NIS-2-Umsetzung in Deutschland – Was jetzt?

7. Februar 2025

Seit letzter Woche ist es offiziell: Die deutsche Umsetzung der Richtlinie (EU) 2022/2555 (sog. NIS-2-Richtlinie) zur Erhöhung der IT-Sicherheit in den EU-Mitgliedstaaten ist vorerst gescheitert. Dies führt dazu, dass viele zukünftig von NIS-2 betroffene Unternehmen weiterhin im Unklaren darüber sind, welche konkreten Maßnahmen sie in der Zukunft ergreifen müssen. Im Folgenden möchten wir etwas Orientierung dazu bieten:

Mindestanforderungen nach der NIS-2- Richtlinie

Am 16. Januar 2023 ist auf Europäischer Ebene die NIS-2-Richtlinie in Kraft getreten. Sie löste die Richtlinie (EU) 2016/1148 (sog. NIS-1-Richtlinie) ab. Im Zentrum der NIS-2-Richtlinie steht der Aufbau eines kohärenten Cybersicherheitssystems innerhalb der EU. Dabei sind im Vergleich zur NIS-1-Richtlinie deutlich mehr Einrichtungen und Unternehmen vom Anwendungsbereich der Richtlinie betroffen. Während die NIS-1-Richtlinie ca. 2000 Unternehmen erfasste, sollen nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) künftig bis zu 30.000 Organisationen unter die Richtlinie fallen. Neben den bereits von der NIS-1-Richtlinie abgedeckten Sektoren wie Energie, Verkehr und Gesundheitswesen umfasst die NIS-2-Richtlinie nun auch zusätzliche Bereiche wie digitale Dienste, Post- und Kurierdienste, Abwasser- und Abfallbewirtschaftung, Hersteller kritischer Produkte sowie die öffentliche Verwaltung. Auf die betroffenen Unternehmen, die in der Richtlinie in wesentliche und wichtige Einrichtung unterteilt werden, kommen deutlich umfassendere und spezifischere Cybersicherheitsmaßnahmen zu. Unter anderem:

- **Neue Mindestanforderungen an die Sicherheit von Netz- und Informationssystemen;**
- **Ausweitung der Berichtspflichten bei Cybersicherheitsvorfällen;**
- **Erhöhte Verantwortlichkeit der Geschäftsführung.**

Für Verstöße gegen die beschriebenen Mindestsicherheitsanforderungen und Berichtspflichten sollen nach Art. 34 NIS-2-Richtlinie abhängig von der Kritikalität der Einrichtung Höchststrafen von bis zu 2 % des weltweiten Jahresumsatzes vorgeschrieben werden.

Verspätete Umsetzung in Deutschland

Deutschland ist vorerst an einer fristgemäßen Umsetzung der NIS-2- Richtlinie gescheitert. Zwar hatte das Bundesinnenministerium im Sommer 2024 einen Entwurf für ein Umsetzungsgesetz (das NIS2UmsuCG) vorgelegt. Dieser Entwurf, der in einzelnen Punkten noch über die beschriebenen Mindestanforderungen von NIS-2 hinausging, hat nach dem Aus der Ampelregierung jedoch keine Mehrheit mehr im deutschen Bundestag gefunden. Für betroffene Einrichtungen und Unternehmen bleibt die Rechtslage dadurch vorerst unverändert: Denn ohne einen nationalen Umsetzungsakt begründet die Richtlinie selbst keine unmittelbaren Verpflichtungen

für Einzelne. Auch wenn der Europäische Gerichtshof in der Vergangenheit eine unmittelbare Wirkung von Richtlinien anerkannt hat, geschah dies ausschließlich zugunsten privater Parteien. Kurzum: Bußgelder durch die Nichtumsetzung der durch NIS-2-Richtlinie vorgeschriebene neuen Cybersicherheitsanforderungen drohen den von der Richtlinie erfassten Unternehmen derzeit nicht.

Anders sieht dies für die deutsche Bundesregierung aus, gegen die von der Europäischen Kommission ein Vertragsverletzungsverfahren wegen der verspäteten NIS-2-Umsetzung eingeleitet wurde. Schon deshalb und natürlich auch wegen des unbestreitbar hohen Handlungsbedarfs im Bereich der IT-Sicherheit, wird die zukünftige Bundesregierung die Umsetzung von NIS-2 deshalb zeitnah angehen müssen. Es ist allerdings noch offen, ob die zukünftige Regierung innerhalb ihres Umsetzungsspielraums auf den bereits vorhandenen Entwurf aufbauen wird. So warb die CDU/CSU-Fraktion, die voraussichtlich Teil der neuen Bundesregierung sein wird, bislang für eine 1:1 Umsetzung der NIS-2-Richtlinie in deutsches Recht und hatte sich gegen den bisherigen (darüber stellenweise hinausgehenden) Entwurf zur NIS-2 Umsetzung positioniert.

Handlungsempfehlung für zukünftig von der NIS-2 betroffene Einrichtungen und Unternehmen

Angesichts der weiterhin absehbaren Gesetzesänderungen im deutschen IT-Sicherheitsrecht sollten sich Unternehmen zumindest in Bezug auf die Mindestvorgaben der NIS-2-Richtlinie frühzeitig vorbereiten. Als Ausgangspunkt dafür kann eine vom BSI bereitgestellte NIS-2-Betroffenheitsprüfung herangezogen werden, mit der vorgeprüft werden kann, ob das eigene Unternehmen in den Anwendungsbereich der Richtlinie fällt und welche Pflichten es zukünftig beachten muss. Durch die verspätete Umsetzung in Deutschland bleibt jetzt aber insgesamt noch etwas Zeit für damit verbundene unternehmensinterne Anpassungen.

BLOMSTEIN wird die weiteren Entwicklungen bei der NIS-2-Umsetzung aufmerksam verfolgen. Wenden Sie sich bei Fragen zum Umgang mit den Entwicklungen im deutschen IT-Sicherheitsrecht jederzeit gerne an Christopher Wolters, Leonard von Rummel und Moritz Schuchert.

***