrieben, so dass die Behörden Cyberbedrohungen simulieren und sich darauf vorbereiten können, ohne diese Übungen für einzelne Organisationen vorzuschreiben.

NCCS

Der NCCS schreibt vor, dass Organisationen mit kritischen Auswirkungen **alle drei Jahre** Cyberangriffsübungen durchführen, um die ständige Bereitschaft zu gewährleisten. Außerdem müssen kritische **IKT-Dienstleister** in diese Übungen einbezogen werden. Diese Vorschrift, die am 31. Dezember 2025 in Kraft tritt, stellt sicher, dass Organisationen mit kritischen Infrastrukturen ihre Bereitschaft durch regelmäßige Übungen aufrechterhalten.

NIS 2	NCCS
Nur auf EU- und nationaler Ebene erforderlich	* Erforderlich alle drei Jahre für Organisationen mit kritischen Auswirkungen * Beteiligte kritische IKT-Dienstleister

Geschäftskontinuitätsplanung

NIS 2

Nach der NIS-2-Richtlinie ist die Geschäftskontinuitätsplanung ein obligatorischer Bestandteil des Cybersicherheits-Risikomanagements. Diese Anforderung stellt sicher, dass kritische Organisationen über Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit verfügen, um ihre operationelle Resilienz auch bei potenziellen Störungen zu gewährleisten.e

NCCS

Der NCCS verlangt, dass die **Geschäftskontinuitätsplanung alle drei Jahre getestet und aktualisiert wird**. Die Verantwortung für die Überwachung dieser Kontinuitätsmaßnahmen liegt bei den Regulierungsbehörden, was eine zusätzliche Ebene der Compliance-Überwachung darstellt.

NIS 2	NCCS Obligatorisches Element des Cybersicherheits-Risikomanagements

Sanktion

NIS 2

Für die NIS 2 können die Sanktionen bei Nichteinhaltung der Cybersicherheitsanforderungen erheblich sein. Für Organisationen mit kritischer Auswirkung können **Geldbußen bis zu 10.000.000 EUR oder 2 % des weltweiten Jahresumsatzes** des Unternehmens aus dem vorangegangenen Geschäftsjahr betragen, je nachdem, welcher Betrag höher ist, was eine starke Abschreckung darstellt.

NCCS

Die NCCS-Sanktionen werden von **Regulierungsbehörden** um- und durchgesetzt, wobei Sanktionen gegen Organisationen verhängt werden, die die Anforderungen an die Geschäftskontinuität und Cybersicherheit nicht erfüllen.

NIS 2	NCCS
Für eine Organisation mit kritischer Auswirkung: mindestens 10.000.000 EUR oder 2 % des Gesamtbetrags seines weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr	Durchgeführt von einer Regulierungsbehörde

4.2.1 Vollständige Vergleichstabelle

Kategorie	NIS 2	NCCS
Betroffene Systeme	Alle Systeme	Systeme innerhalb kritischer und/oder erheblicher Perimeter (physisch, logisch)
Risikoanalyse und Risikomanagement	Obligatorisch	Obligatorisch
Informationsaustausch zwischen den Betroffenen	Freiwillig und auf Vereinbarungsbasis	* Es besteht eine Verpflichtung zur Zusammenarbeit (was, wann, mit wem)
CSOC erstellen	Nicht erforderlich	Obligatorisch
Identifizierung und Meldung von Vorfällen	* Bedeutende Sicherheitsvorfälle im Zusammenhang mit IT/OT-Systemen müssen sofort (innerhalb von 24 Stunden) gemeldet werden, während Bedrohungen und Cyber-nahe Vorfälle dem Computer-Notfallteam (CSIRT) auf freiwilliger Basis gemeldet werden müssen. (Aktualisierung innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats) * Organisationen untersuchen Vorfälle intern; grenzüberschreitende Auswirkungen werden vom Computer-Notfallteam (CSIRT) untersucht.	* Bedeutende Sicherheitsvorfälle im Zusammenhang mit IT/OT-Systemen - oder mit grenzüberschreitenden Auswirkungen auf die Energie - müssen unverzüglich (innerhalb von 4 Stunden) der zuständigen Behörde und dem CSIRT gemeldet werden, einschließlich Bedrohungen und Beinahe-Cyber-Vorfälle. * Alle anderen bedeutenden Sicherheitsvorfälle müssen gemäß den NIS-2-Standards gemeldet werden. * Auf der Grundlage der vom CSOC bereitgestellten Informationen untersucht die Organisation die Vorfälle mit Unterstützung der zuständigen Behörde.
Sicherheit der Lieferkette	* Obligatorisches Element des Cybersicherheits-Risikomanagements * Die Sicherheitsrisikobewertung kritischer Lieferketten muss auf EU-Ebene berücksichtigt werden. * Die Kommission kann Verordnungen zur Regelung der technischen und methodischen Anforderungen an das Risikomanagement im Bereich der Cybersicherheit erlassen, erforderlichenfalls auf sektoraler Ebene. * Ein Zertifikat für einen Lieferanten oder ein geliefertes Produkt oder eine Dienstleistung kann	* Es wurden detaillierte Kriterien für die Risikobewertung und -kontrolle festgelegt. * Die Sicherheitsrisikobewertung kritischer Lieferketten auf EU-Ebene muss berücksichtigt werden. * Beschaffungsempfehlungen werden definiert * Eine Organisation mit erheblicher/kritischer Auswirkung ist verantwortlich für die Umsetzung der Cybersicherheitsanforderungen durch den Lieferanten (Auswahlkriterien, vertragliche Anforderungen) * Kritische IKT-Dienstleister müssen

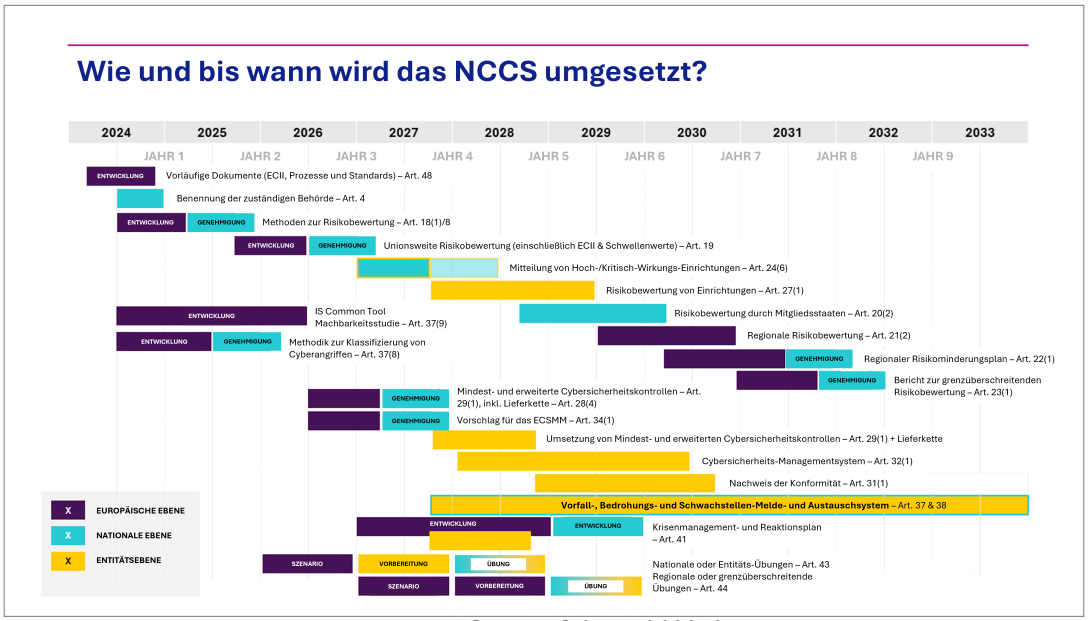
Chapter 5

Zeitplan für die Umsetzung

Der Netzkodex für Cybersicherheit NCCS wurde am 24. Mai 2024 offiziell verabschiedet.

Die Verordnung trat unmittelbar nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Hier können Sie die Zeitleiste sehen:



Zum Vergrößern auf das Bild klicken

Chapter 6

Cybersicherheitsrahmen

In diesem Kapitel werden die Grundlagen des gemeinsamen Rahmens für die Cybersicherheit im Elektrizitätssektor erläutert.

Sie lernen die Bedeutung von Mindest- und erweiterten Kontrollen, den Mapping-Matrix, den Perimeter mit kritischer Auswirkung, den Perimeter mit erheblicher Auswirkung und den Cybersicherheitsmanagementsystem des Rahmenwerks kennen.

6.1 Cybersicherheitsrahmen für den Elektrizitätssektor

NOTE

Bitte beachten Sie, dass die Untertitel des Videos mithilfe von KI-Tools erstellt wurden, wodurch möglicherweise Fehler auftreten können.

Mit der NCCS-Verordnung (NCCS Artikel 28 [1]) wird ein gemeinsamer Cybersicherheitsrahmen für den Elektrizitätssektor geschaffen, der darauf abzielt, Cybersicherheitsrisiken in der gesamten Europäischen Union wirksam zu handhaben. Ziel des Rahmens ist es, die Cybersicherheitsanforderungen und -praktiken der Mitgliedstaaten im Elektrizitätssektor zu harmonisieren.

Der Cybersicherheitsrahmen besteht aus mehreren Komponenten:

- Mindest- und erweiterte Cybersicherheitskontrollen, die gemäß NCCS Artikel 29 [2] und NCCS Artikel 33 [3] entwickelt wurden.

Mapping-Matrix festgelegt in NCCS Artikel 34 [4].

- Cybersicherheitsmanagementsystem definiert in NCCS Artikel 32 [5].

In den folgenden Kapiteln werden diese Themen und das Konzept des Geltungsbereichs ausführlicher beschrieben.

6.2 Mindest- und erweiterte Cybersicherheitskontrollen

Artikel NCCS 29 [6]

Gemäß Artikel 29 Absatz 1 des NCCS [7] müssen die **Übertragungsnetzbetreiber** innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des EU-weiten Berichts zur Bewertung der Cybersicherheitsrisiken mit Unterstützung des ENTSO (Strom) und in Zusammenarbeit mit den DSO der EU einen Vorschlag für **Mindest- und erweiterte Cybersicherheitskontrollen** ausarbeiten.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_34
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29

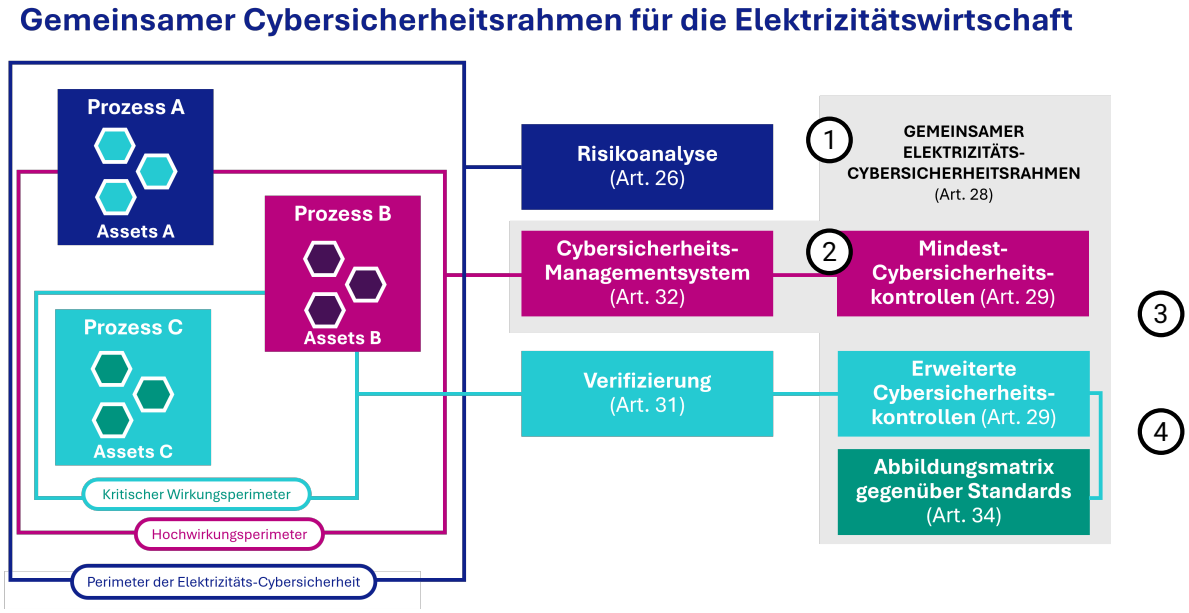
Die Mindest- und erweiterten Cybersicherheitskontrollen können nach dem in NCCS Artikel 31 [8] beschriebenen Verfahren auf der Grundlage der Teilnahme am nationalen System zur Prüfung der Einhaltung der Vorschriften oder durch die Durchführung von Sicherheitsaudits durch einen unabhängigen Dritten gemäß den in NCCS Artikel 25 Absatz 2 [9] aufgeführten Anforderungen geprüft werden.

Die gemäß NCCS Artikel 29 Absatz 1 [10] entwickelten grundlegenden Mindest- und erweiterten Cybersicherheitskontrollen stützen sich auf die Risiken, die im EU-weiten Bericht zur Bewertung des Cybersicherheitsrisikos gemäß NCCS Artikel 19 Absatz 5 [11] ermittelt wurden. Die gemäß NCCS Artikel 29 Absatz 2 [12] entwickelten modifizierten Mindest- und erweiterten Cybersicherheitskontrollen stützen sich auf den regionalen Bericht zur Bewertung des Cybersicherheitsrisikos gemäß NCCS Artikel 21 Absatz 2 [13].

Zu den Mindestkontrollen der Cybersicherheit gehören Kontrollen zum Schutz der unter NCCS Artikel 46 [14] ausgetauschten Informationen.

Die Übertragungsnetzbetreiber (ÜNB) entwickeln gemeinsam mit dem ENTSO-E und dem EU-DSB **Mindest- und erweiterte Kontrollvorschläge zur Cybersicherheit** für die Lieferkette (NCCS Artikel 33 [15]) in Übereinstimmung mit den Mindest- und erweiterten Kontrollen (NCCS Artikel 29 [16]).

[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_31
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19
[12] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_21
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_46
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_33
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_29



1

Risikobewertung Gemäss Artikel 26 des NCCS (NCCS Artikel 26 [17]) ist die Risikobewertung ein strukturierter Prozess, der darauf abzielt, das Netzwerk und die Informationssysteme der Organisation zu schützen. Alle Organisationen mit erheblicher und kritischer Auswirkung müssen alle drei Jahre eine Risikobewertung durchführen. Dieses Verfahren stellt sicher, dass die Organisationen die Sicherheitslage ihrer Systeme kontinuierlich bewerten, potenzielle Bedrohungen und Schwachstellen ermitteln und geeignete Maßnahmen zur Risikominderung ergreifen. Es handelt sich dabei um ein wesentliches Verfahren zur Aufrechterhaltung der Integrität und Widerstandsfähigkeit kritischer Infrastrukturen angesichts der sich entwickelnden Herausforderungen im Bereich der Cybersicherheit.

2

Dieses System schreibt einen umfassenden Ansatz für das Cybersicherheitsmanagement auf Unternehmensebene vor. Das System umfasst beispielsweise die Entwicklung von Cybersicherheitsrichtlinien, die Zuweisung von Verantwortlichkeiten, die Durchführung von Risikobewertungen und die Bereitstellung der erforderlichen Ressourcen. Seine Kernkomponenten sollen sicherstellen, dass die Einrichtung proaktiv mit Cybersicherheitsrisiken umgeht, klare Rollen und Verantwortlichkeiten festlegt und die zum Schutz vor potenziellen Bedrohungen und Schwachstellen erforderlichen Ressourcen bereitstellen kann. Dieses System dient als grundlegender Rahmen für den fortlaufenden Schutz und die Widerstandsfähigkeit der Vermögenswerte der Organisation angesichts der sich entwickelnden Cyber-Bedrohungen.

3

[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

Mindest- und erweiterte Cybersicherheitskontrollen

Einrichtungen mit kritischer und erheblicher Auswirkung werden die Mindest-Cybersicherheitskontrollen im Rahmen des Bereichs mit erheblicher Auswirkung anwenden, während Einrichtungen mit kritischer Auswirkung die erweiterten Cybersicherheitskontrollen im Rahmen des Bereichs mit kritischer Auswirkung anwenden werden.

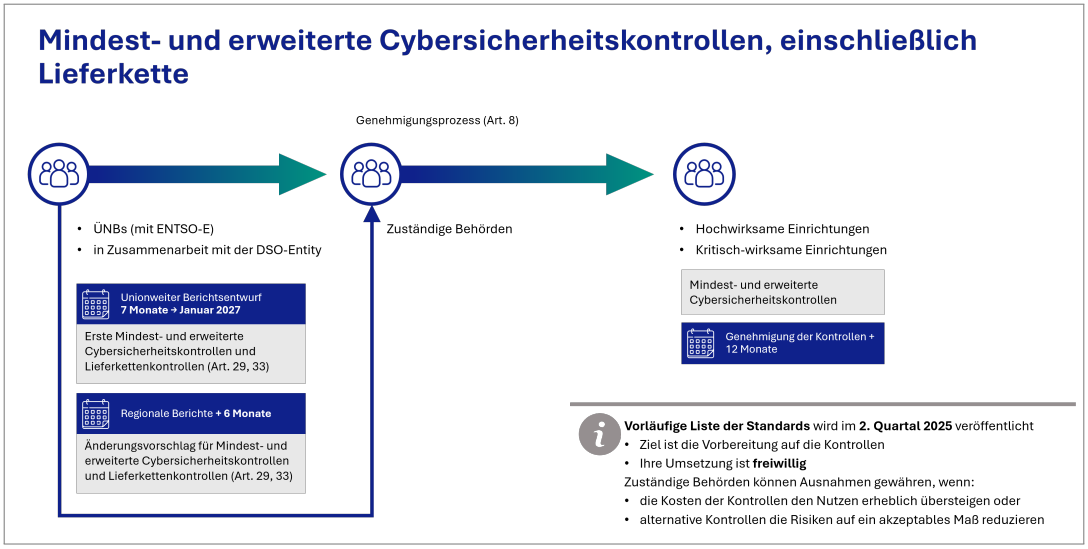
4

Mapping-Matrix

Die in den Buchstaben a und b von (NCCS Artikel 28 Absatz 1 [18]) definierten Kontrollen dienen als Matrix, um die Einhaltung ausgewählter europäischer und internationaler Normen sowie einschlägiger technischer Spezifikationen, einschließlich der geltenden nationalen Normen gemäß (Richtlinie (EU) 2022/2555 Artikel 5 [19]), zu gewährleisten.

GOOD TO KNOW

ACHTUNG: Eine vorläufige Liste von europäischen und internationalen Normen und Kontrollen wird **bis zum 13. Juni 2025** veröffentlicht. Die Umsetzung wird auf **freiwilliger Basis** erfolgen und kann Organisationen darauf vorbereiten, Mindest- und erweiterte Kontrollen durchzuführen. **Organisationen mit kritischer und erheblicher Auswirkung werden Mindest-Cybersicherheitskontrollen innerhalb des Bereichs mit erheblicher Auswirkung und erweiterte Cybersicherheitskontrollen innerhalb des Bereichs mit kritischer Auswirkung anwenden.**



[18] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#art_25

GOOD TO KNOW

Organisationen können bei der zuständigen Behörde eine Befreiung von der Verpflichtung zur Durchführung von Mindest- und erweiterten Cybersicherheitskontrollen beantragen.

Die zuständige Behörde kann eine solche Befreiung gewähren, wenn die Organisation:

- nachweisen kann, dass die Kosten für die Implementierung geeigneter Cybersicherheitskontrollen den Nutzen deutlich übersteigen; oder
- legt einen Plan zur Risikobewertung auf Organisationsebene vor, der die Cybersicherheitsrisiken unter Verwendung alternativer Kontrollmaßnahmen auf ein akzeptables Niveau reduziert, in Übereinstimmung mit den Risikoakzeptanzkriterien. Die zuständige Behörde hat dann drei Monate Zeit, um zu entscheiden, ob die Ausnahme von den Mindest- und erweiterten Cybersicherheitskontrollen gewährt werden kann.

Die Ausnahmen werden für einen Zeitraum von bis zu drei Jahren gewährt, mit der Möglichkeit einer Verlängerung.

6.3 Mapping-Matrix

NCCS Artikel 34 [20]

Mapping-Matrix für die Cybersicherheitskontrollen- und Normen im Elektrizitätssektor

Innerhalb von sieben Monaten nach Vorlage des ersten Entwurfs des EU-weiten Berichts zur Bewertung des Cybersicherheitsrisikos unter NCCS Artikel 19 Absatz 4 [21] erarbeiten die **TSOs** mit Unterstützung des ENTSO (Strom) und in Zusammenarbeit mit dem DSO der EU sowie in Absprache mit der ENISA **einen Vorschlag** für die Ausarbeitung eines Berichts zur Bewertung des Cybersicherheitsrisikos für den EU-weiten Bericht zur Bewertung der Cybersicherheit unter NCCS Artikel 28 Absatz 4 [22]. Der ENTSO (Strom) und der EU DSO dokumentieren die Gleichwertigkeit der verschiedenen Kontrollen und der in NCCS Artikel 28 Artikel 1 [23] (a) und (b) definierten Kontrollen mit den ausgewählten europäischen und internationalen Normen und relevanten technischen Spezifikationen (Mapping-Matrix).

Wird eine solche Zuordnung (mapping) von einer zuständigen Behörde eines Mitgliedstaats bereitgestellt, so integrieren der ENTSO-E und der EU-DSO diese nationale Zuordnung in die Mapping-Matrix.

[20] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_34
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19
[22] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[23] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28

6.4 Cybersicherheitsmanagementsystem

NCCS Artikel 32 [24]

Innerhalb von 24 Monaten, nachdem sie von der zuständigen Behörde darüber informiert wurden, dass sie gemäß NCCS Artikel 24 Absatz 6 [25] als Organisation mit erheblicher oder kritischer Auswirkung eingestuft wurden, muss jede Organisation gemäß NCCS Artikel 32 Absatz 1 [26]

(a) den Geltungsbereich des Cybersicherheits-Managementsystems unter Berücksichtigung von Schnittstellen und Abhängigkeiten zu anderen Einrichtungen festlegen;

(b) sicherstellen, dass das gesamte obere Management über relevante rechtliche Verpflichtungen informiert ist und aktiv durch rechtzeitige Entscheidungen und rasche Reaktionen zur Umsetzung des Cybersicherheits-Managementsystems beiträgt;

(c) sicherstellen, dass die für das Cybersicherheits-Managementsystem benötigten Ressourcen verfügbar sind;

(d) eine Cybersicherheitspolitik festlegen, die dokumentiert und innerhalb der Organisation sowie gegenüber von den Sicherheitsrisiken betroffenen Parteien kommuniziert wird;

(e) Zuständigkeiten für cybersicherheitsrelevante Rollen zuweisen und kommunizieren;

(f) Cybersicherheits-Risikomanagement auf Einrichtungsebene durchführen, wie in NCCS Artikel 26 [27] festgelegt;

(g) die für die Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung des Cybersicherheits-Managementsystems erforderlichen Ressourcen ermitteln und bereitstellen, wobei die notwendige Kompetenz und das Bewusstsein im Bereich Cybersicherheit berücksichtigt werden;

(h) die für die Cybersicherheit relevante interne und externe Kommunikation festlegen;

(i) Erstellung, Aktualisierung und Kontrolle dokumentierter Informationen über das Cybersicherheitsmanagementsystem;

(j) Bewertung der Leistung und Wirksamkeit des Cybersicherheitsmanagementsystems;

(k) Durchführung von internen Audits in geplanten Abständen, um sicherzustellen, dass das Cybersicherheitsmanagementsystem wirksam umgesetzt und aufrechterhalten wird;

(l) Überprüfung der Umsetzung des Cybersicherheits-Managementsystems in geplanten Abständen und Kontrollieren bzw. Korrigieren der Nichteinhaltung der Strategien, Verfahren und Leitlinien des Cybersicherheits-Managementsystems durch die Ressourcen und Aktivitäten.

[24] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[25] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[26] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[27] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

GOOD TO KNOW

Innerhalb von 24 Monaten nach **Identifizierung** müssen alle Organisationen mit erheblicher und kritischer Auswirkung **ein Cybersicherheits-Managementsystem** einrichten und **dieses System danach alle drei Jahre überprüfen**. Gemäß NCCS Artikel 32 Absatz 2 [a] muss der Geltungsbereich des Cybersicherheits-Managementsystems alle Vermögenswerte umfassen, die in den Geltungsbereich der Organisation mit erheblicher und kritischer Auswirkung fallen.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32

6.5 Perimeters

12 Monate nach der Genehmigung der Mindest- und erweiterten Cybersicherheitskontrollen unter NCCS Artikel 8 Absatz 5 [28] oder deren Aktualisierung unter NCCS Artikel 8 Absatz 10 [29], die in NCCS Artikel 2 Absatz 1 [30] des NCCS aufgeführten und als kritischer Auswirkung oder erheblicher Auswirkung bezeichneten Organisationen unter NCCS Artikel 24 [31] des NCCS aufgeführt sind, müssen gemäß NCCS Artikel 26 Absatz 5 [32] des NCCS bei der Ausarbeitung ihres Plans zur Risikominderung auf Unternehmensebene Mindest-Cybersicherheitskontrollen innerhalb des Bereichs mit erheblicher Auswirkung und erweiterte Cybersicherheitskontrollen innerhalb des Bereichs mit kritischer Auswirkung anwenden.

Anforderungen an die Einhaltung der Vorschriften für Unternehmen mit kritischer Auswirkung

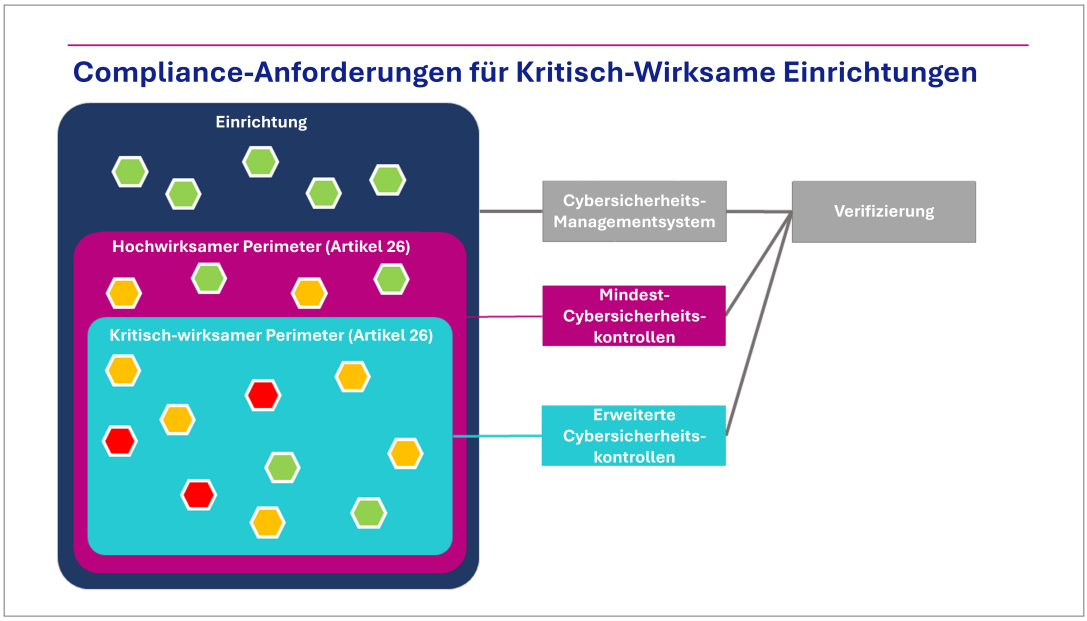
GOOD TO KNOW

Perimeter mir kritischer Auswirkung

Die von der Organisation festgelegte physische und/oder logische Trennung (z. B. Umzäu-

[28] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[29] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[30] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_2
[31] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[32] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art26

nung, Serverräume, Firewalls, Proxyserver usw.), die alle **erheblicher Auswirkung** **und** **Vermögenswert mit kritischen Auswirkungen** sowie alle anderen Geräte umfasst, die sich innerhalb dieser Trennung befinden.

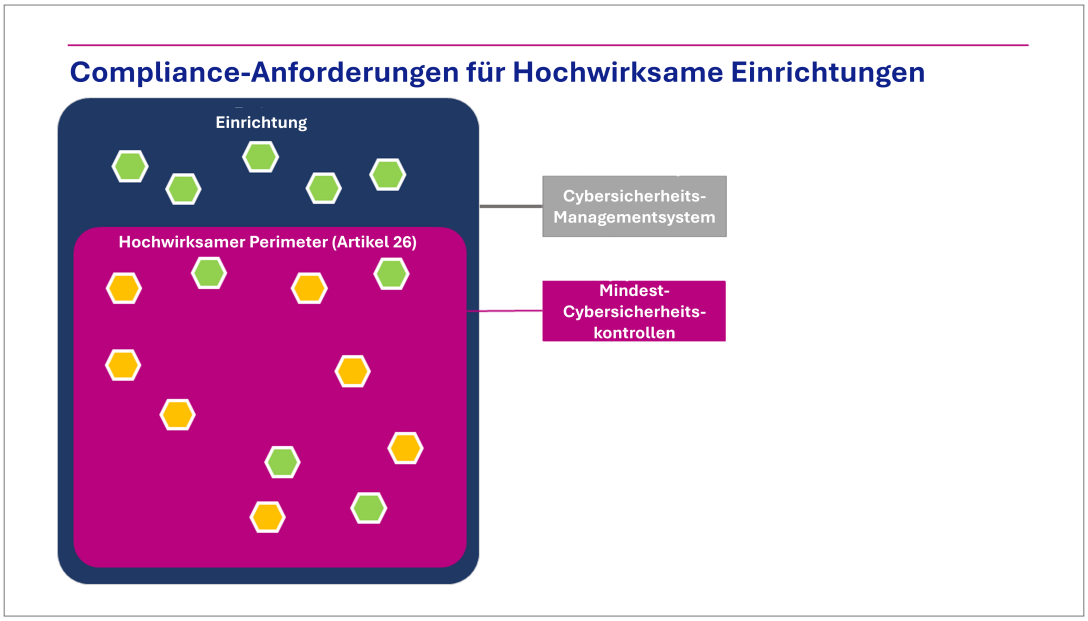


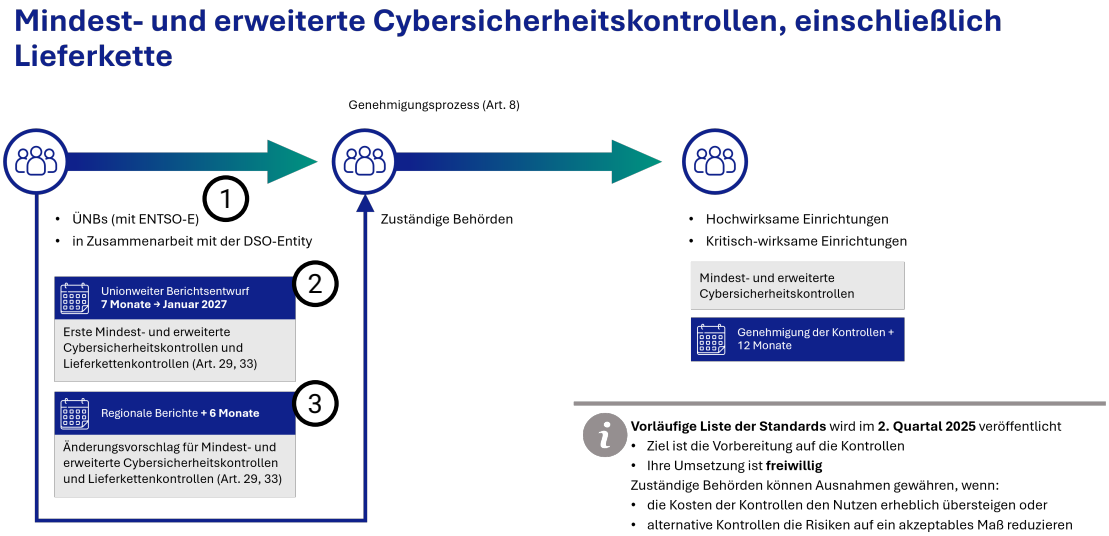
Anforderungen an die Einhaltung der Vorschriften für Organisation mit erheblicher Auswirkung

GOOD TO KNOW

Perimeter mit erheblicher Auswirkung

Die von den Organisationen festgelegte physische und/oder logische Trennung (z.?B. Umzäunung, Serverräume, Firewalls, Proxy-Server usw.), die alle Geräte mit erheblicher Auswirkung sowie alle anderen Geräte umfasst, die sich innerhalb dieser Trennung befinden.





(1)

Die Übertragungsnetzbetreiber (ÜNB) werden mit Unterstützung von ENTSO-E und der DSO-Organisation einen Vorschlag für die Mindest- und erweiterten Cybersicherheitskontrollen ausarbeiten.“

2

Die zuständigen Behörden haben anschließend sechs Monate Zeit, um auf Grundlage des Vorschlags eine Entscheidung über die Mindest- und erweiterten Cybersicherheitskontrollen zu treffen.“

3

Anschließend, im Januar 2028, werden Organisationen mit kritischer und erheblicher Auswirkung die Mindestcybersicherheitskontrollen im Bereich mit erheblicher Auswirkung anwenden sowie die erweiterten Cybersicherheitskontrollen im Bereich mit kritischer Auswirkung.

Chapter 7

Nationale Verifizierungssysteme

Das nationale Verifizierungssystem kann auf einer von der zuständigen Behörde durchgeführten Inspektion, auf unabhängigen Sicherheitsprüfungen oder auf gegenseitigen Peer-Reviews durch Organisationenn mit kritischer Auswirkung im selben Mitgliedstaat basieren, die von der zuständigen Behörde überwacht werden.

Das Personal, das die Peer-Review, Prüfung oder Inspektion durchführt, muss über nachweisbare Kenntnisse verfügen in folgenden Bereichen:

(i) Cybersicherheit im Elektrizitätssektor;

(ii) Cybersicherheitsmanagementsystems;

(iii) die Grundprinzipien der Auditierung;

(iv) Cybersicherheitsrisikobewertung;

(v) gemeinsamer Cybersicherheitsrahmen für den Elektrizitätssektor;

(vi) die nationalen Rechts- und Verwaltungsvorschriften sowie die europäischen und internationalen Normen im Rahmen der Verifizierung;

(vii) Die Verifikation der in den Geltungsbereich des Verifikationsprogramms fallenden Prozesse mit kritischer Auswirkung kann auf der Grundlage einer von der zuständigen Behörde durchgeführten Inspektion, unabhängiger Sicherheitsaudits oder gegenseitiger Peer Rewies durch Organisationenn mit kritischer Auswirkung in demselben Mitgliedstaat erfolgen, die von der zuständigen Behörde beaufsichtigt werden.

Chapter 8

Risikobewertung gemäß der NCCS-Verordnung

Das Ziel dieses Kapitels ist es, den Risikobewertungsprozess gemäß der NCCS-Verordnung darzustellen.

Die Risikobewertung ist ein Eckpfeiler des NCCS; die **Risikobewertung wird zyklisch auf EU-, regionaler, Mitgliedstaaten- und Organisationsebene durchgeführt**. Die Verordnung schreibt die Entwicklung und Anwendung von Risikobewertungsmethoden auf EU- und regionaler Ebene vor. Bei der Risikobewertung müssen potenzielle Cyberbedrohungen, Schwachstellen und die möglichen Auswirkungen von Cyberangriffen berücksichtigt werden.

8.1 Zyklus zur Bewertung von Cybersicherheitsrisiken

NOTE

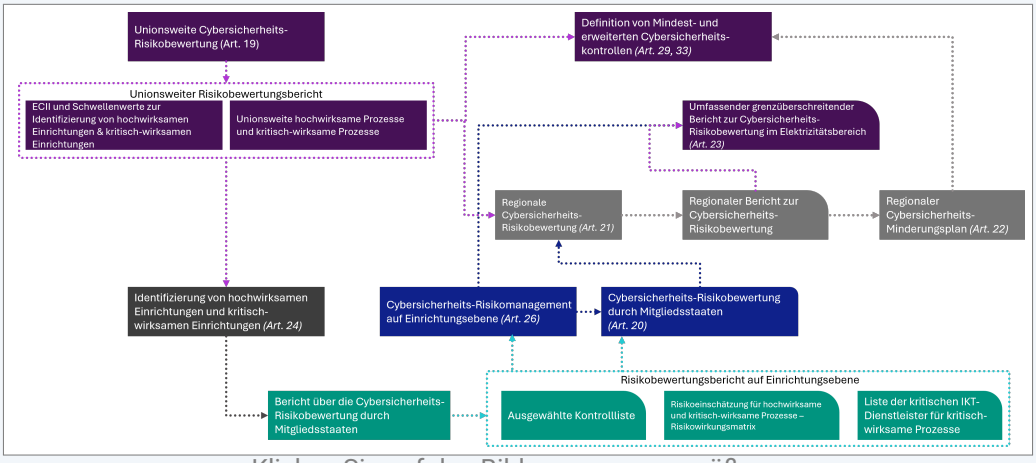
Die Untertitel des Videos wurden mit KI-Tools erstellt, daher können Fehler enthalten sein.

Die NCCS-Verordnung schreibt einen **strukturierten Prozess** für die Identifizierung und Bewertung von Cybersicherheitsrisiken im europäischen Elektrizitätssektor vor. Die **Risikobewertung** ist das zentrale Element dieses Prozesses und **findet zyklisch auf mehreren Ebenen** statt (EU-Ebene, regionale Ebene, Ebene der Mitgliedstaaten, Ebene der Organisationen).

GOOD TO KNOW

Ziel der Risikobewertung ist es, Cybersicherheitsrisiken zu identifizieren, die grenzüberschreitende Stromflüsse auf verschiedenen Ebenen (EU-Ebene, regionale Ebene, Ebene der Mitgliedstaaten, Unternehmensebene) bedrohen.

Der Zyklus umfasst die folgenden Stufen und Schritte:



Klicken Sie auf das Bild, um es zu vergrößern.

8.2 Methoden zur Bewertung von Cybersicherheitsrisiken

Artikel 18 des NCCS [1] behandelt die Methodik zur Cybersicherheits-Risikobewertung.

Zeitleiste	Stufen
Der Prozess zur Bewertung der Cybersicherheitsrisiken wird im März 2025 beginnen, wenn ENTSO-E und die EU-DSO-Organisationen in Absprache mit der NIS-Kooperationsgruppe die Bewertungsmethoden entwickeln werden.	* Union * Regional * Mitgliedstaaten

Risikobewertungsmethode

Die Methoden zur Bewertung von Cybersicherheitsrisiken auf EU-, regionaler und Mitgliedstaatenebene umfassen Folgendes:

a) Die Liste der zu untersuchenden Cyber-Bedrohungen, einschließlich mindestens der folgenden Bedrohungen, die die Lieferkette betreffen:

- schwere und unerwartete Störung der Lieferkette
- Fehlen des IKT-Produkte, IKT-Dienstleistungen oder IKT-Prozesse in der Lieferkette.
- Cyberangriffe, die über Teilnehmer der Lieferkette initiiert werden;
- Weitergabe sensibler Informationen über die Lieferkette, einschließlich der Nachverfolgung der Lieferkette;
- die Einführung von Schwachstellen oder Hintertüren in IKT-Produkten, IKT-Dienstleistungen oder IKT-Prozessen durch Akteure der Lieferkette.

b) Kriterien zur Bewertung der hohen oder kritischen Auswirkungen von Cybersicherheitsrisiken unter Verwendung des definierten Schwellenwerte für Folgen und Wahrscheinlichkeit;

c) Ein Ansatz zur Analyse von Cybersicherheitsrisiken, die sich aus dem Begriff „legacy" (veraltete Systeme), den Kaskadeneffekten von Cyberangriffen und der Echtzeit-Natur der Systeme, die das Netzwerk betreiben, ergeben.

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

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18

Matrix der Risikoauswirkungen

NCCS Artikel 18 Absatz 2 [2]

a) Die **Folgen von Cyberangriffen** anhand der folgenden Kriterien bewerten:

i. Lastverlust;

ii. Reduzierung der Stromerzeugung;

iii. Verlust von Kapazität in der Primärfrequenzreserve;

iv. Verlust an Kapazität zur Wiederherstellung des Betriebs eines Elektrizitätsnetzes ohne Rückgriff auf das externe Übertragungsnetz nach einem vollständigen oder teilweisen Ausfall (sogenannter ‚Black Start')"

v. die voraussichtliche Dauer eines Stromausfalls, von dem Kunden betroffen sind, in Verbindung mit dem Ausmaß des Ausfalls in Bezug auf die Anzahl der Kunden; und

vi. alle anderen quantitativen oder qualitativen Kriterien, die vernünftigerweise als Indikator für die Auswirkungen eines Cyberangriffs auf grenzüberschreitende Stromflüsse dienen könnten;

b) Die **Wahrscheinlichkeit eines Vorfalls** wird als Häufigkeit von Cyberangriffen pro Jahr gemessen.

GOOD TO KNOW

Die Methoden zur Bewertung von Cybersicherheitsrisiken auf EU-Ebene, regionaler Ebene und auf Ebene der Mitgliedstaaten bewerten Cybersicherheitsrisiken unter Verwendung desselben Riskoauswirkungsmatrix.

8.3 Cybersicherheits-Risikobewertung auf Organisationsebene

NCCS Artikel 26 [3] und NCCS Artikel 27 [4] beschreiben die Einzelheiten der Bewertung und des Managements von Cybersicherheitsrisiken auf Organisationsebene.

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27

Gemäß NCCS Artikel 26 Absatz 2 [5] muss während der Phase des Cybersicherheits-Risikomanagements jede Organisation mit erheblicher und kritischer Auswirkung einen Risikominderungsplan auf Organisationsenebene für alle Vermögenswerte innerhalb des erheblichen und kritischen Perimeters entwickeln und alle drei Jahre eine Risikobewertung durchführen.

Die Organisation analysiert die Wahrscheinlichkeit und die Folgen der identifizierten Cybersicherheitsrisiken und ermittelt den Cybersicherheitsrisikograd anhand der Risiko-Auswirkungs-Matrix, die von den Übertragungsnetzbetreibern (TSOs) in Zusammenarbeit mit ENTSO-E für den Strommarkt und den EU-DSO gemäß NCCS Artikel 19 Absatz 2 [6], entwickelt wurde, wobei Methoden zur Bewertung von Cybersicherheitsrisiken auf EU-Ebene, regionaler Ebene und auf Ebene der Mitgliedstaaten integriert werden.

Gemäß NCCS Artikel 26 Absatz 2 [7] muss jede Organisation der Kategorien erheblicher Auswirkung und kritischer Auswirkung ihr Cybersicherheitsrisikomanagement auf einen Ansatz stützen, der auf den Schutz ihres Netzwerks und ihrer Informationssysteme abzielt und aus den folgenden Phasen besteht:

a) Den Kontext herstellen;

b) Durchführung einer Cybersicherheits-Risikobewertung auf Organisationsebene;

c) Management von Cybersicherheitsrisiken;

d) Akzeptanz von Cybersicherheitsrisiken.

Zeitleiste	Stufen
* **Identifizierung von Organisationen mit erheblicher und kritischer Auswirkung + 12 Monate. * Alle 3 Jahre**	* Organisation mit kritischer Auswirkung * Organisation mit erheblicher Auswirkung

Die Schritte des Verfahrens sind wie folgt:

1. Festlegung des Umfangs unter Berücksichtigung Prozesse mit erheblicher Auswirkung, Prozesse mit kritischer Auswirkung oder anderer Prozesse.
2. Festlegung der Kriterien für die Risikobewertung und -akzeptanz (Risiko-Auswirkungs-Matrix).
3. Identifizierung von Cybersicherheitsrisiken, Cyberbedrohungen, Schwachstellen und Cyberangriffsszenarien unter Berücksichtigung von Risikobewertungen auf EU-Ebene.

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

4. Analyse der Wahrscheinlichkeit und der Folgen von Cybersicherheitsrisiken unter Verwendung der Risiko-Auswirkungs-Matrix.
5. Klassifizierung von Vermögenswerten auf der Grundlage der Folgen einer potenziellen Gefährdung sowie Bestimmung von Bereichen mit erheblichen und kritischen Auswirkungen unter Verwendung ECII.
6. Bewertung von Cybersicherheitsrisiken durch deren Rangfolge.
7. Entwicklung eines Plans zur Risikominderung auf Organisationsebene.
8. Entscheidung darüber, ob das Restrisiko auf der Grundlage der Risikoakzeptanzkriterien akzeptabel ist.
9. Führen eines Bestandsverzeichnisses aller Vermögenswerte innerhalb des Bereichs mit erheblicher und kritischer Auswirkung. Dieses Bestandsverzeichnis ist nicht Teil des Risikobewertungsberichts.

Resultate

Berichte über die Cybersicherheits-Risikobewertung auf Organisationsebene:

Bericht zur Bewertung von Cybersicherheitsrisiken auf Organisationsebene gemäß dem Gesetz über Cybersicherheit und Cybersicherheit (NCCS Artikel 27 [8]). Alle Organisationen mit erheblicher oder kritischer Auswirkung müssen innerhalb von 12 Monaten nach ihrer Einstufung als Organisation mit erheblicher oder kritischer Auswirkung einen Bericht bei der zuständigen Behörde einreichen und anschließend alle drei Jahre.

Der Bericht muss folgende Informationen enthalten:

- Eine **Liste ausgewählter Kontrollen** aus dem Risikominderungsplan auf Organisationensebene, wie im (NCCS Artikel 26 Absatz 5 [9]) vorgeschrieben, zusammen mit dem aktuellen Umsetzungsstatus jeder Kontrollmaßnahme.
- **Risikoeinschätzung** in Bezug auf die Gefährdung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten für jeden Prozess auf EU-Ebene, jeden Prozess mit erheblicher Auswirkung und jeden Prozess mit kritischer Auswirkung. Diese Risikoeinschätzung muss der in NCCS Artikel 19 Absatz 2 [10] festgelegten Risiko-Auswirkungs-Matrix entsprechen.
- Eine Liste von Anbietern von kritischen IKT-Diensten, die für ihre Prozesse mit kritischer Auswirkungen unerlässlich sind.

[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_19

GOOD TO KNOW

- Nach der Identifizierung von Organisationen mit erheblicher und kritischer Auswirkung muss innerhalb von 12 Monaten eine Risikobewertung auf Organisationensebene durchgeführt werden, die alle drei Jahre wiederholt werden sollte.

8.4 Cybersicherheitsrisikobewertung auf Ebene der Mitgliedstaaten

NCCS Artikel 20 [11]

Jede zuständige Behörde führt eine Cybersicherheitsrisikobewertung für alle Organisationen mit erheblicher und kritischer Auswirkung in ihrem Mitgliedstaat durch, wobei sie die gemäß Artikel 18 des Gesetzes über die Cybersicherheit (NCCS Artikel 18 [12]) entwickelten und gemäß NCCS Artikel 8 [13] genehmigten Methoden anwendet. **Die Cybersicherheitsrisikobewertung der Mitgliedstaaten muss die Risiken von Cyberangriffen identifizieren und analysieren, die die Betriebssicherheit des Stromnetzes beeinträchtigen und grenzüberschreitende Stromflüsse stören.** Die Cybersicherheitsrisikobewertung der Mitgliedstaaten darf die rechtlichen, finanziellen oder reputationsbezogenen Folgen von Cyberangriffen nicht berücksichtigen.

Innerhalb von 21 Monaten nach der Benachrichtigung der Organisation mit erheblicher und kritischer Auswirkung gemäß NCCS Artikel 24 Absatz 6 [14] und danach alle drei Jahre sowie nach Rücksprache mit der für Elektrizität zuständigen CS-NCA muss jede zuständige Behörde mit Unterstützung der CSIRT einen Bericht über die Bewertung der Cybersicherheitsrisiken in den Mitgliedstaaten an das ENTSO für Elektrizität und die EU-DSO-Organisation vorlegen, der für jeden Geschäftsprozess mit erheblicher und kritischer Auswirkung die folgenden Informationen enthält:

a) der Stand der Umsetzung der Mindest- und erweiterten Cybersicherheitskontrollen gemäß dem Nationalen Cybersicherheitskontrollsystem (NCCS Artikel 29 [15]);

b) eine Liste aller Cyberangriffe, die in den letzten drei Jahren gemäß dem Gesetz über die nationale Cybersicherheit (NCCS Artikel 38 Absatz 3 [16]) gemeldet wurden ;

c) eine Zusammenfassung der in den letzten drei Jahren gemäß dem Gesetz über das nationale Cybersicherheitszentrum (NCCS Artikel 38 Absatz 6 [17]) gemeldeten Informationen zu Cyberbedrohungen ;

[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_20
[12] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38

d) für jeden unionsweiten Prozess mit erheblicher oder kritischer Auswirkung eine Abschätzung der Risiken einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten;

e) Falls erforderlich, eine Liste zusätzlicher Organisationen, die gemäß dem Gesetz über die nationale Sicherheit und die Sicherheit der kritischen Infrastruktur (NCCS Artikel 24 Absatz 2, 3, 5 [18]) als Organisationen mit erheblicher oder kritischer Auswirkung eingestuft wurden .

Der Bericht des Mitgliedstaats über die Bewertung der Cybersicherheitsrisiken berücksichtigt den gemäß VERORDNUNG (EU) 2019/941 DES EUROPÄISCHEN PARLAMENTS Artikel 10 [19] festgelegten Risikovorsorgeplan des Mitgliedstaats.

Die im Bericht über die Bewertung der Cybersicherheitsrisiken der Mitgliedstaaten enthaltenen Informationen dürfen nicht mit bestimmten Organisationen oder Vermögenswerten in Verbindung gebracht werden. Der Bericht zur Bewertung der Cybersicherheitsrisiken des Mitgliedstaats muss auch eine Risikobewertung der vorübergehenden Ausnahmeregelungen enthalten, die von den zuständigen Behörden der Mitgliedstaaten gemäß Artikel 30 des Rechtsakts über die Cybersicherheit (NCCS Artikel 30 [20]) erlassen wurden.

[18] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0941#art_10
[20] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_30

Chapter 9

Lieferkette

Jüngste Cyberangriffe zeigen, dass Organisationen zunehmend Ziel von Angriffen auf Lieferketten werden. Solche Angriffe betreffen nicht nur einzelne unter diese Verordnung fallende Organisationen, sondern können auch Kaskadeneffekte auslösen, die zu groß angelegten Angriffen auf über das Elektrizitätsnetz verbundene Einrichtungen führen.

Zweck dieses Kapitels ist es, die Abschnitte der NCCS-Verordnung darzustellen, die sich mit den **Mindest- und erweiterten Cybersicherheitskontrollen im Zusammenhang mit Lieferketten** befassen, sowie die unverbindlichen Empfehlungen zur Beschaffung im Bereich der Cybersicherheit.

9.1 Überblick über die Cybersicherheit in Lieferketten

NOTE

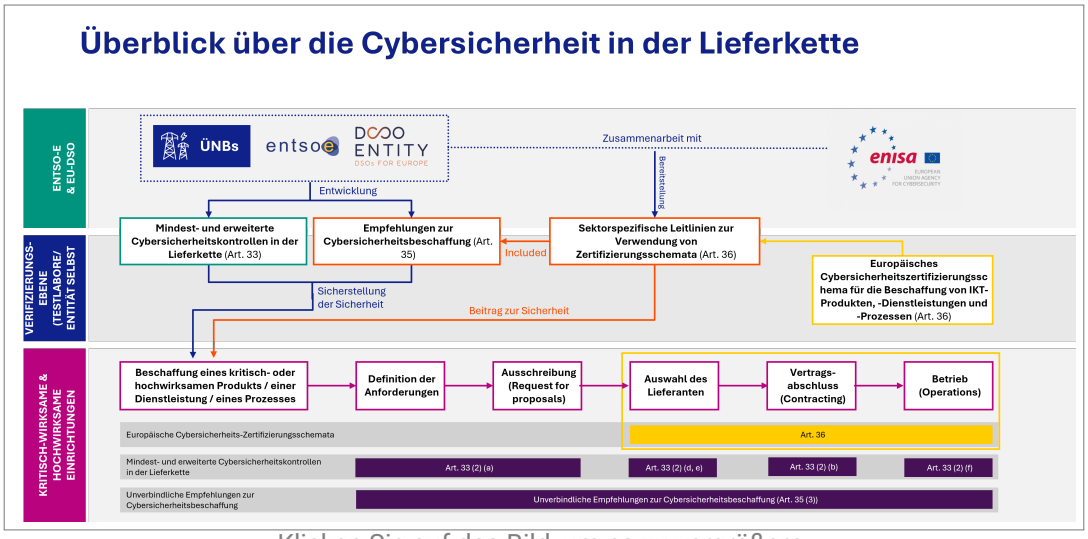
Die Untertitel des Videos wurden mit KI-Tools erstellt, daher können Fehler enthalten sein.

9.2 Mindest- und erweiterte Cybersicherheitskontrollen und Empfehlungen in der Lieferkette

Übertragungsnetzbetreiber (ÜNB) entwickeln in Zusammenarbeit mit ENTSO-E und dem EU-DSO Mindest- und erweiterte Empfehlungen für Cybersicherheitskontrollen für die Lieferkette (NCCS Artikel 33 [1]) in Übereinstimmung mit den Mindest- und erweiterten Kontrollen (NCCS Artikel 29 [2]) sowie den nicht verbindlichen Empfehlungen zur Beschaffung von Cybersicherheit (NCCS Artikel 35 [3]) zu erfüllen. Diese Empfehlungen können von erheblichen und kritischen betroffenen Stellen bei der Beschaffung von IKT-Produkten, IKT-Dienstleistungen und IKT-Prozessen verwendet werden, die innerhalb der erheblichen und kritischen Perimeter identifiziert wurden.

Nicht verbindliche Empfehlungen für die Beschaffung von Cybersicherheit können sektorspezifische Leitlinien für die Verwendung europäischer Cybersicherheitszertifizierungssysteme enthalten, sofern ein geeignetes System für die von Organisationen mit kritischer Ausnwirkung verwendeten IKT-Produkte, IKT-Dienstleistungen oder IKT-Prozesse verfügbar ist. Übertragungsnetzbetreiber (TSOs), ENTSO-E, die EU-DSO und ENISA arbeiten bei der Entwicklung solcher Leitlinien zusammen (NCCS Artikel 36 [4]).

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_33
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_29
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_35
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_36



Klicken Sie auf das Bild, um es zu vergrößern.

GOOD TO KNOW

Lieferanten innerhalb der Lieferkette, die von Organisationen als IKT-Dienstleister mit erheblicher oder kritischer Auswirkung identifiziert werden, werden als kritische IKT-Dienstleister eingestuft (NCCS Artikel 3 Absatz [a]).

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_3

9.3 Minimale und erweiterte Cybersicherheitskontrollen in der Lieferkette

Die Mindest- und erweiterten Cybersicherheitskontrollen in der Lieferkette gelten für die Beschaffung relevanter IKT-Produkte, IKT-Dienstleistungen und IKT-Prozesse.

Die Mindest- und erweiterten Cybersicherheitskontrollen der Lieferkette gelten für Beschaffungsprozesse in Organisationen, die gemäß NCCS Artikel 24 [5] als Organisation mit kritischer Auswirkung und gemäß NCCS Artikel 29 [6] als Organisation mit erheblicher Auswirkung identifiziert wurden. Sie gelten sechs Monate nach der Verabschiedung oder Aktualisierung der Mindest- und erweiterten Cybersicherheitskontrollen gemäß NCCS Artikel 33 Absatz 5 [7].

Innerhalb von sechs Monaten nach Fertigstellung der regionalen Cybersicherheits-Risikobewertungsberichte,

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_29
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33

wie in NCCS Artikel 21 Absatz 2 [8] vorgeschrieben ist, schlagen die Übertragungsnetzbetreiber (ÜNB) in Zusammenarbeit mit ENTSO-E für den Strommarkt und dem EU-DSO der zuständigen Behörde Änderungen an den Mindest- und erweiterten Cybersicherheitskontrollen der Lieferkette vor.

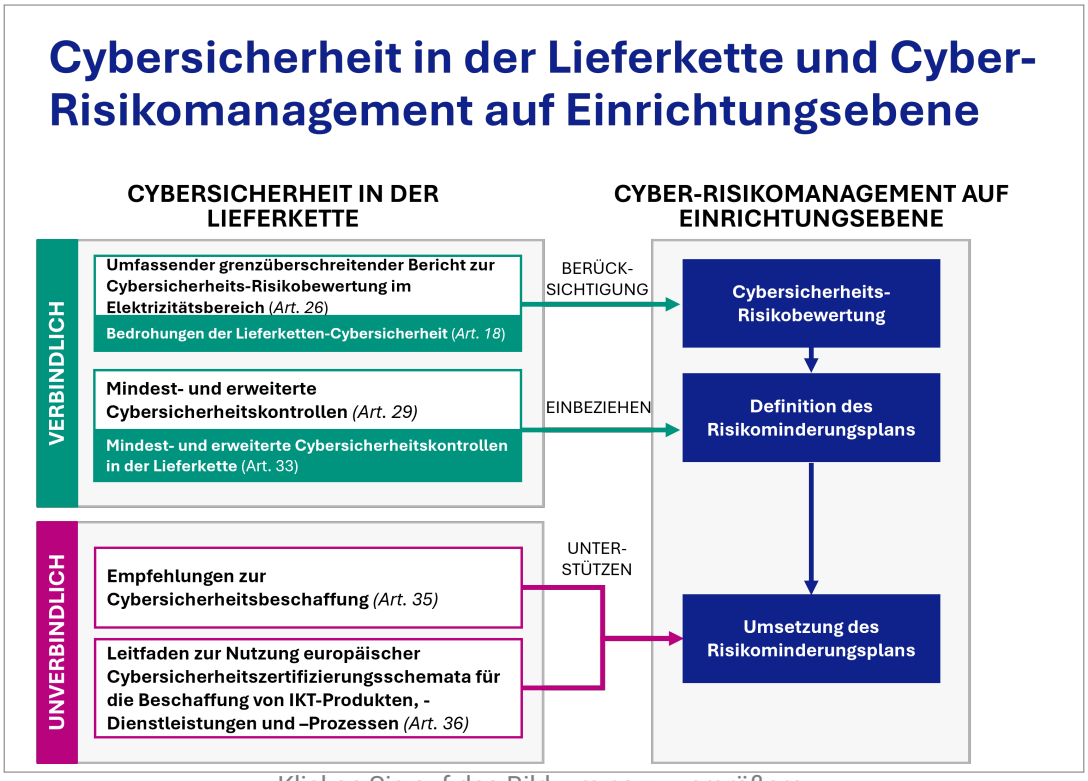
Dieser Vorschlag wird gemäß NCCS Artikel 8 Absatz 10 [9] ausgearbeitet und berücksichtigt die in der regionalen Risikobewertung ermittelten Risiken, die sich auf die Beschaffungsprozesse von Organisationen auswirken. Dies ist in NCCS Artikel 24 [10] und NCCS Artikel 33 Absatz 6 [11] festgelegt.

Während der Phase des Cybersicherheits-Risikomanagements muss jede Organisation mit erheblicher und kritischer Auswirkung einen organisationsweiten Risikominderungsplan für alle Vermögenswerte innerhalb ihrer Perimeter mit erheblicher und kritischer Auswirkung erstellen und alle drei Jahre eine Risikobewertung durchführen (NCCS Artikel 26 [12]).

Während der **Phase der Cybersicherheits-Risikobewertung** muss jede Organisation mit erheblicher und kritischer Auswirkung potenzielle Cybersicherheitsrisiken identifizieren:

- die **Cyber-Bedrohungen**, die im jüngsten umfassenden Bericht zur Bewertung der Cybersicherheitsrisiken im grenzüberschreitenden Elektrizitätssektor (NCCS Artikel 23 [13]) identifiziert wurden;
- **Potenzielle Bedrohungen für die Lieferkette** (NCCS Artikel 18 [14])

[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_21
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_8
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[12] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_23
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18



Klicken Sie auf das Bild, um es zu vergrößern.

9.4 Minimale und erweiterte Kontrollen in der Lieferkette

Die Mindestkontrollen in der Lieferkette sollten Folgendes umfassen

NCCS Artikel 33 Absatz 1 [15]:

a) Empfehlungen für die Beschaffung von IKT-Produkten, IKT-Dienstleistungen und IKT-Prozessen unter Bezugnahme auf Cybersicherheitsspezifikationen, die mindestens Folgendes umfassen:

(i) die Hintergrundüberprüfungen der Mitarbeiter des Lieferanten, die an der Lieferkette beteiligt sind und mit sensiblen Informationen umgehen oder Zugang zu den Vermögenswerten des Unternehmens mit erheblicher oder kritischer Ausnwirkung haben. Die Hintergrundüberprüfung kann eine Überprüfung der Identität und des Hintergrunds von Mitarbeitern oder Auftragnehmern einer Organisation gemäß den nationalen Rechtsvorschriften und Verfahren sowie den einschlägigen und anwendbaren Rechtsvorschriften der Union, einschließlich VERORDNUNG (EU) 2016/679 [16] und Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates Artikel 18 [17] umfassen. Hintergrundüberprüfungen müssen verhältnismäßig sein und sich streng auf das Notwendige beschränken. Sie dürfen ausschließlich zum Zweck der Bewertung eines potenziellen Sicherheit-

[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679
[17] https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

srisikos für die betreffende Organisation durchgeführt werden. Sie müssen in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der Informationen, auf die zugegriffen werden soll, und den wahrgenommenen Risiken stehen und können von der Organisation selbst, von einer externen Organisation, das eine Überprüfung durchführt, oder durch eine staatliche Sicherheitsüberprüfung durchgeführt werden.

(ii) die Verfahren für die sichere und kontrollierte Gestaltung, Entwicklung und Produktion von IKT-Produkten, IKT-Diensten und IKT-Prozessen, wobei die Gestaltung und Entwicklung von IKT-Produkten, IKT-Diensten und IKT-Prozessen gefördert wird, die geeignete technische Maßnahmen zur Gewährleistung der Cybersicherheit enthalten;

(iii) Gestaltung von Netz- und Informationssystemen, bei denen Geräten auch dann nicht vertraut wird, wenn sie sich innerhalb eines sicheren Perimeters befinden, bei denen alle eingehenden Anfragen überprüft werden müssen und das Prinzip der geringsten Privilegien angewendet wird;

(iv) der Zugang des Lieferanten zu den Vermögenswerten der Organisation;

(v) die vertraglichen Verpflichtungen des Lieferanten zum Schutz und zur Beschränkung des Zugriffs auf sensible Informationen der Organisation;

(vi) die zugrunde liegenden Cybersicherheits-Beschaffungsvorgaben für die Unterauftragnehmer des Lieferanten;

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

(viii) die Unterstützung für Sicherheitsupdates während der gesamten Lebensdauer von IKT-Produkten, IKT-Dienstleistungen oder IKT-Prozessen;

(ix) das Recht, die Cybersicherheit in den Design-, Entwicklungs- und Produktionsprozessen des Lieferanten zu überprüfen; und

(x) die Bewertung des Risikoprofils des Lieferanten;

b) diese Einrichtungen verpflichten, bei Vertragsabschlüssen mit Lieferanten, Kooperationspartnern und sonstigen Akteuren in der Lieferkette die in Buchstabe a genannten Beschaffungsempfehlungen zu berücksichtigen – und zwar sowohl bei gewöhnlichen Lieferungen von IKT-Produkten, IKT-Diensten und IKT-Prozessen als auch in Fällen ungeplanter Ereignisse und Umstände wie der Beendigung und dem Übergang von Verträgen im Falle einer Pflichtverletzung des Vertragspartners;

c) Es wird verlangt, dass diese Stellen die Ergebnisse der gemäß Artikel 22 Absatz 1 der (Richtlinie 2014/65/EU 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [18]) durchgeführten koordinierten Sicherheitsrisikobewertungen kritischer Lieferketten berücksichtigen.;

d) Kriterien für die Auswahl und Beauftragung von Lieferanten enthalten, die die in Absatz (a) genannten Cybersicherheitsspezifikationen erfüllen und über ein Maß an Cybersicherheit verfügen, das den Cybersicherheitsrisiken der vom Lieferanten bereitgestellten IKT-Produkte, IKT-Dienstleistungen oder IKT-Prozesse angemessen ist;

[18] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

e) Kriterien zur Diversifizierung der Bezugsquellen für IKT-Produkte, IKT-Dienstleistungen und IKT-Prozesse und zur Verringerung des Risikos einer Anbieterabhängigkeit aufnehmen;

f) Kriterien zur regelmäßigen Überwachung, Überprüfung oder Auditierung der Cybersicherheitsspezifikationen für die internen Betriebsprozesse der Lieferanten während des gesamten Lebenszyklus jedes IKT-Produkts, IKT-Dienstes und IKT-Prozesses enthalten.

Die erweiterten Kontrollen der Lieferkette umfassen Folgendes:

Die erweiterten Kontrollen der Lieferkette umfassen Folgendes, wie in NCCS Artikel 33 Absatz 4 [19] dargelegt:

Bei der Beschaffung umfassen die erweiterten Cybersicherheitskontrollen in der Lieferkette diejenigen Kontrollen, die für Organisationen mit kritischer Ausnwirkung gelten, um sicherzustellen, dass IKT-Produkte, IKT-Dienstleistungen und IKT-Prozesse, die als Vermögenswerte mit kritischer Ausnwirkung verwendet werden, den Cybersicherheitsanforderungen entsprechen. Das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess muss durch das in Artikel 36 des IKT-Sicherheitsgesetzes (NCCS Artikel 36 [20]) genannte europäische Cybersicherheitszertifizierungssystem zertifiziert oder durch ein von der Organisation ausgewähltes und durchgeführtes Auditverfahren überprüft werden.

Der Detaillierungsgrad und der Umfang der Verifizierungsmaßnahmen gewährleisten, dass das IKT-Produkt, die IKT-Dienstleistung oder der IKT-Prozess zur Minderung der in der Risikobewertung der Organisation identifizierten Risiken eingesetzt werden kann. Die Organisation mit kritischer Auswirkung dokumentiert die Maßnahmen, die zur Minderung der identifizierten Risiken ergriffen wurden.

9.5 Beschaffungsempfehlungen in der Lieferkette

Beschaffungsempfehlungen

Inhalt der Beschaffungsempfehlungen für Organisationen mit erhebéicher und kritischer Auswirkung

NCCS Artikel 35 Absatz 1 [21]

a) Die Beschreibung und Klassifizierung der Arten von IKT-Produkten, IKT-Dienstleistungen und IKT-Prozessen, die von Organisationen mit erheblicher Auswirkung und kritischer Auswirkung innerhalb der Perimeter erheblicher und kritischer verwendet werden.

b) Eine Liste von Arten von IKT-Produkten, IKT-Dienstleistungen und IKT-Prozessen, für die unverbindliche Empfehlungen zur Cybersicherheit entwickelt werden, basierend auf den jeweiligen regionalen Berichten zur Bewertung von Cybersicherheitsrisiken und den Prioritäten von Organisationen mit erhebéicher und kritischer Auswirkung.

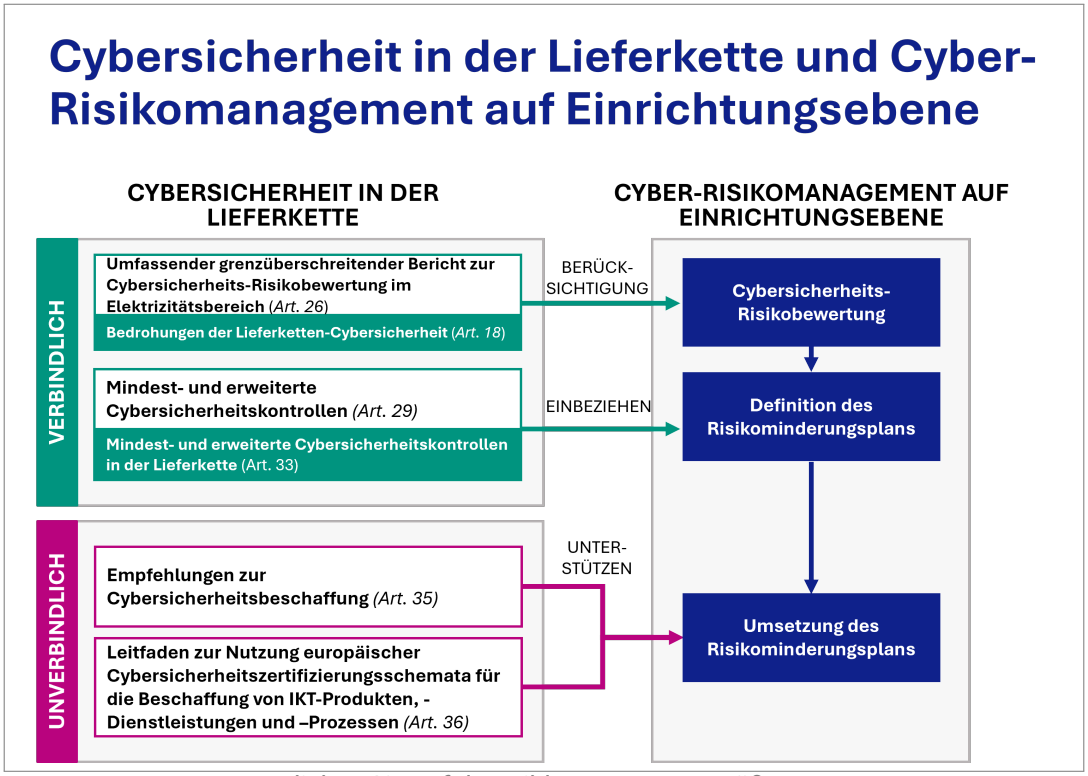
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[20] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_36
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_35

9.6 Risikomanagement in der Lieferkette

Während der Phase des Cybersicherheits-Risikomanagements muss jede erheblicher und kritischer Auswirkung Organisation einen organisationsweiten Risikominderungsplan für alle Vermögenswerte innerhalb ihres Perimeters mit erheblichen und kritischen Auswirkungen erstellen und alle drei Jahre eine Risikobewertung durchführen (NCCS Artikel 26 [22]).

Während der Phase der Bewertung der Cybersicherheitsrisiken müssen alle Organisationen mit erheblicher und kritischer Auswirkung potenzielle Cybersicherheitsrisiken identifizieren, darunter:

- Cyber-Bedrohungen, die im jüngsten umfassenden Bericht zur Bewertung der Cybersicherheitsrisiken für den grenzüberschreitenden Stromsektor (NCCS Artikel 23 [23]) identifiziert wurden.
- Potenzielle Bedrohungen für die Lieferkette (NCCS Artikel 18 [24]).



Klicken Sie auf das Bild, um es zu vergrößern.

[22] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[23] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_23
[24] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_18

Chapter 10

Cybersicherheits-Informationsmanagement

Dieses Kapitel beschreibt, wie die NCCS-Vorschriften die Verwaltung der Begriffe Cyberangriff, Schwachstellen und Bedrohungen regeln.

Gleichzeitige Cyberangriffe können möglicherweise zu einer Stromversorgungskrise führen und damit den grenzüberschreitenden Stromfluss beeinträchtigen. Ein solches Sicherheitsereignis könnte auch andere Sektoren beeinträchtigen, die von der Sicherheit der Stromversorgung abhängig sind.

10.1 Cyberabwehrkapazitäten von Organisationen mit erheblicher bzw. kritischer Auswirkung“

> NOTE
>
> Die Untertitel des Videos wurden mit KI-Tools erstellt, daher können Fehler enthalten sein.

Die NCCS-Verordnung enthält detaillierte Vorschriften für die Reaktion auf Cyberangriffe im Elektrizitätssektor.

- Einrichtung von **CSOC**-Fähigkeiten und Benennung eines **Ansprechpartner auf Organisationsebene** (NCCS Artikel 28 Absatz 1 [1])
- Entwicklung von Fähigkeiten zum Umgang mit erkannten Cyberangriffen mit Unterstützung von CSIRTs (NCCS Artikel 39 Absatz 1 [2])
- Effektive Prozesse implementieren, um **Cyberangriffe, die grenzüberschreitende Stromflüsse beeinträchtigen könnten, zu identifizieren, zu klassifizieren und darauf zu reagieren** (NCCS Artikel 39 Absatz 1 [3])
- **Zusammenarbeit zwischen betroffenen Organisationen mit erheblicher und kritischer Auswirkung**, um Informationen über Cyberangriffe mit Auswirkungen auf grenzüberschreitende Stromflüsse auszutauschen (NCCS Artikel 39 Absatz 2 [4])
- Bezeichnen einen **Ansprechpartner auf Organisationsebene (SPOC)** und sicherstellen, dass dieser bei Bedarf Zugang zu den Informationen über Cyberangriffe hat, die er vom NCCS-NCA erhält (NCCS Artikel 39 Absatz 3 [5])
- Einrichtung von **Verfahren zum Umgang mit Cyberangriffen** (NCCS Artikel 39 Absatz 3 [6])
- **Testen der gesamten Verfahren zum Umgang mit Cyberangriffen** mindestens einmal jährlich (NCCS Artikel 39 Absatz 3 [7])
- Fähigkeiten zur Teilnahme an der Erkennung und Minderung grenzüberschreitender Risiken (NCCS Artikel 40 Absatz 4 [8])
- **Untersuchung der Ursachen** der grenzüberschreitenden Stromkrise – bei Auswirkungen (NCCS Artikel 40 Absatz 4 [9])

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_28
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_40
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_40

- Entwicklung und Testen von Krisenmanagementplänen und **Geschäftskontinuitätsplänen** (NCCS Artikel 41 [10])
- Bis zum 31. Dezember des Jahres nach der Benennung der Organisationen mit **kritischer Auswirkung und danach alle drei Jahre führt jede Organisation mit kritischer Auswirkung eine Cybersicherheitsübung durch** (NCCS Artikel 43 [11])

GOOD TO KNOW

Organisationen müssen die CSOC-Fähigkeit (auch in einem Anbieter von verwalteten Sicherheitsdiensten) einrichten, einen Ansprechpartner auf Organisationsebene benennen, Verfahren zum Umgang mit Cyberangriffen entwickeln, die mindestens einmal jährlich getestet werden müssen, und sicherstellen, dass Organisationen mit kritischer Auswirkung mindestens alle drei Jahre an Cybersicherheitsübungen teilnehmen.

10.2 Meldung von Cyberangriffen

Der folgende Abschnitt beschreibt den Prozess der Meldung eines Cyberangriffs.

TERM

Cyberangriff

Ein Sicherheitsvorfall im Sinne von Artikel 3 Absatz 14 der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates [a] über die Sicherheit von Netzwerken und Informationssystemen.

Ein bösartiger Begriff aus dem Bereich der Informations- und Kommunikationstechnologie: Vorfall, bei dem ein Angreifer versucht, einen Vermögenswert zu zerstören, offenzulegen, zu verändern, zu deaktivieren, zu stehlen, sich unbefugten Zugriff darauf zu verschaffen oder ihn unbefugt zu nutzen.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554

[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_41
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_43

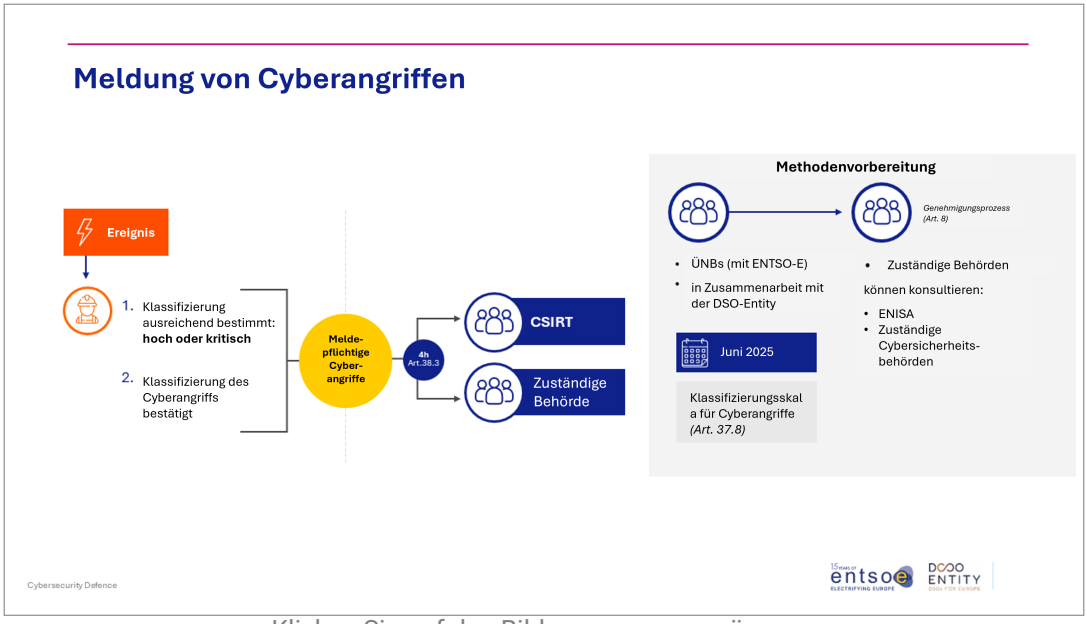
TERM

Der meldepflichtige Cyberangriff

Jede Organisation mit kritischer oder erheblicher Auswirkung muss unverzüglich, spätestens jedoch vier Stunden, nachdem sie Kenntnis von einem meldepflichtigen Cyberangriff erlangt hat, relevante Informationen über den meldepflichtigen Cyberangriff an ihre CSIRTs und zuständige Behörde weitergeben, gemäß (NCCS Artikel 38 Absatz 2 [a]).

Gemäß (NCCS Artikel 38 Absatz 3 [b]) gelten Informationen im Zusammenhang mit einem Cyberangriff als meldepflichtig, wenn die betroffene Organisation auf der Grundlage der Klassifizierungsskala (NCCS Artikel 37 Absatz 8 [c]) die Schwere des Angriffs als „erheblich" bis „kritisch" eingestuft wird. Die Einstufung von Sicherheitsvorfällen wird von der in Absatz 1(c) benannten zentralen Kontaktstelle der Organisation mitgeteilt.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[c] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37



Klicken Sie auf das Bild, um es zu vergrössern.

GOOD TO KNOW

Klassifizierung von Ereignissen

Die Übertragungsnetzbetreiber entwickeln mit Unterstützung des Strommarktes ENTSO-E und in Zusammenarbeit mit den EU-Verteilernetzbetreibern bis zum 13. Juni 2025 eine Methodik für die Klassifizierungsskala von Cyberangriffen (NCCS Artikel 37 [a])

Die Methodik kategorisiert die Schwere von Cyberangriffen in fünf Stufen, wobei die beiden höchsten Stufen „erheblich“ und „kritisch“ sind. Die Klassifizierung basiert auf der Bewertung der folgenden Parameter:

- die potenziellen Auswirkungen unter Berücksichtigung der exponierten Vermögenswerte und Bereiche, die gemäß Buchstabe c) NCCS Artikel 26 Absatz 4 [b] ermittelt wurden; und
- die Schwere eines Cyberangriffs

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37
[b] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

GOOD TO KNOW

Cyberangriffe, die von einer Organisation als bösartig eingestuft werden, erhebliche Auswirkungen auf den grenzüberschreitenden Stromfluss haben können und sich bereits in einem fortgeschrittenen Stadium der Angriffskette befinden (Einstufung „erheblich“ oder „kritisch“), müssen innerhalb von vier Stunden dem CSIRT und der zuständigen Behörde gemeldet werden.

10.2.1 Meldung eines Cyberangriffs

Wenn eine zuständige Behörde Informationen über einen meldepflichtigen Cyberangriff erhält, muss diese zuständige Behörde (NCCS Artikel 37 Absatz 1 [12]):

(a) den Grad der Vertraulichkeit dieser Informationen bewerten und die Organisation unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Erhalt der Informationen, über das Ergebnis ihrer Bewertung informieren;

(b) versuchen, andere ähnliche Cyberangriffe in der Union zu finden, die anderen zuständigen Behörden gemeldet wurden, um die im Zusammenhang mit dem meldepflichtigen Cyberangriff erhaltenen Informationen mit den im Zusammenhang mit anderen Cyberangriffen bereitgestellten Informationen zu korrelieren und die vorhandenen Informationen zu ergänzen, die Reaktionen auf Cybersicherheit zu verstärken und zu koordinieren;

(c) ist für die Entfernung von Geschäftsgeheimnissen und die Anonymisierung der Informationen gemäß den einschlägigen nationalen und Unionsvorschriften verantwortlich;

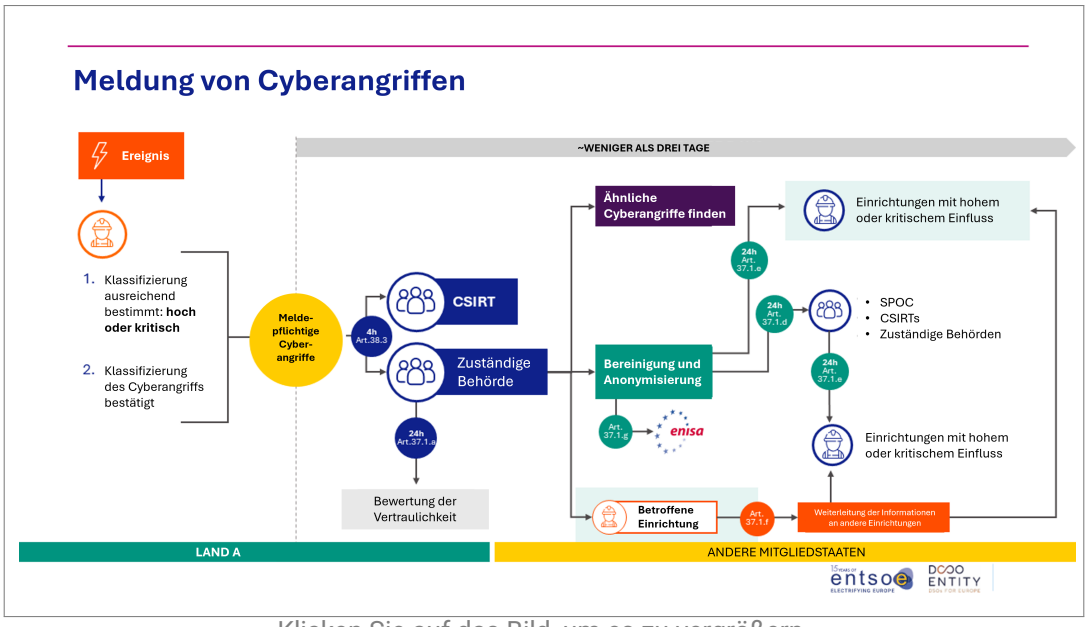
[12] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37

(d) die Informationen unverzüglich, spätestens jedoch 24 Stunden nach Erhalt einer meldepflichtigen Cyberattacke, an die nationalen zentralen Kontaktstellen, CSIRTs und alle gemäß Artikel 4 benannten zuständigen Behörden in anderen Mitgliedstaaten weiterleiten und diesen Behörden oder Stellen regelmäßig aktualisierte Informationen zur Verfügung stellen;

(e) die Informationen über den Cyberangriff nach Anonymisierung und Entfernung von Geschäftsgeheimnissen gemäß Absatz 1 Buchstabe c unverzüglich und spätestens 24 Stunden nach Erhalt der Informationen gemäß Absatz 1 Buchstabe a an die von kritischer und erheblicher Ausnwirkung betroffenen Organisationin seinem Mitgliedstaat weitergeben und regelmäßig aktualisierte Informationen bereitstellen, damit die Organisationen ihre Abwehrmaßnahmen wirksam organisieren können;

(f) kann die meldende Organisation mit erheblicher oder kritischer Auswirkung auffordern, die meldepflichtigen Informationen über Cyberangriffe auf sichere Weise an andere möglicherweise betroffene Organisationen weiterzugeben, um ein Situationsbewusstsein im Elektrizitätssektor zu schaffen und die Verwirklichung eines Risikos zu verhindern, das zu einem grenzüberschreitenden Cybersicherheitsvorfall im Elektrizitätsbereich eskalieren könnte;

(g) ENISA nach Anonymisierung und Entfernung von Geschäftsgeheimnissen einen zusammenfassenden Bericht mit den Informationen über den Cyberangriff übermitteln.



Klicken Sie auf das Bild, um es zu vergrößern.

10.3 Meldung von nicht gepatchten, aktiv ausgenutzten Sicherheitslücken

TERM

Nicht gepatchte, aktiv ausgenutzte Sicherheitslücke

Eine Sicherheitslücke im Sinne von Artikel 6 Nummer 15 der Richtlinie RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a] ist eine Sicherheitslücke, die noch nicht öffentlich bekannt gegeben und behoben wurde und für die es zuverlässige Hinweise darauf gibt, dass ein Akteur ohne Genehmigung des Systembesitzers bösartigen Code auf einem System ausgeführt hat.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

Nicht gepatchte, aktiv ausgenutzte Sicherheitslücken müssen dem CSIRT gemeldet werden, das Unterstützung leistet. Gemäß NCCS Artikel 38 Absatz 4 [13] kann der CSIRT, wenn Organisationen mit kritischer und erheblicher Auswirkung relevante Informationen über nicht behobene Sicherheitslücken, die aktiv ausgenutzt wurden, an den CSIRT melden, diese Informationen an die zuständige Behörde weiterleiten. Angesichts der Sensibilität der gemeldeten Informationen kann der CSIRT die Übermittlung der Informationen aus legitimen Gründen der Cybersicherheit zurückhalten oder verzögern. Nicht gepatchte, aktiv ausgenutzte Sicherheitslücken sollten an die CSIRT gemeldet werden, die Unterstützung leisten wird.

Wenn eine ungepatchte, aktiv ausgenutzte Sicherheitslücke gemäß NCCS Artikel 37 Absatz 2 [14] gemeldet wird, dann:

(a) es unverzüglich über einen geeigneten sicheren Informationsaustauschkanal an ENISA weiterleiten, sofern in anderen Rechtsvorschriften der Union nichts anderes bestimmt ist;

(b) die betroffene Organisation wird dabei unterstützt, vom Hersteller oder Anbieter ein wirksames, koordiniertes und zügiges Management der ungepatchten, aktiv ausgenutzten Sicherheitslücke oder wirksame und effiziente Abhilfemaßnahmen zu erhalten;

(c) die verfügbaren Informationen an den Anbieter weitergeben und den Hersteller oder Anbieter, soweit möglich, auffordern, eine Liste der CSIRTs in den Mitgliedstaaten zu erstellen, die von der nicht gepatchten, aktiv ausgenutzten Sicherheitslücke betroffen sind und die informiert werden müssen;

(d) die verfügbaren Informationen mit den unter dem vorherigen Punkt genannten CSIRTs (Computer Security Incident Response Teams) auf der Grundlage des Need-to-know-Prinzips teilen;

(e) sofern vorhanden, Strategien und Maßnahmen zur Minderung der gemeldeten, nicht gepatchten und aktiv ausgenutzten Sicherheitslücke angeben.

Wenn die zuständige Behörde gemäß NCCS Artikel 37 Absatz 3 [15] von einer ungepachten, aktiv ausgenutzten Sicherheitslücke Kenntnis erlangt, dann:

[13] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37

(a) die vorhandenen Strategien und Maßnahmen zur Minderung der gemeldeten, nicht gepatchten und aktiv ausgenutzten Sicherheitslücke in Abstimmung mit den CSIRTs in seinem Mitgliedstaat teilen;

(b) soll die Informationen mit einem CSIRT in dem Mitgliedstaat, in dem die nicht gepatchte, aktiv ausgenutzte Sicherheitslücke gemeldet wurde, teilen.

GOOD TO KNOW

Nicht gepatchte, aktiv ausgenutzte Sicherheitslücken müssen dem CSIRT gemeldet werden, das Unterstützung bietet.

10.4 Meldung von Cyber-Bedrohungen

TERM

Cyber-Bedrohung

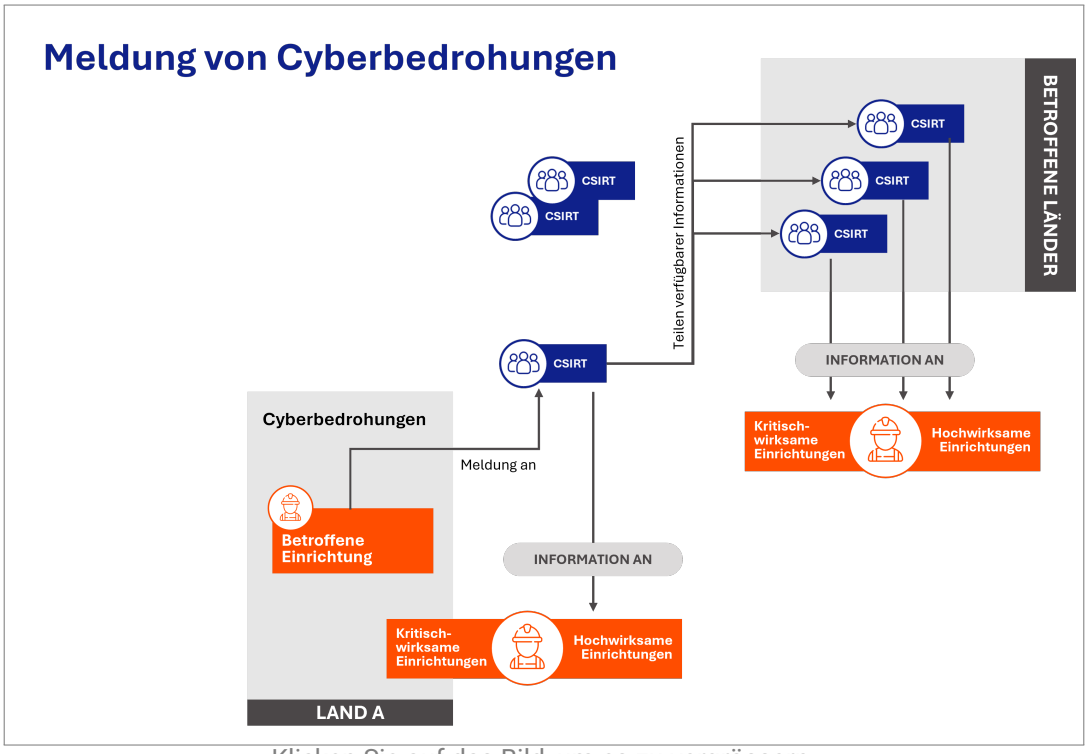
„Cyberbedrohung“ gemäß der Definition in Artikel 2 Nummer 8 der Verordnung VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [a]

Bedrohung bezeichnet jeden potenziellen Umstand, jedes Ereignis oder jede Handlung, die Netzwerke und Informationssysteme, die Nutzer solcher Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881

Bei der Meldung grenzüberschreitender Cyber-Bedrohungen gelten strengere zeitliche Vorgaben:

Die Informationen müssen unverzüglich gemeldet werden. Das nationale CSIRT ist für den Empfang und die Weitergabe dieser Informationen zuständig.



Klicken Sie auf das Bild, um es zu vergrössern.

GOOD TO KNOW

Organisationen müssen Cyber-Bedrohungen unverzüglich an die Stelle CSIRT melden, gemäß NCCS Artikel 37 Absatz 5 [a].

[a] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37

Chapter 11

Hauptaufgaben der Organisationen

Im Folgenden werden die Hauptaufgaben der wichtigsten Interessengruppe beschrieben:

11.1 Organisationen mit erheblicher und kritischer Auswirkung

Organisationen mit erheblicher und kritischer Auswirkung

Im letzten Kapitel fassen wir die wichtigsten Aufgaben von Organisationen mit erheblicher und kritischer Auswirkung zusammen:

- Ernennt eine zentrale Anlaufstelle (SPOC) (NCCS Artikel 38 Absatz 1 [1])
- Alle drei Jahre wird für alle Vermögenswerte innerhalb der Bereiche mit erheblicher und kritischer Auswirkung ein **Cybersicherheitsrisikomanagement auf Organisationsebene** durchgeführt (NCCS Artikel 26 [2], NCCS Artikel 27 [3])
- Führt ein Verzeichnis der Vermögenswerte im **Vermögensverzeichnis**. Das Vermögensverzeichnis ist nicht Teil des Risikobewertungsberichts (NCCS Artikel 26 [4]).

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_26

- Legt alle drei Jahre der zuständigen Behörde einen **Bericht** vor, der folgende Informationen enthält (NCCS Artikel 27 [5]):

  1. Liste der Kontrollen zusammen mit dem aktuellen Umsetzungsstatus jeder Kontrolle
  2. Abschätzung der Risiken in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und relevanten Vermögenswerten für alle Prozesse auf Unionsebene, Prozesse mit erheblicher Auswirkung oder Prozesse mit kritischer Auswirkung
  3. Liste kritischer IKT-Dienstleister auf Grundlage ihrer Prozesse mit kritischer Auswirkung

- Einrichtung eines **Cybersicherheits-Managementsystems** (NCCS Artikel 32 [6])
- **Nachweis** der Einhaltung des Cybersicherheits-Managementsystems und der **Mindest- oder erweiterten Cybersicherheitskontrollen (nur Organisation mit kritischer Auswirkung)** (NCCS Artikel 25 [7])
- **Anwendung von Mindest- und erweiterten Kontrollen in der Lieferkette** (Artikel 33 [8])
- Schafft **CSOC-Fähigkeiten** (NCCS Artikel 38 [9])
- **Meldet Informationen** im Zusammenhang mit Cyberangriffen / Cyberbedrohungen / ungepatchten, aktiv ausgenutzten Sicherheitslücken (NCCS Artikel 38 [10])

Thema	Frist	Meldepflichtige Organisationen
Cyberangriff	Innerhalb von 4 Stunden	CSIRT, zuständige Behörde
Nicht gepatchte, aktiv ausgenutzte Sicherheitslücke	NIS 2	CSIRT
Cyberbedrohung	Unverzüglich	CSIRT

- Entwickelt und testet **Verfahren zum Umgang mit Cyberangriffen** (NCCS Artikel 39 [11]) und **Krisenmanagementpläne** mindestens alle drei Jahre (NCCS Artikel 41 [12]).
- Alle drei Jahre führt die einzige Organisation mit kritischer Auswirkung eine Übung zur Cybersicherheit durch (NCCS Artikel 43 [13]).

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_27
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_32
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_33
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_39
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_41
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_43

11.2 Zuständige nationale Behörde

- Eine nationale Regierungs- oder Regulierungsbehörde, die für die Durchführung der ihr im Rahmen des NCCS Artikel 4 [14] übertragenen Aufgaben **verantwortlich** ist.
- Von jedem Mitgliedstaat **sechs Monate** nach Inkrafttreten zu benennen (NCCS Artikel 4 Absatz 1 [15]).
- **Koordiniert und kooperiert** mit den für Cybersicherheit zuständigen Behörden, NRAs, RP NCAs, CSIRTs und anderen von den einzelnen Mitgliedstaaten bestimmten Behörden, um die Erfüllung der NCCS sicherzustellen und Doppelarbeit zu vermeiden (NCCS Artikel 5 [16]).
- **Kann Aufgaben delegieren** an andere nationale Behörden (NCCS Artikel 4 Absatz 3 [17]).
- **Identifizierung von Organisationen mit erheblicher und kritischer Auswirkung** (NCCS Artikel 24 Absatz 2 [18]).
- **Genehmigung der entwickelten Bedingungen und Methoden** (NCCS Artikel 6 Absatz 2 [19]).
- **Durchführung von Cybersicherheits-Risikobewertungen** (NCCS Artikel 20 Absatz 1 [20]).
- **Gewährung von Ausnahmen von Mindest- und fortgeschrittenen Cybersicherheitskontrollen** (NCCS Artikel 30 Absatz 1 [21]).
- **Kann gemäß nationalem Recht Inspektionen** von Organisationen mit kritischer Auswirkung durchführen, um die Einhaltung der NCCS (NCCS Artikel 25 [22]) zu überprüfen.

11.3 Nationale Regulierungsbehörde

- **Umsetzung der NCCS-Verordnung** gemäß RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES Artikel 59 Absatz 1 Buchstabe e) Punkt [23].
- **Bewertung der Kosten**, die von Übertragungsnetzbetreibern (ÜNB) und Verteilernetzbetreibern (VNB) gemäß der Richtlinie RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES Artikel 11 [24] getragen werden.
- **Durchführung einer Bewertungsanalyse** innerhalb von 12 Monaten nach der Entwicklung der Leistungsbewertungsrichtlinien, wie in der Richtlinie 2019/944 des Europäischen Parlaments und des Rates RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES Artikel 13 Absatz 2 [25] vorgeschrieben.

[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_5
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_4
[18] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_24
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_6
[20] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_20
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_30
[22] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_25
[23] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944#art_59
[24] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944#art_11
[25] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0944#art_13

Chapter 12

Quiz

QUESTION 1

Welche Organisation ist für die Erstellung des unionsweiten Risikobewertungsberichts im Rahmen des NCCS zuständig?

Mark the correct answer.

level: normal

A ENISA

B ACER

C ENTSO-E

D EU DSO

QUESTION 2

Welche der folgenden Aussagen ist charakteristisch für die NCCS-Verordnung?

Mark the correct answer.

level: easy

A Es gilt nur für IT-Systeme.

B Es umfasst die Sicherheit sowohl von OT- als auch von IT-Systemen.

C Es ist für die Mitgliedstaaten nicht rechtsverbindlich.

D Es gilt nur für Stromerzeugungsunternehmen.

QUESTION 3

Ordnen Sie die folgenden Begriffe oder Organisationen den entsprechenden Definitionen zu

Match the letters with the numbers.

level: easy

1

ENTSO-E

2

ACER

3

NIS-2

A

European Cybersecurity Directive for the protection of information systems

B

Agency for the Cooperation of Energy Regulators

C

European Network of Transmission System Operators for Electricity

QUESTION 4

Ordnen Sie die Organisationen ihren Rollen zu

Match the letters with the numbers.

level: normal

1

ENTSO-E

2

ACER

3

EU DSO

4

ENISA

A

Erstellung eines unionsweiten Berichts zur Bewertung der Cybersicherheitsrisiken

B

Abgabe von Stellungnahmen zu Methodiken

C

Unterstützung von Verteilernetzbetreibern

D

Regelmäßige unionsweite Cybersicherheitsübung

QUESTION 5

Ordnen Sie die folgenden Übergangsbestimmungen zum NCCS in chronologischer Reihenfolge an

Write the numbers in the blanks.

level: normal

- Entwicklung von Kontrollen, die durch einschlägige europäische und internationale Normen und nationale Vorschriften vorgeschrieben sind
- Ausarbeitung einer vorläufigen ECII
- Erstellung einer vorläufigen Liste von Organisation mit erheblicher und kritischer Auswirkung

QUESTION 6

Ordnen Sie die Elemente des Cybersicherheits-Rahmenwerks den entsprechenden Kategorien zu

Write the numbers to the correct category on the dotted line.

level: normal

1. Entwicklung von Methoden zur Bewertung von Cybersicherheitsrisiken
2. Prozesse mit erheblicher Auswirkung auf Unionsebene und Prozesse mit kritischer Auswirkung auf Unionsebene
3. Rückverfolgbarkeit der Anwendung von Cybersicherheitsanforderungen von der Entwicklung über die Herstellung bis zur Lieferung von IKT-Produkten, IKT-Dienstleistungen oder IKT-Prozessen
4. ECII, sowie Schwellenwerte für erhebliche und kritische Auswirkungen
5. Prozesse für die sichere und kontrollierte Konzeption, Entwicklung und Herstellung von IKT-Produkten, IKT-Dienstleistungen und IKT-Prozessen
6. Regionale Risikobewertungsberichte
7. Hintergrundüberprüfungen von Mitarbeitern, die mit sensiblen Informationen umgehen oder Zugang zu den Vermögenswerten von erheblicher oder kritischer Auswirkung der Organisation haben

8. Bewertung des Risikoprofils von Lieferanten

Risikobewertung

. . . . . .

Sicherheit der Lieferkette

. . . . . .

QUESTION 7

Was ist das Hauptziel des NCCS-Risikobewertungsprozesses?

Mark the correct answer.

level: normal

A Risikobewertung im Zusammenhang mit der Einführung neuer IT-Systeme

B Entwicklung einer Risikowirkungsmatrix

C Identifizierung und Management von Risiken, die grenzüberschreitende Stromflüsse beeinträchtigen

D Sicherstellung der Einhaltung gesetzlicher Vorschriften

QUESTION 8

Welches Element ist nicht in der Risikowirkungsmatrix enthalten?

Mark the correct answer.

level: easy

A Konsequenzen

B Wahrscheinlichkeit

C Schwellenwerte

D Liste der Lieferanten

QUESTION 9

Wofür steht die Abkürzung ECII?

Mark the correct answer.

level: normal

A Electronic Component Integration Index

B Electricity Cybersecurity Impact Index

C European Cyber Defence Index

D Risk Tool Selection Index

QUESTION 10

Ordnen Sie die Risikobewertungsstufen ihren Aufgaben zu

Match the letters with the numbers.

level: normal

1

Unionsebene

2

Mitgliedstaatenebene

3

Regionale Ebene

A

Identifizierung von Organisationen mit erhebliher und kritischer Auswirkungm

B

Risikowirkungsmatrix

C

Erstellung regionaler Risikobewertungsberichte

QUESTION 11

Ordnen Sie die Cybersicherheitsbedrohungen den entsprechenden Prozessen zu

Match the letters with the numbers.

level: hard

1

Kaskadeneffekte von Cyberangriffen

2

Risiken veralteter Systeme

3

Bedrohungen für die Lieferkette

A

Aktualisierung von Cybersicherheitsstrategien

B

Analyse von Echtzeitsystemen

C

Bewertung des Risikoprofils von Lieferanten

QUESTION 12

Ordnen Sie die folgenden Begriffe ihren Definitionen zu

Match the letters with the numbers.

level: hard

1

Risikowirkungsmatrix

2

Cyberangriffsszenario

3

Risikominderungsplan

A

Ein Tool zur Analyse von Folgen und Wahrscheinlichkeiten

B

Modellierung möglicher Angriff

C

Ein Aktionsplan auf Organisationsebene zum Risikomanagement

QUESTION 13

Ordnen Sie die Stufen der NCCS-Risikobewertungsprozesse

Write the numbers in the blanks.

level: easy

- Unionsebene
- Regionale Ebene
- Nationale Ebene
- Organisationsebene

QUESTION 14

Ordnen Sie die folgenden Schritte anhand der Matrix zu den Auswirkungen auf die Cybersicherheit

Write the numbers in the blanks.

level: hard

- Bestimmung der Konsequenzen
- Kategorisierung der Risiken
- Analyse der Wahrscheinlichkeiten
- Anwendung von Schwellenwerten

QUESTION 15

Ordnen Sie die folgenden Cybersicherheitsstufen den entsprechenden Aufgaben zu

Write the numbers to the correct category on the dotted line.

level: normal

1. Erstellung regionaler Risikobewertungsberichte
2. Entwicklung einer Matrix zur Darstellung der Auswirkungen von Risiken
3. Nationale Risikobewertungsberichte
4. Prozesse mit erheblicher Auswirkung auf Unionsebene und Prozesse mit kritischer Auswirkung auf Unionsebene
5. Regionale Pläne zur Minderung von Cybersicherheitsrisiken
6. Identifizierung von Organisationen mit erheblicher Auswirkung

Unionsebene

. . . . . .

Regionale Ebene

. . . . . .

Nationale Ebene

. . . . . .

QUESTION 16

Welche Cyberangriffe müssen gemeldet werden?

Mark the correct answer.

level: normal

A Alle Cyberangriffe

B Alle böswilligen Cyberangriffe

C Alle böswilligen Cyberangriffe, die als „erheblich“ oder „kritisch“ eingestuft werden

QUESTION 17

Mark the correct answer.

level: normal

A Sie müssen unverzüglich der zuständigen Behörde gemeldet werden.

B Sie müssen innerhalb von 2 Stunden an das CSIRT gemeldet werden.

C Sie müssen innerhalb von 4 Stunden sowohl dem CSIRT als auch der zuständigen Behörde gemeldet werden.

QUESTION 18

Welche Aussage ist richtig?

Mark the correct answer.

level: normal

A Organisationen mit erheblicher und kritischer Auswirkung müssen CSOC-Fähigkeiten aufbauen (auch wenn diese ausgelagert werden).

B Nur Organisationen mit kritischer Auswirkung müssen CSOC-Fähigkeiten aufbauen (auch wenn diese ausgelagert werden).

C Organisationen mit erheblicher und kritischer Auswirkung müssen CSOC-Fähigkeiten aufbauen (diese können nicht ausgelagert werden).

QUESTION 19

Was bedeutet „hohe Wirkungsspanne“?

Mark the correct answer.

level: normal

A Von der Organisation festgelegte physische und/oder logische Abgrenzung (z. B. Zaun, Serverraum, Firewall, Proxy-Server usw.), die alle Vermögenswerte mit erheblicher Auswirkung und alle anderen Vermögenswerte innerhalb dieser Abgrenzung umfasst.

B Von der Organisation festgelegte physische und/oder logische Abgrenzung (z. B. Zaun, Serverraum, Firewall, Proxy-Server usw.), die alle Vermögenswerte mit kritischer und erheblicher Auswirkung und alle anderen Vermögenswerte innerhalb dieser Abgrenzung umfasst.

C Von der Organisation festgelegte physische Abgrenzung (z. B. Zaun, Serverraum, Firewall, Proxy-Server usw.), die alle Vermögenswerte mit erheblicher Auswirkung und alle anderen Vermögenswerte innerhalb dieser Abgrenzung umfasst.

Chapter 13

Entdecken Sie die nächste Stufe aktueller Cybersecurity-Readiness

Sie haben das vollständige NCCS-Material abgeschlossen.

Wir hoffen, dass Sie wertvolle und aufschlussreiche Informationen erhalten haben, die die Cybersicherheitsbemühungen Ihrer Organisation unterstützen.

Unlock AI-Driven Readiness Tiers

Als nächsten Schritt auf Ihrem Weg erhalten Sie einen kompakten Überblick darüber, wie die Readiness Tiers Ihre Organisation durch einen einzigartigen, KI-gestützten, nahezu in Echtzeit stattfindenden Wissenstransfer unterstützen können. Entdecken Sie unsere Readiness Tiers und abonnieren Sie sie, um sofortigen Zugang zu aktuellen Informationen darüber zu erhalten, wie Sie Risiken aus Schwachstellen mindern, verhindern und abwehren können.

Glossary

Agentur der Europäischen Union für Cybersicherheit (ENISA)

ENISA ist die Cybersicherheitsagentur der EU und unterstützt die Mitgliedstaaten bei der Abwehr von Cyberbedrohungen.

Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER)

Eine spezialisierte Agentur der Europäischen Union, die für die Förderung der Integration und des effizienten Funktionierens der EU-Energiemärkte zuständig ist.

https://www.acer.europa.eu/ [1]

VERORDNUNG (EU) 2019/942 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [2]

Akkreditierung

Bestätigung durch eine nationale Akkreditierungsstelle, dass eine Konformitätsbewertungsstelle die in harmonisierten Normen festgelegten Anforderungen und, gegebenenfalls, zusätzliche Anforderungen, einschließlich solcher in relevanten sektoralen Akkreditierungssystemen, erfüllt, um eine spezielle Konformitätsbewertungstätigkeit durchzuführen.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [3]

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 aus-

[1] https://www.acer.europa.eu/
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0942
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008R0765

geführt hat.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [4]

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [5]

Anbieter von verwalteten Diensten

Eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt. RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [6]

Anbieter von verwalteten Sicherheitsdiensten

Bezeichnet einen Anbieter verwalteter Dienste, der Tätigkeiten im Zusammenhang mit dem Management von Cybersicherheitsrisiken durchführt oder dabei unterstützt.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [7]

Ansprechpartner auf Organisationsebene (SPOC)

Bezeichnet den Ansprechpartner auf Organisationsebene, wie in Artikel 38 Absatz 1 Buchstabe c [8] benannt.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [9]

Assurance Level

[4] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L_202401366&qid=1737539416885#art_38
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

Bezeichnet eine Vertrauensgrundlage dafür, dass ein IKT-Produkt, ein IKT-Dienst oder ein IKT-Prozess die Sicherheitsanforderungen eines bestimmten europäischen Cybersicherheitszertifizierungsschemas erfüllt; gibt das Niveau an, auf dem das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess bewertet wurde, misst jedoch nicht die tatsächliche Sicherheit des Produkts, Dienstes oder Prozesses.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [10]

Behörden, die für das Management von Cyberkrisen zuständig sind

Bezeichnet Behörden, die gemäß Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2555 für das Management groß angelegter Cybersicherheitsvorfälle und -krisen (Cyberkrisenmanagement) benannt oder eingerichtet wurden. Die Mitgliedstaaten stellen sicher, dass diese Behörden über angemessene Ressourcen verfügen, um ihre Aufgaben wirksam und effizient wahrzunehmen, und dass Kohärenz mit bestehenden nationalen Krisenmanagementrahmen gewährleistet ist.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [11]

Beinahe-Vorfall

Ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist;

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [12]

Benannter Strommarktbetreiber (NEMO)

Ein Marktteilnehmer, der von der zuständigen Behörde eines Mitgliedstaats benannt wurde, um an der Kopplung des einheitlichen Day-Ahead-Markts oder des einheitlichen Intraday-Markts teilzunehmen.

CER-Richtlinie

Am 14. Dezember 2022 hat die Europäische Union die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen angenommen und die Richtlinie 2008/114/EG des Rates aufgehoben.

RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [13]

[10] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[11] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[12] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557

Computer-Notfallteams (CSIRT)

Eine Organisation, die für das Management von Sicherheitsvorfällen in Netz- und Informationssystemen zuständig ist. RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [14]

Cyber-Bedrohung

„Cyberbedrohung“ gemäß der Definition in Artikel 2 Nummer 8 der Verordnung VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [15]

Bedrohung bezeichnet jeden potenziellen Umstand, jedes Ereignis oder jede Handlung, die Netzwerke und Informationssysteme, die Nutzer solcher Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

Cyberangriff

Ein böswilliger IKT-bezogenen Vorfall, der auf den Versuch eines Angreifers zurückgeht, einen Vermögenswert zu zerstören, freizulegen, zu verändern, zu deaktivieren, zu entwenden oder auf unberechtigte Weise auf diesen Vermögenswert zuzugreifen oder ihn auf unberechtigte Weise zu nutzen.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [16]

Cyberangriff

Ein Sicherheitsvorfall im Sinne von Artikel 3 Absatz 14 der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates [17] über die Sicherheit von Netzwerken und Informationssystemen.

Ein bösartiger Begriff aus dem Bereich der Informations- und Kommunikationstechnologie: Vorfall, bei dem ein Angreifer versucht, einen Vermögenswert zu zerstören, offenzulegen, zu verändern, zu deaktivieren, zu stehlen, sich unbefugten Zugriff darauf zu verschaffen oder ihn unbefugt zu nutzen.

Cyberbedrohung

Bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

[14] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [18]

Cybersicherheit

Bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [19]

Cybersicherheit zuständigen Behörden (CS NCA)

Die nationale zuständige Behörde für Cybersicherheit in einem bestimmten Mitgliedstaat.

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [20]

Cybersicherheitsmaßnahme

Bezeichnet Maßnahmen oder Verfahren, die durchgeführt werden, um Cybersicherheitsrisiken zu vermeiden, zu erkennen, entgegenzuwirken oder zu minimieren.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [21]

Cybersicherheitsoperationszentrum, Betriebszentrum für Cybersicherheit (CSOC)

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.

[18] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[19] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[20] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[21] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [22]

Der meldepflichtige Cyberangriff

Jede Organisation mit kritischer oder erheblicher Auswirkung muss unverzüglich, spätestens jedoch vier Stunden, nachdem sie Kenntnis von einem meldepflichtigen Cyberangriff erlangt hat, relevante Informationen über den meldepflichtigen Cyberangriff an ihre CSIRTs und zuständige Behörde weitergeben, gemäß (NCCS Artikel 38 Absatz 2 [23]).

Gemäß (NCCS Artikel 38 Absatz 3 [24]) gelten Informationen im Zusammenhang mit einem Cyberangriff als meldepflichtig, wenn die betroffene Organisation auf der Grundlage der Klassifizierungsskala (NCCS Artikel 37 Absatz 8 [25]) die Schwere des Angriffs als „erheblich" bis „kritisch" eingestuft wird. Die Einstufung von Sicherheitsvorfällen wird von der in Absatz 1(c) benannten zentralen Kontaktstelle der Organisation mitgeteilt.

DG CONNECT (Generaldirektion Kommunikationsnetze, Inhalte und Technologien der Europäischen Kommission)

Die Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CONNECT) entwickelt und implementiert die politischen Maßnahmen der Europäischen Kommission.

DG ENER (Generaldirektion Energie der Europäischen Kommission)

Die Generaldirektion Energie der Europäischen Kommission ist für die Energiepolitik der EU verantwortlich.

Einrichtung mit erheblichen Auswirkungen

Bezeichnet eine Einrichtung, die einen Prozess mit erheblichen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 [26] ermittelt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [27]

Einrichtung mit kritischen Auswirkungen

Bezeichnet eine Einrichtung, die einen Prozess mit kritischen Auswirkungen durchführt und von

[22] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[23] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[24] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_38
[25] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1730714105315#art_37
[26] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[27] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

den zuständigen Behörden gemäß Artikel 24 [28] bestimmt wird.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [29]

Elektrizitätskoordinierungsgruppe (EKG)

Ziel der Elektrizitätskoordinierungsgruppe ist es, Informationen über strompolitische Maßnahmen mit grenzüberschreitenden Auswirkungen auszutauschen und zu koordinieren und die Zusammenarbeit durch Wissens- und Erfahrungsaustausch zu erleichtern.

KOMMISSIONSENTSCHEIDUNG 2012/C 353/02 [30]

Erhebliche Cyberbedrohung

Eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [31]

Erheblicher Cybersicherheitsvorfall großen Ausmaßes

Bezeichnet einen Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [32]

EU-VNBO (EU DSO)

Europäische Organisation der Verteilnetzbetreiber

Die EU-VNBO wurde von der Europäischen Union gegründet, um die Koordinierung und Entwicklung der Stromverteilungsnetze zu fördern. Sie spielt eine zentrale Rolle bei der Integration der Energiemärkte, der Einbindung erneuerbarer Energiequellen und der Unterstützung der Energiewende.

Die Aktivitäten der EU-VNBO werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

[28] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_24
[29] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[30] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32012D1117(01)
[31] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[32] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

https://eudsoentity.eu/ [33]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [34]

Europäische Kommission (EK)

Die Europäische Kommission ist das Exekutivorgan der Europäischen Union und verantwortlich für die Umsetzung der EU-Rechtsvorschriften, die Entwicklung von Politiken und die Verwaltung des Haushalts.

Europäisches Cybersicherheitszertifizierungsschema

Bezeichnet ein umfassendes Regelwerk aus Vorschriften, technischen Anforderungen, Normen und Verfahren, das auf Unionsebene festgelegt wird und für die Zertifizierung oder Konformitätsbewertung bestimmter IKT-Produkte, IKT-Dienstleistungen oder IKT-Prozesse gilt.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [35]

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [36]

Grenzüberschreitender Stromfluss

Bezeichnet das physikalische Durchströmen einer Menge elektrischer Energie durch ein Übertragungsnetz eines Mitgliedstaats aufgrund der Auswirkungen der Tätigkeit von Erzeugern oder Kunden oder beiden außerhalb dieses Mitgliedstaats auf dessen Übertragungsnetz.

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [37]

IKT

Informations- und Kommunikationstechnologie.

[33] https://eudsoentity.eu/
[34] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[35] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[36] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[37] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02019R0943-20240716

IKT-Altsystem

Bezeichnet ein Produkt, das das Ende seines Lebenszyklus (Ende seiner Lebensdauer) erreicht hat, aus technologischen oder wirtschaftlichen Gründen nicht für Upgrades oder Fehlerbehebungen in Frage kommt oder nicht mehr von seinem Anbieter oder einem IKT-Drittdienstleister unterstützt wird, das allerdings weiterhin genutzt wird und die Funktionen des Finanzunternehmens unterstützt.

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [38]

IKT-Dienstleistung

Bezeichnet einen Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [39]

IKT-Produkt

Bezeichnet ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [40]

IKT-Prozess

Bezeichnet jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [41]

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. DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [42]

Initiator

[38] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554
[39] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[40] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[41] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[42] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

Bezeichnet eine Organisation, die ein Ereignis des Informationsaustauschs, der Informationsweitergabe oder der Informationsspeicherung einleitet.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [43]

Interessenträger

Bezeichnet jede Partei, die ein Interesse am Erfolg und an der kontinuierlichen Funktionsweise einer Organisation oder eines Prozesses hat, wie z. B. Mitarbeitende, Direktoren, Anteilseigner, Regulierungsbehörden, Verbände, Lieferanten und Kunden.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [44]

Konformitätsbewertung

Bezeichnet das Verfahren zur Bewertung, ob spezifische Anforderungen an ein Produkt, ein Verfahren, eine Dienstleistung, ein System, eine Person oder eine Stelle erfüllt sind.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [45]

Konformitätsbewertungsstelle

Eine Stelle, die Konformitätsbewertungstätigkeiten einschließlich Kalibrierungen, Prüfungen, Zertifizierungen und Inspektionen durchführt.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [46]

Kooperationsgruppe für Netz- und Informationssysteme (NIS CG)

Kooperationsgruppe für Cybersicherheit

Die Kooperationsgruppe für Netz- und Informationssicherheit (NIS CG) koordiniert die Cybersicherheitszusammenarbeit in der EU. Die Aufgaben der NIS-Kooperationsgruppe sind in Artikel 11 der NIS-Richtlinie festgelegt.

DURCHFÜHRUNGSBESCHLUSS (EU) 2017/179 DER KOMMISSION [47]

Mitgliedstaat

[43] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[44] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[45] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02008R0765-20210716
[46] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02008R0765-20210716
[47] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32017D0179

Bezeichnet ein Land, das Mitglied der Europäischen Union ist und das EU-Recht einhält.

Nationale Akkreditierungsstelle

Die einzige Stelle in einem Mitgliedstaat, die im Auftrag dieses Staates Akkreditierungen durchführt.

VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [48]

Nationale Regulierungsbehörden (NRB)

Eine offizielle staatliche oder unabhängige Organisation, die für die Regulierung, Überwachung und Kontrolle bestimmter Bereiche innerhalb eines Landes oder einer Region zuständig ist.

Nationale zentrale Anlaufstelle

Bezeichnet die von jedem Mitgliedstaat gemäß Artikel 8 Absatz 3 der RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [49] benannte oder eingerichtete Anlaufstelle.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [50]

Nationale zuständige Behörde (NCA)

Eine nationale zuständige Behörde ist eine offizielle Stelle oder Organisation, die durch Rechtsvorschriften befugt ist, einen bestimmten Sektor oder Bereich zu regeln, zu überwachen und zu kontrollieren. Diese Behörden stellen die Einhaltung nationaler und gegebenenfalls internationaler Gesetze und Standards sicher.

Netz- und Informationssystem

Bezeichnet:

Artikel 6 Nummer 1: . ein elektronisches Kommunikationsnetz gemäß Artikel 2 Nummer 1 der Richtlinie (EU) 2018/1972; . ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, von denen eines oder mehrere aufgrund eines Programms eine automatische Verarbeitung digitaler Daten durchführen; oder . digitale Daten, die von den unter den Buchstaben a und b genannten Elementen gespeichert, verarbeitet, abgerufen oder übertragen werden, zum Zweck ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Wartung;

[48] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02008R0765-20210716
[49] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[50] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [51]

Nicht gepatchte, aktiv ausgenutzte Sicherheitslücke

Eine Sicherheitslücke im Sinne von Artikel 6 Nummer 15 der Richtlinie RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [52] ist eine Sicherheitslücke, die noch nicht öffentlich bekannt gegeben und behoben wurde und für die es zuverlässige Hinweise darauf gibt, dass ein Akteur ohne Genehmigung des Systembesitzers bösartigen Code auf einem System ausgeführt hat.

Normen

Bezeichnet eine von einer anerkannten Normungsorganisation angenommene technische Spezifikation zur wiederholten oder kontinuierlichen Anwendung, deren Einhaltung nicht verbindlich ist. VERORDNUNG (EU) Nr. 1025/2012 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [53]

Organisation

Bezeichnet eine natürliche oder juristische Person, die nach dem nationalen Recht ihres Sitzstaates gegründet und als solche anerkannt ist und in eigenem Namen Rechte ausüben und Verpflichtungen eingehen kann.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [54]

OT (Operational Technology)

OT ist die Kombination aus Produktionsautomatisierung, Maschine-zu-Maschine-Kommunikation und Datenerfassung.

Perimeter mit erheblichen Auswirkungen

Bezeichnet einen von einer der in Artikel 2 Absatz 1 [55] 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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [56]

[51] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[52] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555
[53] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012R1025
[54] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[55] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_2
[56] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

Perimeter mit kritischer Auswirkung

Bezeichnet einen von einer in Artikel 2 Absatz 1 [57] genannten Stelle definierten Perimeter, der alle Anlagen mit kritischer Auswirkung umfasst, auf die der Zugang kontrolliert werden kann und der den Geltungsbereich definiert, in dem fortgeschrittene Cybersicherheitsmaßnahmen gelten.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [58]

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [59]

Prozess mit kritischer Auswirkungen

Bezeichnet einen Geschäftsprozess, der von einer Stelle durchgeführt wird, für den die Indizes zur Bewertung der Auswirkungen auf die Cybersicherheit im Elektrizitätsbereich über dem Schwellenwert für kritische Auswirkungen liegen.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [60]

Regionale Koordinierungszentren (RCC)

Regionale Koordinierungszentren (RCC) haben eine beratende Rolle bei der Entwicklung regionaler Cybersicherheitsrisikobewertungen und -minderungspläne und koordinieren die Zusammenarbeit der Mitgliedstaaten im Bereich der Cybersicherheit.

Eingerichtet gemäß Artikel 35 der Verordnung (EU) 2019/943.

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [61]

Risiko

Das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird.

[57] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366&qid=1737539416885#art_2
[58] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[59] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[60] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[61] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [62]

Risikoauswirkungsmatrix

Bezeichnet eine Matrix, die bei der Risikobewertung genutzt wird, um für jedes bewertete Risiko die mit ihm verbundenen Auswirkungen zu bestimmen.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [63]

Risikovorsorge zuständigen Behörden (RP-NCA)

Die RP-NCA ist für die Entwicklung und Umsetzung von Risikovorsorgeplänen zuständig.

Schwachstelle

Eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [64]

Schwachstellenmanagement im Bereich der Cybersicherheit

Im Bereich der Cybersicherheit“ bezeichnet die Praxis, Schwachstellen zu ermitteln und zu beheben.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [65]

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [66]

Schwellenwert für kritische Auswirkungen

[62] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[63] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[64] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[65] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[66] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [67]

Selbstbewertung der Konformität

Bezeichnet eine Maßnahme eines Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Bewertung, ob diese IKT- Produkte, -Dienste oder -Prozesse die Anforderungen, die in einem spezifischen europäischen Schema für die Cybersicherheitszertifizierung festgelegt sind, erfüllen.

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [68]

Sicherheit von Netz- und Informationssystemen

Die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [69]

Spezifikationen für die Auftragsvergabe

Bezeichnet die von Einrichtungen für die Beschaffung neuer oder aktualisierter IKT-Produkte, -Prozesse oder -Dienste festgelegten Spezifikationen.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [70]

Stromversorgungskrise

Eine bestehende oder drohende Situation, die durch eine im Sinne der Vorgaben der Mitgliedstaaten und der Beschreibung in ihren Risikovorsorgeplänen erhebliche Stromknappheit oder durch die Unmöglichkeit, Kunden mit Strom zu versorgen, gekennzeichnet ist. VERORDNUNG (EU) 2019/941 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [71]

Systembetreiber

[67] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366
[68] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
[69] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[70] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[71] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0941

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Übertragungs- oder Verteilernetzes verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [72]

Systembetriebsregion

Bezeichnet die Systembetriebsregionen gemäß Anhang I des ACER-Beschlusses 05-2022 über die Definition von Systembetriebsregionen, die gemäß Artikel 36 der Verordnung (EU) 2019/943 eingerichtet wurden.

Technische Spezifikation

Bezeichnet ein Dokument, das technische Anforderungen vorschreibt, die von einem Produkt, einem Prozess, einer Dienstleistung oder einem System erfüllt werden müssen, und das eine oder mehrere der folgenden Festlegungen enthält.

VERORDNUNG (EU) Nr. 1025/2012 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [73]

Übertragungsnetzbetreiber (ÜNB)

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung des Übertragungsnetzes in einem bestimmten Gebiet sowie dessen Verbindung mit anderen Netzen und die langfristige Fähigkeit zur Deckung eines angemessenen Bedarfs an Stromübertragung verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [74]

Unionsweiter Prozess mit hoher Auswirkung

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.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [75]

Unionsweiter Prozess mit kritischer Auswirkung

Bezeichnet jeden Prozess im Elektrizitätssektor, an dem mehrere Einrichtungen beteiligt sein

[72] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[73] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012R1025
[74] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[75] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366

können und bei dem die möglichen Auswirkungen eines Cyberangriffs bei der Durchführung der unionsweiten Bewertung des Cybersicherheitsrisikos für kritisch erachtet werden können.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [76]

Verband Europäischer Übertragungsnetzbetreiber (ENTSO-E)

Gemeinsame Organisation der europäischen Übertragungsnetzbetreiber. Sie spielt eine zentrale Rolle bei der Integration des europäischen Strommarktes und der Sicherstellung der Stabilität des Stromsystems.

Die Aktivitäten von ENTSO-E werden durch das EU-Paket „Saubere Energie“ und die Strommarktverordnung (Verordnung (EU) 2019/943) geregelt.

https://www.entsoe.eu/ [77]

VERORDNUNG (EU) 2019/943 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [78]

Vermögenswert mit erheblichen Auswirkungen

Bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit erheblichen Auswirkungen erforderlich ist. DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [79]

Vermögenswert mit kritischen Auswirkungen

Bezeichnet einen Vermögenswert, der für die Durchführung eines Prozesses mit kritischen Auswirkungen erforderlich ist. DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [80]

Vermögenswerte

Eine Software oder Hardware in den Netzwerk- und Informationssystemen, die das Finanzunternehmen nutzt.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [81]

Verteilnetzbetreiber (DSO)

[76] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[77] https://www.entsoe.eu/
[78] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0943
[79] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[80] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[81] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32024R1366

Eine natürliche oder juristische Person, die für den Betrieb, die Wartung und gegebenenfalls die Entwicklung eines Verteilernetzes in einem bestimmten Gebiet sowie für die langfristige Fähigkeit zur Deckung gerechtfertigter Stromverteilungsanforderungen verantwortlich ist.

RICHTLINIE (EU) 2019/944 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [82]

Vertreter

Eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines DNS-Diensteanbieters, einer Einrichtung, die Domänennamen-Registrierungsdienste erbringt, eines TLD-Namenregisters, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen, eines Anbieters verwalteter Dienste, eines Anbieters verwalteter Sicherheitsdienste oder eines Anbieters von einem Online-Marktplatz, von einer Online-Suchmaschine oder von einer Plattform für Dienste sozialer Netzwerke, der bzw. die nicht in der Union niedergelassen ist, zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT — statt an die Einrichtung — hinsichtlich der Pflichten dieser Einrichtung gemäß dieser Richtlinie wenden kann.

DELEGIERTE VERORDNUNG (EU) 2024/1366 DER KOMMISSION [83]

Vorfall

Bezeichnet ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übertragenen oder verarbeiteten Daten oder von über Netz- und Informationssysteme angebotenen oder zugänglichen Diensten beeinträchtigt.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [84]

Vorfallbehandlung

Bezeichnet alle Maßnahmen und Verfahren, die darauf abzielen, Vorfälle zu verhindern, zu erkennen, zu analysieren, einzudämmen oder auf sie zu reagieren und sich davon zu erholen.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES [85]

Zuordnungsmatrix

Erarbeitet gemäß Artikel 34 der DELEGIERTEN VERORDNUNG (EU) 2024/1366 DER KOMMISSION [86], zur Zuordnung der in den Buchstaben a und b genannten Kontrollen zu ausgewählten europäischen und internationalen Normen sowie nationalen gesetzlichen oder regulatorischen

[82] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0944
[83] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401366
[84] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[85] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[86] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401366#art_34

Rahmenwerken.

Resources

FILE 1

Vorläufige Liste von Prozessen mit hoher und kritischer Auswirkung auf Unionsebene

files/Provisional list of Union-wide high-impact and critical-impact processes.pdf

FILE 2

Unterstützendes Dokument zur vorläufigen Liste von Prozessen mit hoher und kritischer Auswirkung

files/Supporting document Provisional list of Union-wide high-impact and critical-impact processes.pdf

FILE 3

Vorläufiger Elektrizitäts-Cybersicherheits-Auswirkungsindex (ECII)

files/Provisional ECII.pdf

FILE 4

Unterstützendes Dokument zum vorläufigen Elektrizitäts-Cybersicherheits-Auswirkungsindex (ECII)

files/Supporting document provisional ECII.pdf

Solutions

Question 1:

A ENISA

B ACER

C ENTSO-E ✓

D EU DSO

Feedback if the answer is correct:

RichtigENTSO-E ist für die EU-weiten Risikobewertungsberichte zuständig.

Feedback if the answer is incorrect:

Falsch. Die richtige Antwort lautet ENTSO-E.

Question 2:

A Es gilt nur für IT-Systeme.

B Es umfasst die Sicherheit sowohl von OT- als auch von IT-Systemen. ✓

C Es ist für die Mitgliedstaaten nicht rechtsverbindlich.

D Es gilt nur für Stromerzeugungsunternehmen.

Feedback if the answer is correct:

Richtig Das NCCS gewährleistet den Schutz sowohl von OT- als auch von IT-Systemen im europäischen Elektrizitätssektor.

Feedback if the answer is incorrect:

Falsch. Die richtige Antwort lautet: Es umfasst die Sicherheit sowohl von OT- als auch von IT-Systemen.

Question 3:

The right matching:

Pair 1:

ENTSO-E

European Network of Transmission System Operators for Electricity

Pair 2:

ACER

Agency for the Cooperation of Energy Regulators

Pair 3:

NIS-2

European Cybersecurity Directive for the protection of information systems

Feedback if the answer is correct:

Großartig Die Begriffe wurden korrekt zugeordnet.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Beschreibungen der Begriffe und versuchen Sie es erneut.

Question 4:

The right matching:

Pair 1:

ENTSO-E

Erstellung eines unionsweiten Berichts zur Bewertung der Cybersicherheitsrisiken

Pair 2:

ACER

Abgabe von Stellungnahmen zu Methodiken

Pair 3:

EU DSO

Unterstützung von Verteilernetzbetreibern

Pair 4:

ENISA

Regelmäßige unionsweite Cybersicherheitsübung

Feedback if the answer is correct:

Gut gemacht Alle Organisationen wurden ihren Rollen korrekt zugeordnet.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Rollen der Organisationen und ordnen Sie sie erneut zu.

Question 5:

The right order:

1. Ausarbeitung einer vorläufigen ECII
2. Erstellung einer vorläufigen Liste von Organisation mit erheblicher und kritischer Auswirkung
3. Entwicklung von Kontrollen, die durch einschlägige europäische und internationale Normen und nationale Vorschriften vorgeschrieben sind

Feedback if the answer is correct:

Richtige Reihenfolge: Ausarbeitung der vorläufigen ECII, Liste der Organisationen, Entwicklung von Kontrollen

Feedback if the answer is incorrect:

Falsch. Die chronologische Reihenfolge lautet: Ausarbeitung der vorläufigen ECII, Liste der Organisationen, Entwicklung von Kontrollen.

Question 6:

The right grouping:

Risikobewertung

- Entwicklung von Methoden zur Bewertung von Cybersicherheitsrisiken
- Regionale Risikobewertungsberichte
- Prozesse mit erheblicher Auswirkung auf Unionsebene und Prozesse mit kritischer Auswirkung auf Unionsebene
- ECII, sowie Schwellenwerte für erhebliche und kritische Auswirkungen

Sicherheit der Lieferkette

- Bewertung des Risikoprofils von Lieferanten
- Prozesse für die sichere und kontrollierte Konzeption, Entwicklung und Herstellung von IKT-Produkten, IKT-Dienstleistungen und IKT-Prozessen
- Rückverfolgbarkeit der Anwendung von Cybersicherheitsanforderungen von der Entwicklung über die Herstellung bis zur Lieferung von IKT-Produkten, IKT-Dienstleistungen oder IKT-Prozessen
- Hintergrundüberprüfungen von Mitarbeitern, die mit sensiblen Informationen umgehen oder Zugang zu den Vermögenswerten von erheblicher oder kritischer Auswirkung der Organisation haben

Feedback if the answer is correct:

Richtig. Die Elemente des Cybersicherheits-Rahmenwerks wurden korrekt gruppiert.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Beschreibungen der Kategorien und versuchen Sie es erneut.

Question 7:

A Risikobewertung im Zusammenhang mit der Einführung neuer IT-Systeme

B Entwicklung einer Risikowirkungsmatrix

C Identifizierung und Management von Risiken, die grenzüberschreitende Stromflüsse beeinträchtigen ✓

D Sicherstellung der Einhaltung gesetzlicher Vorschriften

Feedback if the answer is correct:

RichtigDas Hauptziel des NCCS-Risikobewertungsprozesses ist die Identifizierung und das Management von Risiken, die grenzüberschreitende Energieflüsse beeinträchtigen.

Feedback if the answer is incorrect:

Falsch. Die richtige Antwort lautet: Identifizierung und Management von Risiken, die grenzüberschreitende Stromflüsse beeinträchtigen.

Question 8:

A Konsequenzen

B Wahrscheinlichkeit

C Schwellenwerte

D Liste der Lieferanten ✓

Feedback if the answer is correct:

RichtigDie Liste der Lieferanten ist nicht Teil der Risikowirkungsmatrix.

Feedback if the answer is incorrect:

Falsch. Die richtige Antwort lautet: Liste der Lieferanten.

Question 9:

A Electronic Component Integration Index

B Electricity Cybersecurity Impact Index ✓

C European Cyber Defence Index

D Risk Tool Selection Index

Feedback if the answer is correct:

RichtigECII steht für „Electricity Cybersecurity Impact Index“

Feedback if the answer is incorrect:

Falsch. Die richtige Antwort lautet: „Electricity Cybersecurity Impact Index“

Question 10:

The right matching:

Pair 1:

Unionsebene

Risikowirkungsmatrix

Pair 2:

Regionale Ebene

Erstellung regionaler Risikobewertungsberichte

Pair 3:

Mitgliedstaatenebene

Identifizierung von Organisationen mit erhebliher und kritischer Auswirkungm

Feedback if the answer is correct:

GroßartigJede Stufe wurde korrekt der entsprechenden Aufgabe zugeordnet.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Rollen der Stufen und versuchen Sie es erneut.

Question 11:

The right matching:

Pair 1:

Bedrohungen für die Lieferkette

Bewertung des Risikoprofils von Lieferanten

Pair 2:

Kaskadeneffekte von Cyberangriffen

Analyse von Echtzeitsystemen

Pair 3:

Risiken veralteter Systeme

Aktualisierung von Cybersicherheitsstrategien

Feedback if the answer is correct:

GroßartigDie Bedrohungen wurden korrekt den entsprechenden Prozessen zugeordnet.

Feedback if the answer is incorrect:

Falsch. Versuchen Sie erneut, die Bedrohungen und Prozesse zuzuordnen.

Question 12:

The right matching:

Pair 1:

Risikowirkungsmatrix

Ein Tool zur Analyse von Folgen und Wahrscheinlichkeiten

Pair 2:

Risikominderungsplan

Ein Aktionsplan auf Organisationsebene zum Risikomanagement

Pair 3:

Cyberangriffsszenario

Modellierung möglicher Angriff

Feedback if the answer is correct:

Gut gemacht Alle Begriffe wurden mit der richtigen Definition abgeglichen.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Definitionen der Begriffe und versuchen Sie es erneut.

Question 13:

The right order:

1. Unionsebene
2. Regionale Ebene
3. Nationale Ebene
4. Organisationsebene

Feedback if the answer is correct:

Richtige Reihenfolge: Unionsebene, regionale Ebene, nationale Ebene, Organisationsebene

Feedback if the answer is incorrect:

Falsch. Versuchen Sie es erneut mit der richtigen Reihenfolge der Ebenen.

Question 14:

The right order:

1. Bestimmung der Konsequenzen
2. Analyse der Wahrscheinlichkeiten
3. Anwendung von Schwellenwerten
4. Kategorisierung der Risiken

Feedback if the answer is correct:

Richtige Reihenfolge: Konsequenzen, Wahrscheinlichkeiten, Schwellenwerte, Kategorisierung.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Reihenfolge der Schritte und versuchen Sie es erneut.

Question 15:

The right grouping:

Unionsebene

- Entwicklung einer Matrix zur Darstellung der Auswirkungen von Risiken
- Prozesse mit erheblicher Auswirkung auf Unionsebene und Prozesse mit kritischer Auswirkung auf Unionsebene

Regionale Ebene

- Erstellung regionaler Risikobewertungsberichte
- Regionale Pläne zur Minderung von Cybersicherheitsrisiken

Nationale Ebene

- Identifizierung von Organisationen mit erheblicher Auswirkung
- Nationale Risikobewertungsberichte

Feedback if the answer is correct:

Sehr gutJede Stufe wurde korrekt mit den entsprechenden Aufgaben gruppiert.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Stufen und ihre Aufgaben und versuchen Sie es erneut.

Question 16:

A Alle Cyberangriffe

B Alle böswilligen Cyberangriffe

C Alle böswilligen Cyberangriffe, die als „erheblich“ oder „kritisch“ eingestuft werden ✓

Feedback if the answer is correct:

Großartig Alle böswilligen Cyberangriffe, die als „erheblich“ oder „kritisch“ eingestuft werden, müssen gemeldet werden.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Antworten noch einmal.

Question 17:

A Sie müssen unverzüglich der zuständigen Behörde gemeldet werden.

B Sie müssen innerhalb von 2 Stunden an das CSIRT gemeldet werden.

C Sie müssen innerhalb von 4 Stunden sowohl dem CSIRT als auch der zuständigen Behörde gemeldet werden. ✓

Feedback if the answer is correct:

Großartig Sie müssen innerhalb von 4 Stunden sowohl dem CSIRT als auch der zuständigen Behörde gemeldet werden.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Antworten noch einmal.

Question 18:

A Organisationen mit erheblicher und kritischer Auswirkung müssen CSOC-Fähigkeiten aufbauen (auch wenn diese ausgelagert werden). ✓

B Nur Organisationen mit kritischer Auswirkung müssen CSOC-Fähigkeiten aufbauen (auch wenn diese ausgelagert werden).

C Organisationen mit erheblicher und kritischer Auswirkung müssen CSOC-Fähigkeiten aufbauen (diese können nicht ausgelagert werden).

Feedback if the answer is correct:

Gut Organisationen mit erheblicher und kritischer Auswirkung müssen CSOC-Fähigkeiten aufbauen (auch wenn diese ausgelagert werden).

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Antworten noch einmal.

Question 19:

A Von der Organisation festgelegte physische und/oder logische Abgrenzung (z. B. Zaun, Serverraum, Firewall, Proxy-Server usw.), die alle Vermögenswerte mit erheblicher Auswirkung und alle anderen Vermögenswerte innerhalb dieser Abgrenzung umfasst. ✓

B Von der Organisation festgelegte physische und/oder logische Abgrenzung (z. B. Zaun, Serverraum, Firewall, Proxy-Server usw.), die alle Vermögenswerte mit kritischer und erheblicher Auswirkung und alle anderen Vermögenswerte innerhalb dieser Abgrenzung umfasst.

C Von der Organisation festgelegte physische Abgrenzung (z. B. Zaun, Serverraum, Firewall, Proxy-Server usw.), die alle Vermögenswerte mit erheblicher Auswirkung und alle anderen Vermögenswerte innerhalb dieser Abgrenzung umfasst.

Feedback if the answer is correct:

GroßartigVon der Organisation festgelegte physische und/oder logische Abgrenzung (z. B. Zaun, Serverraum, Firewall, Proxy-Server usw.), die alle Vermögenswerte mit erheblicher Auswirkung und alle anderen Vermögenswerte innerhalb dieser Abgrenzung umfasst.

Feedback if the answer is incorrect:

Falsch. Überprüfen Sie die Antworten noch einmal.