Neues Diskussionspapier zur NIS-2 – Analyse und Key Facts

Nach dem Inkrafttreten der NIS-2 Richtlinie Anfang dieses Jahres warten viele Unternehmen gespannt auf deren Umsetzung in deutsches Recht. Klar ist bisher, dass der Anwendungsbereich der neuen Regelungen deutlich erweitert wird, sodass künftig **auch viele mittelständische Unternehmen betroffen sind**. Derzeit unterliegen die Details zur Umsetzung der NIS-2 Vorgaben noch einem dynamischen Veränderungsprozess. Das zeigt sich vor allem daran, dass im September ein neuer Referentenentwurf veröffentlicht wurde, welcher als Diskussionspapier diente und auf den mehr als 30 Verbände und Institutionen mit Stellungnahmen reagiert haben. Diese wurden schließlich vom Bundesministerium für Inneres („BMI“) in einem **Werkstattgespräch Ende Oktober 2023** mit den Beteiligten Verbänden und Institutionen aufgenommen und fließen in die kommende Ressortabstimmung des BMI mit ein.

Die wichtigsten Veränderungen im Vergleich zum zweiten Referentenentwurf werden nachfolgend kurz dargestellt:

1. Nachweispflichten

Eine der wohl wichtigsten Änderungen des Diskussionspapiers besteht im Bereich der Nachweispflichten. Statt der anfänglich vorgesehenen zwei-jährlichen Prüfungen für KRITIS- Betreiber und besonders wichtige Einrichtungen, wurde die Spanne nun auf drei Jahre angehoben. Zudem sollen nur noch die Betreiber kritischer Anlagen der Pflicht unterliegen. Der letzte Referentenentwurf sah noch eine Nachweispflicht für besonders wichtige Einrichtungen vor. Für diese soll die Nachweispflicht jedoch nur noch auf Verlangen des Bundesamtes für Sicherheit in der Informationstechnik bestehen.
Die Form der Nachweispflichten in Form von Audits, Prüfungen und Zertifizierungen bleibt laut dem Diskussionspapier weiter bestehen. Die Änderung des Nachweiszeitraums hat zur Folge, dass die ersten Prüfungen frühestens im Oktober 2027 stattfinden werden.

Von diesen Nachweispflichten zu unterscheiden ist die vom Gesetzgeber angestrebte Rechenschaftspflicht im Sinne von Art. 5 Abs. 2 DSGVO analog. Während

die Nachweispflicht betroffene Unternehmen dazu verpflichtet, die Einhaltung von Risikomanagement-maßnahmen innerhalb eines bestimmten Zeitraums unaufgefordert nachzuweisen, ist die Umsetzung von Maßnahmen bei der Rechenschaftspflicht beständig zu dokumentieren. Die Vorlage dieser Dokumente hat nach Aufforderung durch das BSI zu erfolgen, beispielsweise bei Stichproben oder im Anschluss eines Vorfalls, sodass diese stets auf aktuellem Stand bereitzuhalten sind.

2. Betreiber & Sektoren

In dem Diskussionspapier wurden zudem die betroffenen Betreiber & Sektoren weitergehend konkretisiert. Anlage 1 und 2 des Entwurfs nennen zum einen **„Sektoren mit hoher Kritikalität" (Anlage 1)** und zum anderen **„Sonstige kritische Sektoren" (Anlage 2).** Auf dieser Basis soll die Einteilung in die Einrichtungskategorien stattfinden. Zu den besonders wichtigen Einrichtungen sollen alle Unternehmen zählen, die den Sektoren in Anlage 1 angehören und mehr als 250 Mitarbeiter oder über 50 Mio. EUR Jahresumsatz und über 43 Mio. EUR Bilanzsumme vorweisen können. Hingegen sollen zu den wichtigen Einrichtungen alle solche Unternehmen zählen, die den Sektoren in Anlage 1 und 2 angehören und über mehr als 50 Mitarbeiter oder über 10 Mio. EUR Jahresumsatz und Bilanzsumme verfügen. Eine Übersicht der in Anlage 1 und 2 genannten Sektoren im Folgenden:

Anlage 1	Anlage 2
Energie Stromversorgung, Fernwärme/ kälte, Kraftstoff, Heizöl, Gas	**Transport/Verkehr** Post und Kurier
Transport/Verkehr Luftverkehr Schienenverkehr, Schifffahrt, Straßenverkehr	**Entsorgung** Abfallbewirtschaftung
Finanz/Versicherungen Banken, generelle Finanzmarktinfrastruktur	**Chemie** Herstellung, Handel, Produktion
Wasserwirtschaft Trinkwasser, Abwasser	Lebensmittel Großhandel, Produktion, Verarbeitung
IT und Telekommunikation Internet Exchange Points, Domain Name Systems, TLD, Cloud Provider, Rechenzentrumsdienste, Content Delivery Networks, Trust Service Provider, elektronische Kommunikation und Dienste, Managed Services und Security Services	**Verarbeitendes Gewerbe** Medizin/Diagnostika, Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, Hersteller von elektronischen Erzeugnissen, Maschinenbau, Kfz/Teile, Fahrzeugbau
Weltraum Bodeninfrastrukturen	**Digitale Dienste** Marktplätze, Suchmaschinen, soziale Netzwerke
Gesundheit Dienstleistungen, Referenzlabore, Forschungs und Entwicklungsanbieter, Hersteller pharmazeutischer Erzeugnisse, Medizinprodukthersteller	**Forschung** Forschungseinrichtungen

Zu begrüßen ist, dass im Werkstattgespräch mit dem BMI hervorgehoben wurde, dass sich der Betrieb einer kritischen Anlage nicht auf sämtliche Teile eines Unternehmens auswirkt. Vorbehaltlich der Ressortabstimmung würde das bedeuten, dass die speziellen Anforderungen für kritische Anlagen nicht für das gesamte Unternehmen oder den gesamten Konzern gelten, mithin die übrigen Unternehmensteile nicht „infiziert" werden.

3. Änderung der Mindestanforderungen

In dem Diskussionspapier wurden zudem die Kriterien für die Auswahl der Mindestanforderungen konkretisiert. Wie auch schon im letzten Referentenentwurf festgelegt, muss bei der **Auswahl der Maßnahmen das Ausmaß der Risikoexposition, die Größe der Einrichtung, etwaige Umsetzungskosten, sowie die Eintrittswahrscheinlichkeit und die Schwere von Sicherheitsvorfällen** berücksichtigt werden. Geändert wurden hingegen die Anforderungen an die Sicherheit in der Lieferkette. Laut dem letzten Referentenentwurf mussten die Einrichtungen die bestehende Cybersicherheitspraxis ihrer Partner bei der Auswahl der Maßnahmen berücksichtigen und diese in die Entscheidung einfließen lassen. Zwar wurden diese Anforderung nunmehr im Gesetzestext gestrichen, finden sich allerdings in der Gesetzesbegründung wieder. Daher können sie künftig durch Auslegung mittelbar in den das Umsetzungsgesetz mit einfließen.

4. Pflichten & Haftung für Geschäftsleiter

Der Referentenentwurf aus dem Juli 2023 statuierte weitreichende Pflichten für die Geschäftsleiter betroffener Unternehmen. So hieß es in dem Entwurf, dass die Geschäftsleiter Risikomanagementmaßnahmen billigen und zusätzlich deren Umsetzung selbstständig überwachen müssen. Ein Delegieren der Überwachungstätigkeit an Dritte war laut dem Referentenentwurf nicht zulässig. Der Entwurf sah für die Verletzung der Überwachungspflicht eine persönliche Haftung der Geschäftsführer besonders wichtiger und wichtiger Einrichtungen vor.

Das Diskussionspapier aus dem September 2023 kippt diese Anforderungen nun wieder. Anders als in dem Entwurf aus dem Juli 2023 dürfen sich Geschäftsführer zukünftig eines Dritten bedienen, um die Umsetzung der Risikomanagementmaßnahmen zu überwachen. Auch die vorgesehene Klarstellung bezüglich der Geschäftsführerhaftung bei Unterlassung der Überwachungspflicht wurde aus dem Papier entfernt. Dies ändert jedoch nichts an der grundsätzlichen Haftung des Geschäftsführers gegenüber seiner Organisation, da seine Binnenhaftung auch weiterhin besteht. Entfernt wurde außerdem die Schulungspflicht für Mitarbeiter betroffener Einrichtungen, welche im letzten Referentenentwurf noch vorgesehen war. Die Schulungspflicht für Geschäftsleiter von besonders wichtigen und wichtigen Einrichtungen bleibt hingegen bestehen.

5. Erste Einordnung

Aus dem neuen Diskussionspapier gehen nochmals zahlreiche zum Teil tiefgreifende Veränderungen hervor. Einige Änderungen vereinfachen die Handhabe des neuen Gesetzes. Zugleich wurden aber auch einige Sicherheitsvorgaben maßgeblich entschärft. Ob die neuen Regelungen des Diskussionsentwurfes auch in Zukunft Bestand haben werden, wird sich in den nächsten Monaten zeigen. Die Lage bleibt dynamisch.
Es gilt nun abzuwarten, wie die Entwürfe tatsächlich umgesetzt werden. Diese Unsicherheit bringt viele Unternehmen zu Recht in eine Zwangslage. Denn eines ist klar: Von dem neuen Gesetz werden viele große und mittelständige Unternehmen betroffen sein und es braucht einige Vorlaufzeit, um die neuen Regelungen im Unternehmen umzusetzen. Daher ist es wichtig, sich zum jetzigen Zeitpunkt schon auf die neuen Regelungen einzustellen und Vorbereitungsmaßnahmen zu treffen.

6. Was Sie jetzt tun können

Sie sollten sich auf die Umsetzung der NIS-2 Richtlinie vorbereiten, da eine durchdachte Umsetzung **Qualitätseinbußen verhindert**, die **Resilienz** Ihres Unternehmens **stärkt** und eine **schnellere Eingliederung neuer Maßnahmen** in das Unternehmensumfeld **ermöglicht.** Ist die Lage so dynamisch wie bei der Umsetzung der NIS-2 Richtlinie, stellt sich die Frage, wie eine solche Vorbereitung aussehen kann. Um Ihnen die Antwort auf diese Frage zu erleichtern, haben wir Ihnen die wichtigsten Punkte einer guten Vorbereitung auf die Umsetzung der NIS- 2 Richtlinie zusammengefasst:

Betroffenheit klären
Zuallererst gilt es herauszufinden, ob Ihr Unternehmen in den Anwendungsbereich der neuen Regelungen fällt. Sie müssen nur dann Maßnahmen ergreifen, wenn Sie zu den betroffenen Einrichtungen gehören. Prüfen Sie, ob die Kriterien zur Einordnung auf Ihr Unternehmen oder bestimmte Anlagen Ihres Unternehmens zutreffen.

Ressourcen einplanen
Wenn Ihr Unternehmen oder Bereiche Ihres Unternehmens in den Anwendungsbereich der neuen Regelungen fallen, sollten Sie für die Umsetzung der Anpassungen Ressourcen einplanen. Dabei sollten einerseits Budgets festgelegt und andererseits personelle Ressourcen bereitgestellt werden.

Verantwortlichkeit klären
Für die Umsetzung der neuen Anforderungen sollten Verantwortliche bestimmt werden. Bestimmen Sie eine oder mehrere Personen, die für die Umsetzung der Regelung operativ als Hauptverantwortliche gelten. Suchen Sie Sich zudem frühzeitig kompetente externe Partner, die Sie bei der Umsetzung unterstützen.

Risikoanalyse
Nachdem die Verantwortlichkeiten geklärt wurden, sollte eine Risikoanalyse durchgeführt werden. Ermitteln Sie die größten Risiken Ihres Unternehmens und legen Sie dabei den Fokus auf Risiken, welche die Cybersicherheit Ihres Unternehmens betreffen.

Maßnahmen ermitteln
Die Risikoanalyse gibt Ihnen Hinweise auf die zu ergreifenden Maßnahmen. Der Referentenentwurf zum Umsetzungsgesetz der NIS-2 Richtlinie kann dazu eine Hilfestellung geben. Beachten Sie bei der Auswahl der Maßnahmen stets die persönliche Risikolage Ihres Unternehmens, insbesondere, dass die Geschäftskontinuität bestehen bleibt. Die Maßnahmen müssen fortlaufend auf ihre Wirksamkeit überprüft werden.

7. Fazit

Die Entwicklung rund um die Umsetzung der NIS-2 Richtlinie bleibt in Bewegung. Bis zur Umsetzung der neuen Richtlinie wird es wohl immer wieder neue Veränderungen geben, die Unternehmen die Planung zur Umsetzung erschwert. **Trotz dessen ist es wichtig, dass man frühzeitig beginnt, sich auf die neuen Regelungen vorzubereiten und die Betriebsstrukturen dementsprechend anzupassen.** Verlieren Sie in dieser Hinsicht keine Zeit, da eine frühzeitige Umsetzung Ihr Unternehmen resilienter macht.

Durch das Werkstattgespräch ist das Bemühen des Gesetzgebers deutlich geworden, die Schwellenwerte, Nachweis- sowie Meldefristen aus den Referentenentwürfen an die Übrigen IT-Sicherheitsgesetze anzupassen und eine Vereinheitlichung mit dem geplanten KRITIS- Dachgesetz und der EU-Verordnung „Digital Operational Resilience Act“ (DORA) zu erreichen. Eine solche **Harmonisierung zwischen den IT-Sicherheitsgesetzen** würde den betroffenen Unternehmen die Umsetzung der umfassenden Vorgaben zumindest ein wenig erleichtern und wäre daher zu begrüßen.

Ihre Ansprechpartner für alle Fragen rund um NIS-2 und Cybersicherheit:

Dirk Koch
Rechtsanwalt | Partner
CEHv11 – Certified Ethical Hacker
Data Protection Risk Manager CIPP/E
koch@byte.law

Olga Stepanova, LL.M. (Berkeley)
Rechtsanwältin | Partnerin
Fachanwältin für gewerblichen Rechtsschutz und für Informationstechnologierecht
stepanova@byte.law

bytelaw Rechtsanwälte
Bockenheimer Landstraße 51-53
60325 Frankfurt

T +49 (0) 69 - 1 53 91 91 90
M info@byte.law
I byte.law