Whitepaper

SKW Schwarz

August 2025

Whitepaper zur Umsetzung der NIS2-Richtlinie

Ein Leitfaden für Unternehmen, Geschäftsleiter und Rechtsabteilungen

Whitepaper zur Umsetzung der NIS2-Richtlinie

Ein Leitfaden für Unternehmen, Geschäftsleiter und Rechtsabteilungen

Inhalt

Die Zahl der **Cyberangriffe** auf Unternehmen in Deutschland steigt seit Jahren unaufhörlich an. Nach aktuellen Umfragen unter Unternehmensführern steht die Sorge davor, Opfer von Cyberattacken auf das eigene IT-System zu werden oder von Hacks auf die eingesetzten IT-Dienstleister betroffen zu sein, an oberster Stelle der befürchteten Risiken für den Bestand ihrer Unternehmen.[1] In den Fokus der Cyberkriminellen geraten dabei zunehmend auch weniger prominente und mittelständische Unternehmen. Den betroffenen Unternehmen können aus solchen Attacken empfindliche Umsatzverluste und Schäden im Umgang mit ihren Kunden entstehen. Neben dem individuellen Interesse der Unternehmer bedrohen die Cyberangriffe aber auch das öffentliche Interesse an einem funktionierenden Gemeinwesen, wenn wichtige Lieferketten oder die Produktion von Gütern gestört werden.

[1] Eine Umfrage aus dem Jahr 2023 ergab, dass rund 58 Prozent der befragten Unternehmen in Deutschland mindestens einmal Opfer einer Cyber-Attacke geworden waren. https://de.statista.com/statistik/daten/studie/1230157/umfrage/unternehmen-die-in-den-letzten-12-monaten-eine-cyber-attacke-erlebt-haben/#statisticContainer.

Der steigenden Gefahr tritt deshalb nun auch der Gesetzgeber entgegen. Im Januar 2023 ist eine neue Richtlinie der Europäischen Union (EU) über Netz- und Informationssysteme in Kraft getreten, die sog. NIS2-Richtlinie. Die Vorgaben aus der neuen Richtlinie hätten bereits bis zum 17. Oktober 2024 in deutsches Recht umgesetzt werden müssen. Das deutsche NIS2-Umsetzungsgesetz war schon weit im Entwurfsstadium vorangeschritten, wurde aber von dem Bruch der Ampelkoalition überholt. Dennoch müssen Unternehmen und die Geschäftsleitung sich schon jetzt auf NIS2 vorbereiten. Es ist nicht davon auszugehen, dass die Verschiebung der gesetzlichen Umsetzung über das Ende des Jahres 2025 hinausgeht.

Zugleich werden sich gegenüber der bisherigen Rechtslage die Pflichten und der Kreis der betroffenen Unternehmen erheblich ausweiten und verschärfen. Im Falle eines Verstoßes gegen die neuen Compliance-Vorgaben drohen empfindliche Bußgelder in Millionenhöhe. Besonders wachsam müssen Geschäftsführer und Vorstände der betroffenen Unternehmen sein. Sie werden persönlich in die Pflicht und Haftung genommen. Auf der anderen Seite kann die Umsetzung der NIS2 Vorgaben auch positive Effekte wie ein gesteigertes Kunden- oder Investorenvertrauen mit sich bringen. Insofern sollten Sie NIS2 auch als Chance für Ihr Unternehmen ansehen.

Flankiert wird NIS2 durch die am gleichen Datum in Kraft getretene EU Critical Entities Resilience Directive oder „*CER-Richtlinie*“, die ebenfalls bis zum 17. Oktober 2024 in nationales Recht zu überführen war. Diese Richtlinie stellt für „Betreiber kritischer Anlagen“ Anforderungen an die physische Resilienz auf (z.B. Schutzzäune, etc.). Alle Betreiber kritischer Anlagen unter der CER-Richtlinie werden automatisch auch unter NIS2 fallen. Die Umsetzung der CER-Richtlinie in Deutschland durch das sog. KRITIS-Dachgesetz teilt jedoch das Schicksal des NIS2-Umsetzungsgesetzes und verspätet sich bis auf Weiteres.

In diesem Whitepaper erfahren Sie, ob Ihr Unternehmen nach dem aktuellen Stand von NIS2[2] betroffen ist und was dies für Sie und Ihr Unternehmen bedeutet.

[2] Ein verabschiedetes Gesetz vom Bundestag liegt zum Redaktionsschluss dieses Papiers nicht vor. Das Papier beruht daher auf der NIS2-Richtlinie sowie den bis Juli 2025 veröffentlichten Entwürfen für ein deutsches NIS2-Umsetzungsgesetz.

Die aktuelle Gesetzeslage

Bislang galten Cybersicherheitsvorgaben nur für die Betreiber kritischer Infrastrukturen (sog. „KRITIS“-Betreiber), Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse. Die aktuellen Regelungen basieren auf der EU-NIS1-Richtlinie und finden sich im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und den begleitenden sog. KRITIS-Verordnungen. Diese Gesetzeslage bleibt bis zum Inkrafttreten eines reformierten BSI-Gesetzes durch das NIS2-Umsetzungsgesetz (und KRITIS-Dachgesetz) anwendbar.

Die Vorgaben aus der NIS2-Richtlinie selbst **gelten nicht unmittelbar** für Privatunternehmen. Stattdessen muss die Richtline erst in ein nationales Gesetz implementiert werden, damit die neuen Pflichten für sie anwendbar werden. Dasselbe gilt für die CER-Richtlinie. Zumindest eine mittelbare Bedeutung ergibt sich allerdings daraus, dass gerade große Unternehmen, die mit vielen Lieferanten arbeiten, vertraglich ihre Geschäftspartner bereits auf die Einhaltung der zum Stand der Technik zählenden Sicherheitsanforderungen gem. NIS2 verpflichten.

Aktueller Stand der neuen Gesetzgebung

In Deutschland verspätet sich die Umsetzung der NIS2- und CER-Richtlinie. Deshalb wurde seitens der Europäischen Union ein Vertragsverletzungsverfahren gegen die Bundesrepublik eingeleitet.

Zwar hatte die geschiedene Ampelkoalition bereits einen umfassenden Regierungsentwurf für ein sog. NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz („NIS2-UmsuCG“) in den Bundestag eingebracht. Nach der vorgezogenen Neuwahl des Deutschen Bundestages muss aber aufgrund des sog. *„Diskontinuitätsprinzips“* – jedenfalls formal – ein neuer Vorschlag in den Bundestag eingebracht werden.

Das nunmehr CSU-geführte Bundesinnenministerium (BMI) der neuen Bundesregierung hat mittlerweile einen Entwurf für ein *„Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“* verabschiedet. Dieser gleicht in weiten Teilen dem bekannten NIS2-UmsuCG-Entwurf der Ampel-Koalition. Wenn der Entwurf im Bundestag diskutiert und verabschiedet worden ist, soll das NIS2-Umsetzungsgesetz bis Ende 2025 in Kraft treten. Im Bundestag werden derweil Stimmen laut, die weitere Änderungen an dem vorgelegten Gesetzesentwurf fordern.

Andere Länder sind da schon weiter: Während etwa in Frankreich oder Polen ebenfalls bislang nur Entwürfe vorliegen, sind in Belgien, Italien, Kroatien, Litauen, Lettland und Ungarn bereits nationale NIS2-Umsetzungsgesetze in Kraft getreten.

Dessen ungeachtet mahnt das Bundesamt für Sicherheit in der Informationstechnik (BSI), welches als künftige Aufsichtsbehörde fungieren wird, Unternehmen zu einer raschen Vorbereitung auf NIS2. Denn ein künftiges NIS2-Umsetzungsgesetz wird aller Voraussicht nach keinerlei weitere Schonfristen mehr für Unternehmen vorsehen, sondern sofort mit Inkrafttreten anwendbar sein.

Im Anfang steht daher für Sie eine **Betroffenheitsprüfung:**

Ist mein Unternehmen betroffen?

In einem ersten Schritt sollten Sie sich einen Eindruck darüber verschaffen, ob Ihr Unternehmen möglicherweise von NIS2 betroffen ist und wenn ja, in welcher Kategorie. NIS2 stellt im Wesentlichen **zwei Kategorien** von Einrichtungen auf. Das sind zum einen die **wesentlichen Einrichtungen** und zum anderen die **wichtigen Einrichtungen**.[3] Nachdem in vergangenen Entwürfen für ein deutschen NIS2-Umsetzungsgesetz noch unterschiedliche Pflichten an diese Kategorien geknüpft wurden, war dies in den zuletzt diskutierten Entwürfen nicht mehr der Fall und Unterschiede zwischen wesentlichen und wichtigen Einrichtungen ergaben sich nur noch mit Blick auf die Höhe von Sanktionen sowie hinsichtlich Überprüfungen durch das BSI, die von wesentlichen Einrichtungen zu dulden sind. Ob dies im Laufe des Gesetzgebungsverfahrens noch geändert wird, bleibt abzuwarten.

Spezielle zusätzliche Pflichten gelten in jedem Fall für **Betreiber von kritischen Anlagen**. Die Betreiber kritischer Anlagen werden nicht in der NIS2-Richtlinie selbst definiert, sondern in der CER-Richtline. Die CER-Richtline soll in Deutschland durch das KRITIS-Dachgesetz sowie dazugehörigen KRITIS-Rechtsverordnungen umgesetzt werden. Die kritischen Anlagen werden sich weitestgehend mit den kritischen Infrastrukturen (KRITIS) nach bisheriger Rechtslage decken.[4] Dabei handelt es sich um Anlagen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil im Falle ihrer Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Ihre Kritikalität wird regelmäßig durch anlagenbezogene Schwellenwerte ermittelt.

[3] In der englischen Version der NIS2-Richtlinie wird der Begriff „essential entity“ verwendet, der in der offiziellen deutschen Übersetzung mit „wesentliche Einrichtung“ wiedergegeben wird. Der deutsche Gesetzgeber hat hingegen den Begriff „besonders wichtige Einrichtung“ verwendet. Zum besseren Verständnis, verzichtet das Whitepaper aber auf diesen Begriff und verwendet gleichbedeutend die Bezeichnung „wesentliche Einrichtung“ zu besseren Lesbarkeit.

[4] Das betrifft vor allem die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung.

NIS2 macht die Betreiber solcher Anlagen – unabhängig von der Größe des Unternehmens – automatisch zu wesentlichen Einrichtungen. Es ist aber auch nicht ausgeschlossen, dass durch die geänderte Rechtslage Unternehmen, die bisher nach BSI-Gesetz reguliert waren, sich nun nicht mehr unter den betroffenen Einrichtungen wiederfinden. Das könnte etwa für bisher regulierte *„Unternehmen im besonderen öffentlichen Interesse“* (*„UBI“*) gelten, denn diese entfallen als separate Begriffskategorie.

Sonderregelungen gelten auch für TLD-Name-Registries und DNS-Diensteanbieter, die unabhängig von ihrer Größe als wesentliche Einrichtungen gelten und spezielle Pflichten zu erfüllen haben (darunter die Pflicht zum Führen einer Datenbank über Domain-Namen-Registrierungsdaten und ein Zugangsgewährungsrecht für Behörden). Betreiber öffentlicher Telekommunikationsnetzwerke und Erbringer von öffentlichen Telekommunikationsdiensten sowie Betreiber bestimmter Energieanlagen nach dem Energiewirtschaftsgesetz werden nicht im BSI-Gesetz reguliert, sondern analog in den für diese Bereiche speziellen Gesetzen (TKG oder EnWG).

Wesentliche Einrichtungen

Unterfällt Ihr Unternehmen einem der folgenden Sektoren, stellt es **per se** eine *wesentliche Einrichtung* dar, und zwar unabhängig davon, ob es seine Dienste entgeltlich oder unentgeltlich erbringt:

- Betreiber einer Anlage aus dem Sektor Öffentliche Verwaltung – Zentralregierung;
- Betreiber kritischer Anlagen;
- Qualifizierte Vertrauensdiensteanbieter;[5]
- Top Level Domain Name Registries,
- DNS-Diensteanbieter.

[5] Zu den sog. Vertrauensdiensten zählen elektronische Dienste zur Erstellung, Überprüfung, Bewahrung und Validierung von elektronischen Signaturen oder ähnlichen Zertifizierungen. „Qualifiziert“ sind derartige Vertrauensdienste, wenn sie die speziellen Vorgaben der europäischen „eIDAS-Verordnung“ (electronic Identification, Authentication and Trust Service-Verordnung) erfüllen.

Besonders geregelt sind auch **Anbieter von Telekommunikationsdiensten[6] und öffentlich zugänglichen Telekommunikationsnetzwerken**. Solche Anbieter unterfallen den wesentlichen Einrichtungen, wenn sie 50 oder mehr Mitarbeiter beschäftigen oder einen Jahresumsatz plus eine Jahresbilanzsumme von jeweils über EUR 10 Millionen aufweisen. Auf Entgeltlichkeit kommt es auch in diesem Bereich nicht an.

Für **alle bisher noch nicht genannten Unternehmen** kommt es für die Frage, ob sie der Kategorie der wesentlichen Einrichtungen unterliegen, einerseits auf die **Größe** des Unternehmens und **zusätzlich** auf die Zugehörigkeit zu einem bestimmten **Sektor** an. Nur wenn **beide Voraussetzungen zugleich** erfüllt sind, ist Ihr Unternehmen von NIS2 als wesentliche Einrichtung erfasst. Im Gegensatz zu den oben genannten Sonderbereichen sind hier nach den bisherigen Entwürfen für ein deutsches Umsetzungsgesetz außerdem nur Unternehmen erfasst, die ihre Waren oder Dienstleistungen **gegen Entgelt** anbieten. Da diese Unterscheidung in der Richtlinie allerdings nicht angelegt ist, bleibt abzuwarten, ob dies auch in neuen Entwürfen beibehalten wird.

Das Größenkriterium:
Ihr Unternehmen kann die relevante Schwelle eines **Großunternehmens** auf zwei alternativen Wegen erreichen: zum einen, wenn im Unternehmen **250 oder mehr Mitarbeiter** beschäftigt sind; oder zum anderen, wenn es einen **Jahresumsatz von über EUR 50 Millionen und zudem eine Jahresbilanz von über EUR 43 Millionen** aufweist.

[6] Gemeint sind neben Diensten, die den Zugang zum Internet ermöglichen, v.a. Dienste, die eine Kommunikation im Verhältnis Mensch-Mensch oder Maschine-Maschine bezwecken (z.B.: Email- oder Chatprogramme). Nicht umfasst sind Dienste, bei denen die interpersonelle Kommunikation nur eine untergeordnete Nebenfunktion darstellt (nicht daher z.B. Onlineshops mit Chatfunktion).

Die Mitarbeiterzahl entspricht bisherigen Entwürfen zufolge der Zahl der Jahresarbeitseinheiten (JAE), das heißt der Zahl der Personen, die in dem Unternehmen oder auf Rechnung des Unternehmens während des gesamten Berichtsjahres einer Vollzeitbeschäftigung nachgegangen sind. Für die Arbeit von Personen, die nicht das ganze Jahr gearbeitet haben oder die im Rahmen einer Teilzeitregelung tätig waren, und für Saisonarbeit wird der jeweilige Bruchteil an JAE gezählt. Auszubildende oder in der beruflichen Ausbildung stehende Personen, die einen Lehr- bzw. Berufsausbildungsvertrag haben, sind in der Mitarbeiterzahl nicht berücksichtigt. Die Dauer des Mutterschafts- bzw. Elternurlaubs wird nicht mitgerechnet.

Besonderheiten ergeben sich bei der Zurechnung von Umsatzgrößen und Mitarbeiterzahlen in **Konzernstrukturen**: Nach Art. 2 NIS2-RL gilt diese für alle öffentlichen oder privaten Einrichtungen, die nach Art. 2 des Anhangs der Empfehlung 2003/361/EG („KMU-Empfehlung“) als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben. Gerade im Zusammenhang mit der Berechnung der maßgeblichen Kennzahlen in Konzernverhältnissen ist große Sorgfalt gefordert. Denn nach der KMU-Empfehlung sind in bestimmten Verhältnissen auch die Unternehmenskennzahlen von anderen Unternehmen zu berücksichtigen. Besitzt ein Unternehmen demnach sog. Partner- oder verbundene Unternehmen im Sinne der KMU-Empfehlung, werden bei der Ermittlung der o.g. Schwellwerte nicht nur die Unternehmenskennzahlen des eigentlichen Unternehmens herangezogen, sondern auch die Unternehmenskennzahlen aller Partner- bzw. verbundenen Unternehmen. Ferner ist zu berücksichtigen, dass auch verbundene Unternehmen, die nicht in Deutschland oder der EU ansässig oder tätig sind, bei der Berechnung der Schwellenwerte einzubeziehen sind.

Die Richtlinie macht in der Zurechnung der Werte von verbundenen und Partnerunternehmen keinen Unterschied, ob diese anderen Unternehmen ebenfalls auf einem NIS2-betroffenen Sektor tätig sind. Der obsolete Entwurf für das NIS2-UmsuCG enthielt noch eine Bestimmung, nach der bei der Schwellwertberechnung nur solche Geschäftsfelder einzubeziehen seien, die der betroffenen Einrichtungsart entsprechen. In neueren Entwürfen ist diese Beschränkung entfallen.

Nach dem deutschen Umsetzungsgesetz soll aktuell zudem eine solche Zurechnung der Kennzahlen von verbundenen Unternehmen u.a. dann nicht erfolgen, wenn das verbundene Unternehmen seine informationstechnischen Systeme, Komponenten und Prozesse rechtlich, wirtschaftlich und tatsächlich unabhängig betreibt. Durch diese Ausnahmeregelung soll eine Konzerngesellschaft, die eigenständig über ihre IT-Infrastruktur entscheiden kann, auch eigenständig bei der Schwellwertberechnung zu betrachten sein.

Das Sektor-Kriterium:
Erreicht Ihr Unternehmen diese Schwellenwerte, ist damit noch nichts entschieden. Es kommt zusätzlich auf die Zugehörigkeit zu einem der sogenannten Sektoren mit hoher Kritikalität an. Die Sektoren mit **hoher Kritikalität** sind im Einzelnen in umfangreichen Listen in den Anhängen der Richtlinie und des Entwurfs des NIS2-Umsetzungsgesetzes aufgelistet. Zu diesen Sektoren gehören etwa bestimmte Energieversorgungsunternehmen, Unternehmen aus dem Verkehrs- und Transportbereich, ausgewählte Unternehmen aus dem Gesundheitssektor sowie gewisse Unternehmen aus dem IT- und Telekommunikationssektor.

Eine genauere Prüfung ermöglicht Ihnen die Übersichtstabelle unten in diesem Whitepaper (s. Seite 11 →).

Wichtige Einrichtungen

Neben den *wesentlichen Einrichtungen* kennt die NIS2 Richtlinie noch eine zweite Kategorie der „nur“ wichtigen Einrichtungen. Tatsächlich bleiben die Compliance-Anforderungen an diese Unternehmenskategorie auf einem ähnlich hohen Niveau. Ob überhaupt Unterschiede in den Pflichten gemacht werden, muss die weitere Umsetzung von NIS2 zeigen.

Auch die Einstufung als wichtige Einrichtung hängt von dem Erreichen bestimmter **Größenwerte** und der Zugehörigkeit zu einem betroffenen **Sektor** ab.

Zu den betroffenen Sektoren gehören diesmal alle der bereits angesprochenen Sektoren mit hoher Kritikalität und zusätzlich die sog. **sonstigen kritischen Sektoren**, welche sich ebenfalls im Einzelnen aus langen Tabellen in den Anhängen der Gesetzesunterlagen ergeben.

Die Größenschwellen sind hier niedriger angesetzt: Sie werden bereits von allen Unternehmen erreicht, die mindestens 50 Mitarbeiter beschäftigen oder (alternativ) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils mehr als EUR 10 Millionen aufweisen (**„mittlere Unternehmen“**).

Per Se als wichtige Einrichtungen einzustufen sind nur (nichtqualifizierte) Vertrauensdiensteanbieter[8]. Grundsätzlich ausgenommen sind hingegen diejenigen Finanzunternehmen, die bereits aus der parallel eingeführten DORA Verordnung der EU vergleichbaren Anforderungen wie die wesentlichen Einrichtungen unterliegen.

[8] Siehe hierzu bereits oben, Fn. 5.

Übersichtstabelle

Sie werden gemerkt haben, dass die Prüfung der Betroffenheit von NIS2 kein leichtes Unterfangen ist.

Eine erste unverbindliche Einschätzung können Sie sich auch ohne eigene juristische Kenntnisse mit Hilfe unseres SKW Schwarz NIS2 Betroffenheitstools verschaffen (s. Seite 28 →).

Mit Blick auf die betroffenen Sektoren (mit hoher Kritikalität oder sonstige kritische Sektoren) ist eine hundertprozentig genaue Betroffenheitsanalyse ohne individuelle Rechtsberatung wohl auch gar nicht möglich. Denn die Anlagen der Gesetzesmaterialien enthalten ein schier unüberschaubares Dickicht an Sektoren und Untersektoren, Ausnahmen und Verweisungen auf andere Verordnungen.

Was dieses Whitepaper Ihnen aber bieten kann, ist untenstehend eine übersichtliche Tabelle, anhand derer Sie die Betroffenheit Ihres Unternehmens von NIS2 bestmöglich abschätzen können. Gleichzeitig können Sie prüfen, in welcher Kategorie Sie betroffen sind und welche konkreten Compliance-Vorgaben deshalb für Ihr Unternehmen gelten:

Übersichtstabelle

Größe ▸ Sektor ▾	Mitarbeiterzahl ≥ 250	Mitarbeiterzahl ≥ 50	Jahresumsatz > EUR 50 Mio. und Jahresbilanzsumme > EUR 43 Mio.	Jahresumsatz und Jahres-bilanzsumme > EUR 10 Mio.	Andere
Öffentliche Bundesverwaltung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung
Qualifizierter Vertrauensdiensteanbieter	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung
Nichtqualifizierter Vertrauensdiensteanbieter	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung
TLD-Name-Register, DNS-Diensteanbieter	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung
Betreiber kritischer Anlagen nach CER-Richtlinie / KRITIS-Dachgesetz	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung
Anbieter von Telekommunikationsdiensten oder öffentlich zugänglichen Telekommunikationsnetzen	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Wesentliche Einrichtung	Nicht betroffen
Energieversorgung					
Stromversorgung (weiter Begriff! Auch Betreiber von einzelnen Energieerzeugungsanlagen oder Betreiber von Ladepunkten für E-Fahrzeuge!)	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Fernwärme- bzw. Fernkälteversorgung	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Kraftstoff- und Heizölversorgung	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Gasversorgung	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Transport & Verkehr					
Verkehrsunternehmen aus Luft-, Schienen- und Schifffahrt, inkl. Infrastrukturbetreiber und Serviceunternehmen	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen

Übersichtstabelle					
Größe ▸ Sektor ▾	Mitarbeiterzahl ≥ 250	Mitarbeiterzahl ≥ 50	Jahresumsatz > EUR 50 Mio. und Jahresbilanzsumme > EUR 43 Mio.	Jahresumsatz und Jahres-bilanzsumme > EUR 10 Mio.	Andere
Betreiber von bestimmten Anlagen zur Straßenverkehrs-beeinflussung, z.B. Tunnel-leitzentralen	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Finanz- & Versicherungswesen					
Kreditinstitute, Wertpapier-handelsplätze und Central Counter Parties	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Gesundheit					
Erbringer von Gesundheits-dienstleistungen, z.B. Krankenhäuser	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Forschungs- und Entwicklung für Arzneimittel zur Anwendung beim Menschen	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Hersteller von pharmazeutischen Erzeugnissen	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Hersteller bestimmter kritischer Medizinprodukte	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Wasser- & Abwasser					
Trinkwasserversorgung und Abwasserbeseitigung, sofern nicht nur Nebentätigkeit	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
IT & Telekommunikation					
Betreiber von Internet Exchange Points (Internetknotenpunkten)	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Anbieter von Cloud-Computing-Diensten	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Anbieter von Rechenzentrumsdiensten	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Betreiber von Inhaltszustell-netzen (Content Delivery Networks)	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Anbieter öffentlicher elektronischer Kommunikationsnetze	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen

Übersichtstabelle					
Größe ▸ Sektor ▾	Mitarbeiterzahl ≥ 250	Mitarbeiterzahl ≥ 50	Jahresumsatz > EUR 50 Mio. und Jahresbilanzsumme > EUR 43 Mio.	Jahresumsatz und Jahres-bilanzsumme > EUR 10 Mio.	Andere
Managed Services Provider und Managed Security Services Provider	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Weltraum					
Bodeninfrastrukturen, die die Erbringung von weltraumgestützten Diensten unterstützen	Wesentliche Einrichtung	Wichtige Einrichtung	Wesentliche Einrichtung	Wichtige Einrichtung	Nicht betroffen
Post- & Kurierdienste	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Abfallbewirtschaftungs-unternehmen	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Produktion, Herstellung & Handel mit chemischen Stoffen	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Industrielle Produktion, Verarbeitung und Großhandel mit Lebensmitteln	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Verarbeitendes Gewerbe / Herstellung von Waren[1]					
Hersteller von Medizinprodukten	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Hersteller von Computern, Handys oder anderen elektronischen Geräten, inkl. einzelnen elektronischen Bauteilen	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Hersteller von Batterien und Akkumulatoren	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen

[9] Hierzu gehören unter anderem alle Unternehmen, deren Wirtschaftszweig in der sog. „Statistischen Systematik der Wirtschaftszweige der Europäischen Gemeinschaft“ unter den Abteilungen 26 bis 30 aufgelistet ist. Diese Statistik können sie hier aufrufen: https://ec.europa.eu/eurostat/documents/3859598/5902453/KS-RA-07-015-DE.PDF.pdf/680c5819-8a93-4c18-bea6-2e802379df86?t=1414781445000

Übersichtstabelle					
Größe ▸ Sektor ▾	Mitarbeiterzahl ≥ 250	Mitarbeiterzahl ≥ 50	Jahresumsatz > EUR 50 Mio. und Jahresbilanzsumme > EUR 43 Mio.	Jahresumsatz und Jahres-bilanzsumme > EUR 10 Mio.	Andere
Hersteller von Glasfaser- und anderen Kabeln	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Hersteller von Fahrzeugen und Maschinen aller Art, inkl. einzelner Bauteile	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Hersteller von Haushaltsgeräten	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Hersteller aus dem Bereich Luft-, Schiff- und Raumfahrt	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Anbieter digitaler Dienste					
Anbieter von Online-Marktplätzen	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Anbieter von Online-Suchmaschinen	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Anbieter von Plattformen für Dienste sozialer Netzwerke	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Wichtige Einrichtung	Nicht betroffen
Andere	Nicht betroffen	Nicht betroffen	Nicht betroffen	Nicht betroffen	Nicht betroffen

Konzerninterne Leistungen:

In Konzernstrukturen werden regelmäßig die Beschaffung und der Betrieb der IT-Infrastruktur – mithin Managed IT Services und Rechenzentrumsleistungen – in eine oder einzelne Konzerngesellschaften ausgelagert und zentralisiert. In diesem Fall stellt sich die Frage, ob solche IT-Konzerngesellschaften bei Überschreitung der Schwellenwerte aufgrund dieser Tätigkeit in den Anwendungsbereich von NIS2 fallen, was von besonderer Bedeutung ist, wenn der Konzern im Übrigen nicht einem der Sektoren zuzuordnen ist.

Laut ErwGr. 35 zur NIS2-RL sollen solche Unternehmen und Organisationen nicht als Anbieter von Rechenzentrumsdiensten gelten, die lediglich „interne Rechenzentren“ betreiben. Damit sind solche Einheiten, die ihre IT-Dienste rein intern im Unternehmen

erbringen, vom Anwendungsbereich der NIS2 nicht erfasst. Dies bedeutet im Umkehrschluss jedoch, dass solche Einheiten, die darüber hinaus ihre IT-Dienste auch für andere Konzerngesellschaften oder gar gegenüber Dritten anbieten, als klassische *„Anbieter von Rechenzentrumsdiensten“* oder „Managed Services Provider und Managed Security Services Provider“ einzustufen sind. Auch in den zuletzt diskutierten Entwürfen für das deutsche NIS2-Umsetzungsgesetz wird im Begründungsteil ausdrücklich festgehalten, dass ausgegliederte Konzern-IT-Gesellschaften in den Anwendungsbereich fallen können, auch wenn sie ihre Dienste ausschließlich anderen Konzerngesellschaften gegenüber erbringen.

Reine Nebentätigkeiten:
Die Richtlinie macht in der Frage der Betroffenheit indes keinen Unterschied, ob eine NIS2-betroffene Tätigkeit von dem Unternehmen als Haupt- oder nur als Nebentätigkeit ausgeführt wird. Der deutsche Gesetzgeber versucht, diesen weiten Anwendungsbereich einzugrenzen. Zuletzt findet sich eine Regelung im NIS2-Gesetzentwurf, nach der bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 solche Geschäftstätigkeiten unberücksichtigt bleiben können, „die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind.“.

Ob diese deutsche Ausnahmeregelung mit der NIS2-RL vereinbar und damit europarechtskonform ist, wird jedoch durchaus in Frage gestellt. Unternehmen sollten daher die weitere rechtliche Entwicklung streng im Auge behalten, bevor sie sich auf die Wirksamkeit der nationalen Regelung verlassen und NIS2 nicht anwenden.

Welche Compliance-Pflichten werden gelten?

Haben Sie einen Eindruck davon gewonnen, in welcher Kategorie Ihr Unternehmen von NIS2 betroffen ist, stellt sich weiter die Frage nach den konkret zu implementierenden Cyberschutzmaßnahmen. Abhängig davon, welche Kategorie einschlägig ist, unterliegt Ihr Unternehmen – aber auch die Geschäftsleitung selbst – bestimmten Compliance-Vorgaben.

Werfen Sie hierzu einen Blick in die zweite Tabelle weiter unten, um Ihre konkreten Compliance-Pflichten ableiten zu können. Bitte beachten Sie, dass die Unterscheidung zwischen wesentlichen und „nur“ wichtigen Einrichtungen in den letzten Entwürfen des deutschen Umsetzungsgesetzes nicht mehr zu Unterschieden im Pflichtenkatalog geführt hat. Lediglich die Duldung von Überprüfungen durch das BSI verblieb als Unterschied. Ob dies in einem neuen Entwurf der Unions-SPD geführten Regierung beibehalten wird, bleibt abzuwarten.

Ihre Compliance-Pflichten		
Pflicht	**Wesentliche Einrichtung**	**Wichtige Einrichtung**
▸ Risikomanagementmaßnahmen	✓	✓
▸ Billigung und Überwachung der Risikomanagementmaßnahmen durch die Geschäftsleitung	✓	✓
▸ Meldungen an das BSI im Falle eines erheblichen Sicherheitsvorfalles	✓	✓
▸ Registrierungspflicht gegenüber dem BSI	✓	✓
▸ Unterrichtung der Kunden im Falle eines erheblichen Sicherheitsvorfalls	✓	✓
▸ Teilnahme der Geschäftsleitung an Schulungen	✓	✓
▸ Pflicht zur Duldung von Überprüfungen durch das BSI	✓	-

Sonderbestimmungen für Betreiber bestimmter Einrichtungen	
Betreiber *kritischer Anlagen*:	Es gelten sämtliche Pflichten für *wesentliche Einrichtungen*. Zusätzlich gilt Folgendes: ✓ Höherer Aufwand bei Risikomanagementmaßnahmen ✓ Nachweis der Risikomanagementmaßnahmen ✓ Einsatz von Systemen zur Angriffserkennung ✓ Erweitere Meldepflicht bei erheblichem Sicherheitsvorfall ✓ Erweiterte Registrierungspflicht
Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister	Es gelten sämtliche Pflichten für *wesentliche Einrichtungen*. Zusätzlich gilt Folgendes: ✓ Sammlung und Pflege von DNS-Registrierungsdaten in eigener Datenbank ✓ Vorhaltung von öffentlichen Verfahren zur Überprüfung der Genauigkeit und Vollständigkeit der Datenbank ✓ Unverzügliche öffentliche Zugänglichmachung der nichtpersonenbezogenen DNS-Registrierungsdaten nach einer Registrierung eines Domain-Namens ✓ Zugangsgewährung gegenüber Behörden ✓ Kooperation zwischen TLD Name Registries und DNS-Diensteanbieter

Wo besteht schon jetzt Handlungsbedarf?

Risikomanagementmaßnahmen: Handlungsbedarf!

Wesentliche und wichtige Einrichtungen sind dazu verpflichtet, sog. Risikomanagementmaßnahmen zu ergreifen. Die Geschäftsleitung muss diese Maßnahmen billigen und überwachen. Betreiber kritischer Anlagen sind zudem verpflichtet, die Einführung solcher Maßnahmen gegenüber dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) nachzuweisen.

Mit der Einführung von Risikomanagementmaßnahmen sollten Sie bereits jetzt beginnen.

Konkret geht es dabei um Maßnahmen technischer und organisatorischer Art, die dazu geeignet sind, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten und Prozesse, die Ihr Unternehmen nutzt, zu vermeiden. Die Maßnahmen müssen geeignet und wirksam sein, die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Die Maßnahmen müssen verhältnismäßig sein und sich an der individuellen Risikoexposition der jeweiligen Einrichtung orientieren. Tendenziell gilt hier: Je höher der zu erwartende Schaden bei einem Sicherheitsvorfall und je höher dessen Wahrscheinlichkeit, desto höher ist auch der Maßnahmenaufwand, der Ihnen zugemutet werden kann. Für die Betreiber kritischer Anlagen gelten hier besonders hohe Anforderungen. Es sind also auch aufwändigere Maßnahmen als verhältnismäßig anzusehen. In jedem Falle sollen die Maßnahmen den jeweils aktuellen Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen.[10]

[10] Der Bundesverband IT-Sicherheit e.V. hat am 17.06.2025 eine vollständig überarbeitete und ergänzte Fassung der Handreichung „Stand der Technik in der IT-Sicherheit“ veröffentlicht, abrufbar hier: https://www.teletrust.de/fileadmin/user_upload/2025-06_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf. Die Handreichung soll Unternehmen Hilfestellung zur Bestimmung des Standes der Technik in der IT-Sicherheit bieten und kann als Referenz z.B. für vertragliche Vereinbarungen und für die Einordnung implementierter Sicherheitsmaßnahmen dienen.

Zum Mindeststandard im Pflichtenprogramm der Risikomanagementmaßnahmen zählen:

→ **eine Risikoanalyse Ihres Unternehmens**
Einrichtungen müssen Risiken identifizieren, analysieren und bewerten. Auf dieser Basis sind geeignete Sicherheitsmaßnahmen zu planen und umzusetzen, um die eigene Angriffsfläche zu minimieren (u.a. was macht Ihnen Sorge und wie realistisch sind Ihre Sorgen?),

→ **ein Back-Up-Management zur Wiederherstellung des Betriebs nach einem Notfall**
Einrichtungen müssen Maßnahmen zur Sicherstellung der Betriebsfähigkeit im Falle eines Sicherheitsvorfalles ergreifen und erproben. Dazu gehören regelmäßige Backups, Wiederherstellungspläne und die Identifikation kritischer Geschäftsprozesse, um Ausfälle zu begrenzen (u.a. wo liegen die Back-ups, wie weit reichen sie zurück, wer kann sie anfordern und wie schnell lassen sie sich wieder einspielen?),

→ **Prüfung der Sicherheit von Lieferketten**
Risiken, die durch Dienstleister und Zulieferer entstehen, müssen systematisch bewertet und gesteuert werden. Dies umfasst u.a. vertragliche Cybersicherheitsklauseln und ein Lieferanten-Risikomanagement-System (u.a. sind alle Ihre wichtigen Lieferanten genau so gut aufgestellt wie Ihr Unternehmen, bzw. weiß Ihr Lieferant überhaupt, was Sie von ihm erwarten und verlassen Sie sich dabei allein auf die Selbstauskunft des Lieferanten?),

→ **Schulungen der Mitarbeiter im Bereich Cybersicherheit**
Mitarbeitende müssen regelmäßig zu Cybersicherheitsrisiken und zu Verhalten bei (möglichen) Sicherheitsvorfällen geschult werden (u.a. wie oft schulen Sie oder sind Ihre Mitarbeitenden schon „schulungsmüde“? Wann genügen Online Schulungen? Nutzen Sie die Chancen Mitarbeitende über Schulungen zu Ihrer wichtigsten Verteidigungslinie aufzubauen?),

→ **Bewältigung von Sicherheitsvorfällen; konzernübergreifende (analoge) Meldeketten**
Es müssen Prozesse und Pläne zur Erkennung, Meldung und Bewältigung von Cybervorfällen etabliert werden. Dazu zählen Notfallpläne, Incident-Response-Teams und regelmäßige Tests der Reaktionsfähigkeit, um im Ernstfall schnell und effektiv handeln zu können (u.a. wo haben Sie die wichtigsten Kontaktdaten griffbereit, wenn die digitalen Systeme nicht verfügbar sind? Sind alle Entscheidungsträger immer erreichbar, wenn sie benötigt werden? Welche anderen Meldeprozesse haben Sie bereits installiert, die Sie hier mitnutzen können (z.B. nach DSGVO)?),

→ **der Einsatz von Kryptografie und Verschlüsselung**
Es sind angemessene Verschlüsselungstechnologien in Betracht zu ziehen und zu implementieren (u.a. entsprechen die Schlüssellängen und –technologien noch dem aktuellen Stand der Technik?),

→ **Verfahren zur Zugriffskontrolle von Anlagen und Systemen**
Es sind technische und organisatorische Maßnahmen zur Kontrolle und Protokollierung von Zugriffen auf Systeme und Daten zu implementieren. Dazu zählen rollenbasierte Zugriffsrechte, regelmäßige Überprüfung von Berechtigungen und der Schutz vor Schadsoftware (u.a. haben Sie ein aktuelles Berechtigungs- und Rollenkonzept? Wie oft prüfen Sie dessen Aktualität?),

→ **eine Multi-Faktor-Authentifizierung (MFA) oder kontinuierliche Authentifizierung**
(Ohne MFA wird es heutzutage sehr schwer, den Vorwurf der Fahrlässigkeit zu vermeiden!),

→ **gesicherte Notfallkommunikationssysteme.**

Praxistipp: Wie kann die Umsetzung dieser NIS2-Vorgaben in der Praxis gelingen?

Der Gesetzgeber macht keine expliziten Vorgaben hinsichtlich der Art und Weise der Umsetzung. Wir haben in der Beratungspraxis allerdings gute Erfahrungen mit folgendem, zweistufigem Vorgehen gemacht:

Im **ersten Schritt** empfiehlt sich eine **GAP-Analyse** zur Bestimmung des **NIS2-Reifegrades**. Dabei wird - jeweils konkret bezogen auf die o.g. Anforderungen von NIS2 – der IST-Zustand der Einrichtung mit dem SOLL-Zustand unter NIS2 abgeglichen. Dies kann beispielsweise in einem Workshop erreicht werden, an dem Vertreter der Geschäftsleitung, die IT (CISO-Level als auch operative IT) sowie die Rechtsabteilung teilnehmen. Es bietet sich an, den Workshop anhand eines bewährten Fragenkataloges zu strukturieren, der die o.g. Anforderungen von NIS2 in detaillierterer Tiefe adressiert. In dieser Weise kann jeweils eine Reifegradbestimmung im Hinblick auf die einzelnen Anforderungen getroffen werden. Je nach Stand der Einrichtung, kann dabei auf bereits vorhandene Zertifizierungen (bspw. ISO 27001) aufgesetzt werden. **Aber Achtung:** ISO 27001 und NIS2 haben viele Überscheidungen, sind aber leider nicht identisch. Es genügt nicht, sich allein auf ISO 27001 Kataloge zu verlassen, sondern es braucht ein konkretes Mapping zu den NIS2 Anforderungen.

Es obliegt der Einrichtung selbst, ob sie dabei auf die Unterstützung eines externen Dienstleisters zurückgreift. SKW Schwarz hat gemeinsam mit externen technischen Kooperationspartnern einen Workshop konzipiert, in dem wir die Reifegradbestimmung anhand eines Fragenkataloges vornehmen, der sowohl die rechtlichen Anforderungen, als auch die technischen Anforderungen adressiert (interdisziplinärer Ansatz aus Recht & Technik). Die Reifegradbestimmung inkl. der ggf. identifizierten GAPs wird sodann in einem Abschlussbericht festgehalten und dokumentiert.

Im **zweiten Schritt** sind die ggf. identifizierten GAPs anhand eines Maßnahmenplanes, der auch Prioritäten festlegt, zu schließen. Die Abarbeitung des Maßnahmenplanes sollte wiederum dokumentiert werden.

Registrierungspflicht: Noch kein akuter Handlungsbedarf

Wesentliche und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, sich beim BSI zu registrieren. Nach Inkrafttreten des Gesetzes (voraussichtlich bis Ende 2025) haben Sie dafür **drei Monate** Zeit, sofern Ihr Unternehmen in diesem Zeitpunkt als eine der vorgenannten Einrichtungen gilt. Insofern ist hier akut noch kein Handlungsbedarf gegenüber dem BSI. Im Rahmen der Registrierungspflicht muss das Unternehmen allerdings u.a. einen aktuellen Kontakt inkl. E-Mail-Adresse, IP-Adressbereichen und Telefonnummern benennen. Dieser **NIS2-Kontakt** und seine notwendige Vertretung müssen frühzeitig identifiziert und ggf. geschult oder über organisatorische Maßnahmen zur Wahrnehmung dieser Aufgabe befähigt werden. Auch hier gilt es schon jetzt die Entwicklung zu beobachten und die Verantwortlichen im Unternehmen zu identifizieren.

Eine besondere Herausforderung mag sich dabei für Unternehmen und Konzernverbünde stellen, die in mehreren EU-Mitgliedsstaaten tätig sind und EU-weit Niederlassungen betreiben. Für diese Unternehmen stellt sich die Frage, bei welcher Aufsichtsbehörde die Registrierungspflicht besteht. Laut Gesetzesbegründung zum Entwurf des NIS2-Umsetzungsgesetzes soll für Konzernstrukturen unter Effizienzgesichtspunkten die Benennung einer oder mehrere **einheitlicher Kontaktstellen** innerhalb des Konzerns für mehrere Unternehmensteile sinnvoll sein. Daher soll die Benennung einer solchen einheitlichen Kontaktstelle grundsätzlich ermöglicht werden, sofern sichergestellt ist, dass für alle registrierungspflichtigen Einrichtungen bzw. Anlagen die erforderlichen Informationen vorliegen, und die benannte übergeordnete Kontaktstelle innerhalb des Konzerns auch auf anlagen- oder einrichtungsspezifische Rückfragen des BMI Auskunft geben kann. Damit wird zunächst die grundsätzliche Möglichkeit geschaffen, innerhalb eines Konzerns eine zentrale Kontaktstelle in Deutschland zu benennen.

Hieraus folgert allerdings kein übergreifendes Konzernprivileg in dem Sinne, dass bei europaweit agierenden Konzernen die Registrierung einer Kontaktstelle für den gesamten Konzern ausreichen würde. Vielmehr ist jede Legaleinheit für sich zu betrachten und die Zuständigkeit der entsprechenden Aufsichtsbehörde zu prüfen. Insoweit ist gemäß Art. 26 NIS2-RL jeder Mitgliedsstaat zuständig, in dem eine registrierungspflichtige Einrichtung eine Niederlassung betreibt.

Eine Ausnahme besteht für solche Einrichtungen, die per se örtliche ungebundene Dienste erbringen, nämlich:

- DNS-Diensteanbieter,
- TLD-Namenregister,
- Einrichtungen, die Domänennamen-Registrierungsdienste erbringen,
- Anbieter von Cloud-Computing-Diensten / Rechenzentrumsdiensten,
- Betreiber von Inhaltszustellnetzen,
- Anbieter von verwalteten Diensten,
- Anbieter von verwalteten Sicherheitsdiensten sowie
- Anbieter von Online Marktplätzen, Online Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke.

Für diese Einrichtungen besteht die Registrierungspflicht bei der Aufsichtsbehörde des Mitgliedsstaates, in der sie ihre Hauptniederlassung haben, mithin dort wo die Entscheidungen im Bereich Cybersicherheitsrisikomanagement vorwiegend getroffen werden.

Anbieter öffentlicher elektronischer Kommunikationsnetze und Kommunikationsdiensteanbieter unterliegen wiederum den Aufsichtsbehörden der Mitgliedsstaaten, in denen sie ihre Dienste erbringen.

Dies hat zur Konsequenz, dass gerade bei europaweit tätigen Konzernen, die in verschiedenen Geschäftsfeldern tätig sind, in Abhängigkeit ihrer Tätigkeitsbereiche die Pflicht zur Registrierung bei verschiedenen Aufsichtsbehörden besteht. Innerhalb Deutschlands kann dann eine zentrale Kontaktstelle unter den oben genannten Voraussetzungen benannt werden.

Meldepflichten: Handlungsbedarf!

Wesentliche Einrichtungen und wichtige Einrichtungen sind dazu verpflichtet, dem BSI im Falle eines sog. erheblichen Sicherheitsvorfalles Statusmeldungen zu übermitteln. Hierbei handelt es sich etwa um besonders kritische Cyberangriffe oder andere Ereignisse, die besonders schwerwiegende Störungen im IT-und Datensystem des Unternehmens hervorrufen.

Die konkrete Pflicht zur Meldung entsteht zwar erst im Moment eines konkreten erheblichen Sicherheitsvorfalls. Dennoch sollten Unternehmen bereits jetzt entsprechende innerbetriebliche **Meldeketten** einrichten und diese auf ihre Funktionsfähigkeit **testen**. Schon vor dem Eintritt eines Sicherheitsvorfalls sollten die Zuständigkeiten festgelegt sein, wer über die Übermittlung einer Meldung entscheidet und wer die Meldung übermittelt. Denn spätestens innerhalb von **24 Stunden** nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall muss eine **frühe Erstmeldung** an das BSI abgegeben werden. Dann wird kaum Zeit sein, diese Meldewege zu identifizieren und aufzustellen.

In der frühen Erstmeldung muss angegeben werden, ob der Verdacht besteht, dass der Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte. *Wer im Unternehmen kann dies ermitteln, wo liegen die benötigten Informationen und welche externe Unterstützung wird hierfür benötigt?*

Spätestens **nach 72 Stunden** muss eine **weitere Statusmeldung** abgegeben werden, in der die Informationen der ersten Meldung aktualisiert werden und eine erste Bewertung der Folgen des Sicherheitsvorfalls angegeben wird. Auch diese Frist kann in den meisten Fällen nur eingehalten werden, wenn die Infrastruktur hierfür bereits aufgebaut ist und die Verantwortlichkeiten sowohl im Unternehmen als auch in Zusammenarbeit mit Dienstleistern und Kunden geklärt und bekannt sind.

Spätestens **einen Monat** nach der zweiten Statusmeldung muss eine Abschlussmeldung an das BSI übermittelt werden, die einen Bericht und eine Analyse über die Auswirkungen des Vorfalls, seine Ursachen und die getroffenen Abhilfemaßnahmen enthalten muss.

Zu beachten bleiben gleichzeitig noch die bereits bestehenden **Meldepflichten gemäß der Datenschutzgrundverordnung (DSGVO)**. Sofern der Vorfall zu einer Verletzung des Schutzes personenbezogener Daten geführt hat (es genügt, dass die Daten dem Verantwortlichen z.B. durch Verschlüsselung oder blockierte Systeme nicht zugänglich waren), muss der datenschutzrechtlich Verantwortliche hierüber (möglichst) innerhalb von 72 Stunden eine Meldung an die Datenschutz-Aufsichtsbehörde machen. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche auch die betroffene Person unverzüglich von der Verletzung.

Wie ist jedoch mit den Meldepflichten im Falle eines Vorfalls umzugehen, der mehrere Unternehmen einer Unternehmensgruppe betrifft? Wurde bei der Aufsichtsbehörde im Rahmen der Registrierung eine einheitliche Kontaktstelle hinterlegt, ist es zur Wahrung der Meldeobliegenheit ausreichend, wenn diese Kontaktstelle auch Meldungen für andere Konzernunternehmen durchführt, soweit sie zu anlagen- oder einrichtungsspezifischen Rückfragen des BMI Stellung nehmen kann. Betrifft ein meldepflichtiger Sicherheitsvorfall mehrere Einrichtungen innerhalb einer Konzerngruppe und sind für diese Einrichtungen innerhalb der Konzerngruppe eine oder mehrere einheitliche, ggf. auch geschäftsbereichsübergreifende Kontaktstellen benannt, so kann bei Abgabe einer Vorfallsmeldung auch unmittelbar im Meldeformular angegeben werden, welche weiteren Einrichtungen innerhalb des Konzerns vom Vorfall betroffen sind. Mehrfachmeldungen innerhalb einer Konzerngruppe zu ein- und demselben Vorfall sind mithin nicht zwingend erforderlich.

Bei grenzüberschreitenden Sicherheitsvorfällen besteht die Meldepflicht konsequenterweise mithin gegenüber jeder für die Einrichtung zuständigen Aufsichtsbehörde, in deren Zuständigkeitsbereich der Sicherheitsvorfall sich auswirkt.

Unterrichtungspflichten: Handlungsbedarf!

Wesentliche Einrichtungen und wichtige Einrichtungen sind im Falle eines erheblichen Sicherheitsvorfalls auf Anweisung des BSI verpflichtet, **die Empfänger ihrer Leistungen** unverzüglich über den erheblichen Sicherheitsvorfall zu unterrichten, soweit der Vorfall geeignet ist, die Erbringung der jeweiligen Leistung zu beeinträchtigen.

Da der Unterrichtungspflicht eine **Anweisung des BSI** vorausgehen muss, besteht zwar insoweit noch kein akuter Handlungsbedarf. Dennoch sollten Unternehmen – entsprechend den Meldeketten an das BSI – schon jetzt **vorbereitende Maßnahmen** ergreifen. Dazu gehört insbesondere, Melde- und Entscheidungsketten einzurichten und sie zu testen. Auch sollte eine **NIS2-Kontaktperson** bestimmt werden, die Anweisungen des BSI entgegennimmt und die in der Erstmeldung an das BSI benannt wird.

Wesentliche und wichtige Einrichtungen aus den Sektoren Finanz- und Versicherungswesen, IT und Telekommunikation, Verwaltung von IKT-Diensten und digitale Dienste sind jedoch **auch ohne Anweisung** des BSI dazu verpflichtet, den potentiell von einer erheblichen Cyberbedrohung betroffenen Empfängern und dem BSI unverzüglich alle Maßnahmen mitzuteilen, die die Kunden als Reaktion auf diese Bedrohung ergreifen können. Diese Unterrichtungspflicht greift allerdings nur dann, wenn in Abwägung der Interessen der Einrichtung und derjenigen des Kunden, die Interessen des Kunden überwiegen. Die Einrichtung und Testung entsprechender **Meldeketten** ist auch hier dringend zu empfehlen.

Schulungen der Geschäftsleitung: Handlungsbedarf!

Die Geschäftsleiter wesentlicher Einrichtungen und wichtiger Einrichtungen werden nach der neuen Rechtslage regelmäßig an Schulungen teilnehmen müssen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben. Aufgrund der **persönlichen Haftung** der Geschäftsleiter mit Blick auf die Risikomanagementmaßnahmen ist eine möglichst frühzeitige Ansetzung solcher Schulungen ebenso wie die regelmäßige Auffrischung anzuraten! Zudem sollte jede Schulung sorgfältig dokumentiert werden, um sie im Zweifelsfall nachweisen zu können.

Überprüfungen durch das BSI: Noch kein akuter Handlungsbedarf.

Das BSI wird bei wesentlichen Einrichtungen die Einhaltung der Compliance-Vorgaben nach dem neuen deutschen NIS2 Umsetzungsgesetz überprüfen können. Zum Zwecke der Überprüfung muss die Einrichtung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten gestatten. Gegenüber wesentlichen Einrichtungen wird das BSI auch verbindliche Anweisungen in Bezug auf Maßnahmen zur Umsetzung der Compliance-Vorgaben erlassen können. Auch wenn hier noch kein akuter Handlungsbedarf besteht, sollten Sie Ihr Unternehmen auf solche Überprüfungen vorbereiten. Denn wenn es einmal so weit ist, sollte ein Ablaufplan und geeignete Infrastruktur (z.B. Datenaufbereitungsräume) zur Verfügung stehen, um die Behörde zu unterstützen und betriebliche Interessen (z.B. Geheimnisschutz) beim Zugriff durch die Behörde zu wahren. Sorgen Sie daher rechtzeitig dafür, dass Sie die herausgabepflichtigen Daten von denen trennen können, zu denen das BSI keinen Zugriff benötigt und die vertraulich bleiben sollten.

Systeme zur Angriffserkennung: Handlungsbedarf!

Die Betreiber kritischer Anlagen werden zum Einsatz von sog. Systemen zur Angriffserkennung verpflichtet. Die Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollen dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Der Einsatzaufwand ist im Verhältnis zu den Folgen eines Sicherheitsvorfalls zu sehen. Zu bedenken gilt es, dass solche Systeme einer fortlaufenden Aktualisierung bedürfen, damit sie jederzeit den gesetzlichen Anforderungen entsprechen und zuverlässig alle aktuellen Bedrohungen abwehren können.

Welche Bußgelder drohen?

Die Pflicht zur Einführung von **Risikomanagementmaßnahmen** sollte besser ernst genommen werden. Denn die vorsätzliche oder fahrlässige Nichtergreifung oder mangel- oder lückenhafte Umsetzung stellt eine **Ordnungswidrigkeit** dar, die bei wesentlichen Einrichtungen mit einer Geldbuße bis zu **EUR 10 Mio.** oder einem Höchstbetrag von **2% des Vorjahresumsatzes** geahndet wird. Das gilt auch für eine verspätete Umsetzung der Maßnahmen! Bei wichtigen Einrichtungen sind die Höchstbeträge mit **EUR 7 Mio.** und **1,4% des Vorjahresumsatzes** etwas niedriger angesetzt, aber dennoch empfindlich.

Betreiber kritischer Anlagen sollten zudem an die **Nachweispflicht** über die Risikomanagementmaßnahmen denken, die erstmalig drei Jahre nach Inkrafttreten des Gesetzes fällig wird. Schon das Fehlen des Nachweises kann die o.g. Bußgelder nach sich ziehen. Das Gesetz dreht an dieser Stelle die **Beweislast zu Lasten der Unternehmen**: Nicht das BSI oder ein anderer Dritter muss Ihnen einen Verstoß nachweisen, sondern Sie müssen zeigen, dass Sie alles richtiggemacht haben.

Kommt die Geschäftsleitung von wichtigen und wesentlichen Einrichtungen ihrer persönlichen Pflicht zur Billigung und Überwachung der Risikomanagement-maßnahmen nicht nach und entsteht dem Unternehmen daraus ein Schaden, **haftet die Geschäftsleitung persönlich**. Ein Ausschluss der persönlichen Haftung ist – auch im Nachhinein – nicht möglich! Versicherungsunternehmen werben in diesem Zusammenhang bereits mit einer Einbeziehung des Schutzes in ihre Managerhaft-pflichtversicherungen (**D&O-Versicherungen**). Bei (grob) fahrlässigen und vorsätzlichen Verstößen schließt aber auch die D&O-Versicherung üblicherweise den Schutz aus.

Die Wichtigkeit funktionierender **Meldeketten** kann an dieser Stelle gar nicht überbe-tont werden. Denn auch mangelnde, verspätete, oder falsche Meldungen an das BSI stellen eine **Ordnungswidrigkeit** dar, die entsprechend verfolgt wird.

Auch eine falsche oder verspätete **Registrierung** als wesentliche oder wichtige Einrichtung beim BSI (drei Monate nach Inkrafttreten) zieht ein Bußgeld – bis zu **EUR 500.000** – nach sich.

Schließlich sollte **Aufforderungen und Anweisungen des BSI im Einzelfall** nach-gekommen werden. Denn dem BSI stehen bußgeldbewehrte Aufsichts- und Durch-setzungsmaßnahmen zu. Während dies bei den wesentlichen Einrichtungen durchaus auch einmal zu anlasslosen Überprüfungen führen kann, muss bei den wichtigen Einrichtungen hierfür zumindest ein Anfangsverdacht für mangelhafte Zustände in dem Unternehmen gegeben sein.

Wie können wir Sie unterstützen?

SKW Schwarz unterstützt Sie ganzheitlich bei der NIS2-Umsetzung. Unser Leistungsspektrum umfasst:

- Die Durchführung einer Reifegradbestimmung („GAP-Analyse“) im Hinblick auf die Anforderungen der NIS2-Richtlinie bzw. des nationalen Umsetzungsgesetzes. Bei der Reifegradbestimmung arbeiten wir mit unseren technischen Dienstleistern zusammen. Ein Abschlussbericht dokumentiert den Reifegrad und gibt Handlungsempfehlungen für die Schließung etwaig vorhandener Schwachstellen. Ihr Mehrwert: Sie erhalten einen klaren, umsetzbaren Fahrplan, der Sie durch die NIS2-Compliance führt. Die Reifegradbestimmung – inklusive Workshop und Abschlussbericht – bieten wir gerne zu einem angemessenen Pauschalpreis an.

- Die Beantwortung sämtlicher, rechtlicher Spezialfragen rund um NIS2, beispielsweise zur Betroffenheit, zu Meldepflichten, zu Dokumentationspflichten, zu Vertragsklauseln in Verträgen mit Zulieferern und Dienstleistern.

- Die Korrespondenz mit Aufsichtsbehörden.

- Die Durchführung von Schulungen für Mitarbeiter/innen und Geschäftsleitung (soweit dies technische Details betrifft, führen wir diese in Kooperation mit technischen Dienstleistern durch).

Weiterführende Informationen

Mit dem **NIS2-Tool von SKW Schwarz** haben Sie die Möglichkeit, sich einen ersten kostenlosen Überblick zur Frage der Betroffenheit Ihres Unternehmens von der NIS2-Richtlinie zu verschaffen. Unser kostenloses Betroffenheits-Tool sowie weitere hilfreiche Tipps und Infos finden Sie auf unserer NIS2-Landingpage (→).

Auch das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** bietet mit zahlreichen Beiträgen auf ihrer Website praxisnahe Hilfestellungen zur Umsetzung der NIS2-Richtlinie. Dazu zählen Webinare im Rahmen der Beitragsreihe „nis-2know“, die über aktuelle Entwicklungen und notwendige Maßnahmen informieren, sowie hilfreiche Artikel u.a. zur Risikoanalyse, Meldepflicht und ein (sektorspezifisches) FAQ.

Neben einer anschaulichen Darstellung der Neuerungen samt Video hat die **European Union Agency for Cybersecurity (ENISA)** eine *„Technical Implementation Guidance“* veröffentlicht, die kostenfrei heruntergeladen werden kann. Dieser Leitfaden bietet eine wertvolle Orientierung für die praktische Umsetzung und beinhaltet unter anderem ein Mapping zu relevanten ISO-Normen.

Ihre Ansprechpartner bei uns

Jan-Dierk Schaal
Partner

+49 (0)40 3 34 01 - 340
j.schaal@skwschwarz.de

Dr. Matthias Orthwein
Partner

+49 (0)89 2 86 40 - 102
m.orthwein@skwschwarz.de

Fabian Bauer
Counsel

+49 (0)69 63 00 01 - 82
f.bauer@skwschwarz.de

Henrik Hofmeister
Associate

+49 (0)89 2 86 40 - 102
h.hofmeister@skwschwarz.de

Weitere Autorin

Franziska Wulf
Wissenschaftliche Mitarbeiterin

10719 Berlin
Kranzler Eck
Kurfürstendamm 21
T +49 30 8892650-0
F +49 30 8892650-10

60598 Frankfurt/Main
Mörfelder Landstraße 117
T +49 69 630001-0
F +49 69 6355-22

20457 Hamburg
Willy-Brandt-Straße 59
T +49 40 33401-0
F +49 40 33401-530

80333 München
Wittelsbacherplatz 1
T +49 89 28640-0
F +49 89 28094-32

skwschwarz.de