Bedeutung der NIS-2-EU-Richtlinie für die Cybersicherheit

Key Facts

- Stärkung und Vereinheitlichung der Cybersicherheit EU-weit
- Neue Grenzwerte und Sektoren für Kritische Infrastrukturen
- Aktualisierung der nationalen Gesetzgebung

Autoren

↗ **Christian Rost**
↗ **Heinz-Werner Funke**

Im Januar 2023 ist die zweite EU-Richtlinie für Netzwerk- und Informationssicherheit (NIS 2) in Kraft getreten. Sie soll das Cybersicherheitsniveau innerhalb der EU vereinheitlichen und erhöhen. In Deutschland werden durch die NIS-2-Richtlinie nun auch kleine und mittlere Institutionen erfasst.

Zum Schutz Kritischer Infrastrukturen tragen sowohl die physische Sicherheit als auch die digitale oder auch Cybersicherheit bei. Beide Bereiche werden durch EU-Richtlinien reguliert, die am 16. Januar 2023 in Kraft getreten sind. Geregelt werden

1. die physische Sicherheit durch die EU-Richtlinie 2022/2557[1], auch „Directive on Critical Entities Resilience“ genannt oder kurz CER-Richtlinie, und
2. die Cybersicherheit durch die EU-Richtlinie 2022/2555[2], auch „The Network and Information Security Directive“ oder kurz NIS-2-Richtlinie genannt.

Sämtliche EU-Mitgliedstaaten müssen beide EU-Richtlinien innerhalb von 21 Monaten, also bis spätestens zum 17. Oktober 2024, in nationales Recht überführen. Die nationale Umsetzung der CER-Richtlinie für Deutschland erfolgt in Form des zukünftigen Kritische-Infrastrukturen-Dachgesetzes (KRITIS-Dachgesetz)[3]. Die nationale Umsetzung der im weiteren Verlauf betrachteten europäischen NIS-2-Richtlinie wird für Deutschland in Form des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) erfolgen. Bis zur abschließenden Umsetzung des NIS2UmsuCG in nationales Recht besteht keine vollumfängliche Rechtssicherheit, ein ausreichend konkreter Ausblick auf die zu erwartenden Veränderungen ist jedoch bereits jetzt möglich.

Zu den wesentlichen Veränderungen zählen beispielsweise die Anpassung der Sektoren und Grenzwerte (siehe Infokasten „Einheitliche Größen-Schwellenwerte nach NIS2UmsuCG“ und Infokasten „Sektoren aller Anwendungsbereiche nach NIS2-UmsuCG“), die Ausweitung der Pflichten, die Erhöhung der Sicherheitsanforderungen und der Sanktionen.

Auswirkung des NIS2UmsuCG

Der vorliegende Referentenentwurf des NIS2UmsuCG zeigt eine deutliche Orientierung an den Vorgaben der NIS-2-Richtlinie. Die nationale Umsetzung geht an einigen Punkten, wie vormals beim IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0), über die EU-Vorgaben hinaus.

Auch wenn sich das NIS2UmsuCG zurzeit in der Ressortabstimmung befindet, wird der „Geist“ des vorliegenden Entwurfs voraussichtlich beibehalten werden. Zeitgleiche Regelungen wie das KRITIS-Dachgesetz, die Nationale Sicherheitsstrategie und die China-Strategie des Bundes bekräftigen

Einheitliche Größen-Schwellenwerte nach NIS2UmsuCG

Unternehmensgröße	Beschäftigtenanzahl	Umsatz	Bilanz
Mittel (medium)	50 bis 250	und bis 50 Mio. EUR	oder bis 43 Mio. EUR
	1 bis 50	und 10 Mio. EUR bis 50 Mio. EUR	und 10 Mio. EUR bis 43 Mio. EUR
Groß (large)	Mindestens 250	oder mindestens 50 Mio. Euro	und mindestens 43 Mio. Euro

dies. Damit ergeben sich folgende exemplarisch hervorgehobene Veränderungen:

- mehrstufiges Meldeverfahren bei erheblichen Sicherheitsvorfällen (§ 31 NIS2UmsuCG)
- persönliche Haftung der Geschäftsleitung (§ 38 NIS2UmsuCG)
- Erhöhung der Sanktionen bei Verstößen (§ 60 NIS2UmsuCG)
- Einführung eines Chief Information Security Officers auf Bundesebene (CISO Bund)
- neuer Sektor: öffentliche Verwaltung
- Ausweitung der Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit Fokus auf besonders wichtige Einrichtungen

Die Bedeutung von NIS 2 für Unternehmen

Durch die NIS-2-Richtlinie und die erforderliche nationale Umsetzung in Form des NIS2UmsuCG werden das bestehende BSI-Gesetz (BSIG)[4] und die bestehende KRITIS-Verordnung (KRITISV)[5] merklich beeinflusst. Die Erweiterung der Sektoren und die Anpassung der Schwellenwerte (siehe Infokasten „Einheitliche Größen-Schwellenwerte nach NIS2UmsuCG“ und Infokasten „Sektoren aller Anwendungsbereiche nach NIS2UmsuCG“) werden zu einem signifikanten Anstieg der registrierungspflichtigen Institutionen führen: ersten Schätzungen folgend um das Sechsfache, also auf gut 30.000 Institutionen.

Das NIS2UmsuCG unterscheidet in Anlehnung an die „wesentlichen“ und „wichtigen“ Einrichtungen der NIS-2-Richtlinie zwischen „besonders wichtigen“ und „wichtigen“ Einrichtungen. Darüber hinaus können Einrichtungen, beispielsweise aufgrund ihres als bedeutend anzusehenden Versorgungsgrads, zusätzlich zu den „Betreibern kritischer Anlagen“ zählen. Es kann davon ausgegangen werden, dass bisherige Betreiber, die unter die KRITISV fallen, den „Betreibern kritischer Anlagen“ zugeordnet werden.

Der Unterschied bei den Zuordnungen besteht in der

- Abstufung zu erfüllender Pflichten und Anforderungen sowie der
- Beaufsichtigung und Sanktionierung durch zuständige Aufsichtsbehörden.

Die Zuordnung ergibt sich aus der Kombination der Institutionsgröße, dem infrage kommenden Sektor und verschiedenen Sonderfällen. Sie erfordert von jeder Institution eine eigenständige gründliche Prüfung.

Die Schwellenwerte zur Ermittlung der Institutionsgröße werden durch das NIS2-

Sektoren aller Anwendungsbereiche nach NIS2UmsuCG

- Energie
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Informationstechnik und Telekommunikation
- Verwaltung von IKT-Diensten
- öffentliche Verwaltung
- Weltraum
- Logistik
- Produktion
- Chemie
- verarbeitendes Gewerbe
- Forschung
- Ernährung
- Siedlungsabfallentsorgung
- Anbieter digitaler Dienste

Anlagen nach NIS2UmsuCG

Anlage	Kriterien
Wichtige Einrichtungen	• Mittlere Institution und Zugehörigkeit zu Sektoren mit hoher Kritikalität • Mittlere oder große Institution und Zugehörigkeit zu Sektoren mit normaler Kritikalität • Hersteller von Gütern mit IT-Sicherheitsfunktionen oder gemäß Teils B der Kriegswaffenliste • Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung • Vertrauensdiensteanbieter
Besonders wichtige Einrichtungen	• Große Institution und Zugehörigkeit zu Sektoren mit hoher Kritikalität • Mittlere Institution als Anbieter von Telekommunikationsdiensten oder -netzen • Betreiber kritischer Anlagen • Qualifizierter Vertrauensdiensteanbieter, TLD-Name Registries oder DNS-Diensteanbieter
Kritische Anlagen	• Bisherige Betreiber Kritischer Infrastrukturen • Institutionen mit Zugehörigkeit zu Sektoren mit hoher Kritikalität und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind.

Jedes Unternehmen muss die Betroffenheit eigenverantwortlich feststellen. Die Aufgliederung der Sektoren in die zugehörigen Branchen wird wie bereits dargestellt in der zukünftigen Rechtsverordnung behandelt, die sich vermutlich an der aktuell geltenden KRITISV orientieren wird.

UmsuCG vorgegeben und basieren auf der EU-Richtlinie 2003/361/EC[6] zur Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (siehe Infokasten „Einheitliche Größen-Schwellenwerte nach NIS2UmsuCG“).

Die Sektoren werden durch das NIS2-UmsuCG vorgegeben (siehe Infokasten „Sektoren aller Anwendungsbereiche nach NIS2UmsuCG“). Die Aufgliederung der Sektoren in die zugehörigen Branchen wird in einer noch nicht verfügbaren Rechtsverordnung behandelt. Diese wird sich vermutlich an der aktuell geltenden KRITISV orientieren, sodass bereits jetzt als Betreiber Kritischer Infrastruktur geltende Einrichtungen zukünftig als Betreiber kritischer Anlagen gelten.

Darüber hinaus bestehen Sonderfälle, durch die ausgewählte Institutionen und Branchen aufgrund ihrer Relevanz und unabhängig von ihrer Größe als besonders wichtige oder wichtige Institution eingestuft werden. In der Regel ist das dann der Fall, wenn diese Institutionen aufgrund ihrer Stellung oder Reichweite einen bedeutenden Einfluss auf die öffentliche Sicherheit oder Gesundheit haben oder sie derart systemrelevant sind, dass ihr Ausfall ein bedeutendes systemisches Risiko darstellt.

Verschärfung der Sanktionen

Mit der NIS-2-Richtlinie/dem NIS2UmsuCG werden Strafen und Sanktionen deutlich ausgeweitet und verschärft. Sie orientieren sich dabei an denen der EU-Datenschutz-Grundverordnung (EU-DSGVO)[7].

Für besonders wichtige Einrichtungen und kritische Anlagen liegen die Bußgelder bei bis zu zehn Millionen Euro oder mindestens zwei Prozent des Jahresumsatzes, je nachdem, welcher Betrag höher ist.

Für wichtige Einrichtungen liegen die Bußgelder bei bis zu sieben Millionen Euro oder mindestens 1,4 Prozent des Jahresumsatzes, je nachdem, welcher Betrag höher ist.

Zu erfüllende Pflichten

Betroffene Institutionen müssen die geforderten Pflichten der NIS-2-Richtlinie/des NIS2UmsuCG erfüllen. Diese können wie in Tabelle 1 dargestellt grob in zwei Bereiche unterteilt werden: die Pflichten gegenüber Aufsichtsbehörden und die Maßnahmen zum Erreichen des Stands der Technik.

Dabei stellt die Umsetzung von Maßnahmen zur Cybersecurity lediglich einen Oberbegriff dar, unter dem Maßnahmen zusammengefasst sind wie Cyberrisikomanagement, Sicherheit in der Lieferkette, Business Continuity Management (BCM), Penetrationstests oder die Reaktion auf Vorfälle.

Im Folgenden werden die Anforderungen, die in der Tabelle 1 aufgeführt sind, näher erläutert.

Identifizierung kritischer Dienstleistungen, Anlagen und Komponenten
Infrage kommende Institutionen sind für

Quelle: OpenKRITIS[8]

Pflichten	Aufgaben	Verantwortlich (A)	Durchführung (R)	Dritte (C/I)	Wann
Identifikation (1)	Analyse der KRITIS-Bereiche und eigene Betroffenheit	Geschäftsführung	Geschäftsführung (KRITIS-Org.)		jährlich
Registrierung (2)	Meldung der KRITIS-Bereiche Registrierung beim BSI	Geschäftsführung	Geschäftsführung (KRITIS-Org.)	BSI	nach (1)
Geltungsbereich (3)	KRITIS-Bereiche definieren Scope im Unternehmen	Geschäftsführung	KRITIS-Org.		nach (1) vor (6)
Meldungen (4)	Meldung Angriffe und Vorfälle an das BSI	Geschäftsführung	IT-Sicherheit	BSI	unverzüglich
Komponenten (5)	Kritische Komponenten identifizieren & melden an das BMI	Geschäftsführung	KRITIS-Org.	BSI	vor Einsatz
Cyber Security (6)	Maßnahmen umsetzen nach dem Stand der Technik	Geschäftsführung	Fachbereiche IT-Sicherheit		regelmäßig
Prüfungen (7)	Nachweis der Cyber Security in den KRITIS-Bereichen	Geschäftsführung	KRITIS-Prüfer	BSI	zweijährlich

Tabelle 1: Pflichten für Institutionen

> „Haben Institutionen ‚kritische' Bereiche identifiziert, müssen sie sich gemäß den gesetzlichen Melde- und Nachweispflichten selbst mit ihren kritischen Bereichen beim BSI registrieren."

die Identifizierung kritischer Dienstleistungen, Anlagen und Komponenten sowie für die Feststellung der Betroffenheit als „verpflichtete Institution" eigenverantwortlich. Die bisherigen Schwellenwerte wurden wie oben dargestellt mit der NIS-2-Richtlinie beziehungsweise dem NIS2UmsuCG grundlegend verändert und deutlich herabgesetzt.

Registrierung kritischer Dienstleistungen und Komponenten beim BSI
Haben Institutionen „kritische" Bereiche identifiziert, müssen sie sich gemäß den gesetzlichen Melde- und Nachweispflichten selbst als „verpflichtete Institution" mit ihren kritischen Bereichen beim BSI registrieren. Wichtige Einrichtungen und besonders wichtige Einrichtungen müssen dies innerhalb von drei Monaten nach Inkrafttreten einer entsprechenden Verordnung oder eines Gesetzes durchführen. Darüber hinaus gilt für Betreiber kritischer Anlagen, dass die von ihnen betriebenen kritischen Anlagen innerhalb eines Werktags nach eigener Identifikation beim BSI registriert werden müssen.

Es bietet sich an, die Registrierung bis zum Inkrafttreten des NIS2UmsuCG vorzubereiten, sodass diese innerhalb der gegebenen Fristen durchgeführt werden kann. Darüber hinaus kann das BSI eine Institution eigenständig ermitteln und registrieren, wenn die Institution ihre Pflicht zur Registrierung nicht erfüllt.

Kontaktstelle betreiben
Institutionen sind verpflichtet, eine Kontaktstelle für ihre kritischen Bereiche zu benennen, zu betreiben und dies gegenüber dem BSI nachzuweisen. Über die Kontaktstelle müssen Institutionen jederzeit erreichbar sein und ihrer Meldepflicht bei erheblichen IT-Störungen nachkommen.

Meldepflichten
Verpflichtete Institutionen müssen erhebliche Störungen in ihren kritischen Bereichen unverzüglich nach Erkennen der (IT-) Störung an das BSI melden. Meldepflichtige Störungen können Prozesse, Komponenten und IT-Systeme betreffen.

Gemäß dem NIS2UmsuCG gilt nun der Grundsatz: Schnelligkeit vor Vollständigkeit. Dazu wird der neue Meldeprozess in drei Stufen unterteilt – eine Erstmeldung innerhalb von 24 Stunden nach Kenntniserlangung, eine Bestätigung innerhalb von 72 Stunden, optionale Zwischenmeldungen und eine Abschlussmeldung innerhalb eines Monats nach der Bestätigung.

Informationssicherheitsmanagementsystem (ISMS)
Verpflichtete Institutionen müssen zum Management von Cyberrisiken für den kritischen Bereich ein ISMS etablieren, um Risiken zu mindern.

KRITIS-Management
Verpflichtete Institutionen sollten eine zentrale Organisation zur Koordinierung und Steuerung der zahlreichen Pflichten einrichten, die „KRITIS-Organisation". Die KRITIS-Organisation kann in Abstimmung mit dem ISMS den kritischen Geltungsbereich definieren, die kritischen Prozesse steuern und überwachen sowie die operative Umsetzung technischer und organisatorischer Maßnahmen (TOMs) begleiten und überwachen. Sie dient somit als Steuerungs- und Kontrollorgan zur Vorbereitung auf das erste Audit und für den späteren Linienbetrieb.

Welche Vorteile bieten NIS2UmsuCG/NIS 2?

Risiko von Cyberangriffen reduzieren
Mit der Umsetzung der NIS-2-Richtlinie/des NIS2UmsuCG wird das Risiko von Cyberangriffen reduziert, die Auswirkungen von Cyberangriffen werden eingedämmt.

Besseres Management von Sicherheitsvorfällen
Ein klares und durchdachtes Vorfallmanagement hilft Institutionen, Sicherheitsvorfälle unmittelbar zu erkennen, zu klassifizieren und einzudämmen. Somit werden negative Folgen wie Ausfallzeiten, verminderte Produktivität oder Reputationsschäden abgemildert.

Verbesserte Business Continuity
Erprobte Business-Continuity-Pläne helfen dabei, Kosten durch Ausfallzeiten zu minimieren und sicherzustellen, dass kritische Prozesse auch im Fall eines Sicherheitsvorfalls weiterlaufen oder zeitnah wieder zur Verfügung stehen.

Höhere Effizienz und Produktivität
Die Vorgaben der NIS-2-Richtlinie/des NIS2UmsuCG helfen Institutionen dabei, ihre Sicherheitsprozesse zu optimieren und den Aufwand für das Management der Informationssysteme zu reduzieren.

Risikomanagement
Verpflichtete Institutionen müssen im Rahmen eines übergreifenden Risikomanagements sämtliche Risiken für die kritischen Bereiche behandeln.

Institutionen können einen für sie geeigneten anerkannten Standard zum Aufbau und Betrieb eines Risikomanagements wählen. Infrage kommen beispielsweise die ISO 31000 oder spezifischere Standards wie die ISO 27005[9] oder der BSI-Standard 200-3[10].

Business Continuity Management und IT-Notfallmanagement
Verpflichtete Institutionen müssen im Rahmen eines Business Continuity Managements (BCM) Maßnahmen zur Gewähr-

> „Die erforderlichen Aufwände, die Kosten und den Umsetzungszeitraum muss jede Institution aufgrund der unterschiedlichen Gegebenheiten für sich ermitteln.“

leistung der Betriebskontinuität und des Fortbestands ergreifen und damit den Betrieb, die Prozesse und sonstige Komponenten innerhalb der kritischen Bereiche im Krisenfall schützen.

Institutionen können einen für sie geeigneten anerkannten Standard zum Aufbau und Betrieb eines BCM wählen. Infrage kommt beispielsweise der BSI-Standard 200-4[11].

Sicherheitsvorfall-Management
Institutionen sind verpflichtet, IT-Störungen oder erhebliche Beeinträchtigungen zu erkennen und nach Bekanntwerden unverzüglich dem BSI zu melden.

Die Erkennung und Meldung erheblicher IT-Störungen kann im Rahmen eines Sicherheitsvorfall-Managements strukturiert bearbeitet und dokumentiert werden.

Institutionen können einen für sie geeigneten anerkannten Standard zum Aufbau und Betrieb eines Sicherheitsvorfall-Managements wählen. Infrage kommt beispielsweise eine Kombination aus dem IT-Grundschutzbaustein DER[12] für den Rahmen und die NIST IR-8286D[13] zur konkreten Ausgestaltung.

Lieferanten-/Dienstleister-Management
Institutionen sind verpflichtet, Risiken in der Lieferkette (Supply-Chain) und im Einkauf zu bewerten, die einen direkten Einfluss auf die kritischen Bereiche haben. Damit diese Risiken bewertet werden können, ist ein Mindestmaß an Transparenz durch Dienstleister hinsichtlich der genauen Ausgestaltung ihrer Dienste und der implementierten Sicherheitsmaßnahmen erforderlich.

Institutionen können eine für sie geeignete Vorgehensweise zur Sicherung der Lieferkette wählen. Infrage kommen beispielsweise Empfehlungen des BSI[14], der ENISA[15] oder auch der OWASP[16].

Umsetzung des Stands der Technik
Institutionen müssen zum Erreichen eines angemessenen Sicherheitsniveaus der IT- und Anlagentechnik in ihren kritischen Bereichen Cybersecuritymaßnahmen nach dem Stand der Technik umsetzen.

Der Stand der Technik ist ein juristischer Begriff, der beispielsweise durch die Handreichung des Bundesverbandes IT-Sicherheit e. V. (TeleTrusT)[17] und durch branchenspezifische Sicherheitsstandards (B3S)[18] spezifiziert wird.

Exemplarisch hervorzuheben sind dabei Maßnahmen wie die Einführung eines Identity/Privilege and Access Managements (IAM/PAM), das Asset-Management, die Einführung einer Zwei-Faktor-Authentifizierung oder der weitgehende Einsatz von Verschlüsselungsverfahren zum Schutz ruhender und beweglicher Daten.

Systeme zur fortlaufenden Angriffserkennung
Verpflichtete Institutionen müssen Cyberangriffe in kritischen Bereichen erkennen. Das NIS2UmsuCG schreibt in der aktuellen Fassung Systeme zur fortlaufenden Angriffserkennung nur für Betreiber kritischer Anlagen vor.

Umzusetzende Maßnahmen werden durch die Orientierungshilfe für Systeme zur Angriffserkennung (OH SzA)[19] des BSI verbindlich vorgegeben.

Aufwände, Kosten, Umsetzungszeiträume

Die erforderlichen Aufwände, die Kosten und den Umsetzungszeitraum muss jede Institution aufgrund der unterschiedlichen Gegebenheiten für sich ermitteln. Selbst in derselben Branche kann der Unterschied zwischen Institutionen sehr groß sein.

Eine erste Orientierung zur Ermittlung der Kosten und Aufwände können die Empfehlungen des BSI[20] und der Europäischen Kommission[21] liefern. Das BSI liefert den Ausgangspunkt für ein anzusetzendes

Cybersicherheitsbudget, die Europäische Kommission die notwendige Erhöhung, damit die Anforderungen der NIS-2-Richtlinie erfüllt werden können.

- BSI: Das Budget für Cybersicherheit sollte bis zu 20 Prozent des IT-Budgets betragen.
- Europäische Kommission: Erstmalig erfasste Institutionen sollten das Budget für die Cybersicherheit um bis zu 22 Prozent erhöhen, bereits von der NIS-1-Richtlinie erfasste Institutionen um bis zu 12 Prozent.

Der Umsetzungszeitraum bezieht sich auf das Inkrafttreten des NIS2UmsuCG. Ab dem Zeitpunkt gelten sämtliche Pflichten unmittelbar und gestellte Anforderungen müssen erfüllt sein. Der Nachweis der Umsetzung muss zu dem vom BSI gesetzten Zeitpunkt erbracht werden.

Handlungsempfehlungen

Die NIS-2-Richtlinie muss bis zum 17. Oktober 2024 in nationales Recht überführt werden. Durch die NIS-2-Richtlinie werden sehr viele Institutionen erstmalig erfasst und müssen sich auf die neue Regulierung einstellen. Institutionen, die durch die NIS-1-Richtlinie[22] und das IT-SiG 2.0[23] bereits erfasst werden, müssen sich auf schärfere Kontrollen, Nachweispflichten sowie deutlich höhere Sanktionen einstellen.

Der vorliegende Referentenentwurf des NIS2UmsuCG zeigt zudem, dass die nationale Umsetzung an einigen Punkten wie schon beim Vorgänger über die EU-Vorgaben hinausgeht.

Bereits jetzt kann der eigene Reifegrad der Cybersecurity anhand eines Soll-Ist-Vergleichs gegenüber dem Stand der Technik und den zu erfüllenden Pflichten festgestellt werden. Dieses gilt für die gesetzlichen Unfallversicherungen ebenso wie für deren Mitgliedsunternehmen.

Zu empfehlen ist ein ganzheitlicher, bedarfsgerechter Ansatz. Hierzu kann die Basis-Absicherung des BSI-IT-Grundschutzes[24] als Einstieg genutzt werden mit dem Ziel, die Standard-Absicherung für die gesamte Institution zu erreichen. Die Kern-Absicherung kann ergänzend zur Basis-Absicherung für den Bereich der besonders wichtigen Geschäftsprozesse, Komponenten und IT-Systeme (kritischen Anlagen) verwendet werden.

Die Zeit zur Umsetzung erforderlicher technischer und organisatorischer Maßnahmen ist sehr knapp bemessen. Dabei sollten auch die Lieferketten und der Einkauf nicht vergessen werden. In diesen Bereichen werden kurzfristige Veränderungen, beispielsweise durch vertragliche Bindungen, nur eingeschränkt möglich sein.

Daher gilt für alle Unternehmen die Empfehlung, rechtzeitig zu klären, ob sie künftig durch das NIS2UmsuCG verpflichtet sein werden.

Fußnoten

[1] https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=de
[2] https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=de
[3] https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html (abgerufen am 02.08.2023)
[4] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html
[5] https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32003H0361
[7] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679
[8] https://www.openkritis.de/betreiber/index.html
[9] https://www.din.de/de
[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html
[11] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html
[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html
[13] https://csrc.nist.gov/News/2022/nist-releases-nistir-8286d
[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-entwicklung-einsatz-produkte.pdf
[15] https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
[16] https://cyclonedx.org/
[17] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/
[18] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Branchenspezifische-Sicherheitsstandards-B3S/branchenspezifische-sicherheitsstandards-b3s_node.html
[19] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=8
[20] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210415_HO-Umfrage.html
[21] https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union
[22] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinie/nis-richtlinie_node.html
[23] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html
[24] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_09/Lektion_2_09_node.html