Anlage zur PARITÄTISCHEN Fachinformation vom 26. Juli 2024 (Regierungsentwurf für NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz beschlossen)

Wer muss für mehr Cybersicherheit sorgen?

Die europäische NIS2-Richtlinie (NIS2-RL) für mehr Cybersicherheit in der Europäischen Union (abrufbar hier) muss bis 17. Oktober 2024 in deutsches Recht umgesetzt werden. Die Bundesregierung hat nun einen entsprechenden Gesetzesentwurf für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2-UmsuCG) verabschiedet (abrufbar hier).

Alle Unternehmen, einschließlich sozialer Träger, haben die Möglichkeit, auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu prüfen, ob sie von den anstehenden Änderungen betroffen sind (Zugang hier).

Nachstehend werden zudem zum besseren Verständnis und als zusätzliche Hilfestellung einige Grundregeln des Anwendungsbereiches erläutert. Es handelt sich aber keinesfalls um eine abschließende Aufzählung aller in Betracht kommender Anwendungsfälle und kann keine Prüfung im Einzelfall ersetzen.

Der aktuelle Entwurf für ein NIS2UmsuCG regelt in § 28 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik neu (BSIG-neu) u.a., welche natürlichen und juristischen Personen des Privatrechts von den anstehenden Änderungen betroffen sind. Dazu zählen die besonders wichtigen Einrichtungen (der Begriff entspricht dem der „wesentlichen Einrichtungen“ aus der NIS2-RL) und die wichtigen Einrichtungen.

I. Besonders wichtige Einrichtungen

Als besonders wichtige Einrichtung gelten nach § 28 Abs. 1 BSIG-neu (neben anderen)

- Betreiber kritischer Anlagen
- sowie sonstige natürliche oder juristische Personen [...], die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind, sofern sie mindestens 250 Mitarbeiter beschäftigen oder einen Jahresumsatz von über 50

Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

1. *Betreiber kritischer Anlagen*

Der Begriff des Betreibers kritischer Anlage richtet sich nach § 28 Abs. 6 und 7 BSIG-neu i.V.m. der Rechtsverordnung nach § 58 Absatz 4 BSIG (abrufbar hier). Hierunter kann u. a. (in Abhängigkeit von Stichtagregelung und Schwellenwert) im Gesundheitsbereich die stationäre medizinische Versorgung fallen, also z. B. Krankenhäuser mit einer entsprechenden Größe.

2. *Sonstige natürliche oder juristische Personen des Privatrechts*

Darüber hinaus fallen private Unternehmen unabhängig von ihrer Rechtsform nur unter die gesetzlichen Regelungen, wenn sie den in Anhang 1 BSIG-neu genannten Sektoren zuzuordnen sind und die genannten Schwellenwerte erreichen.

a) Sektoren des Anlage 1

Anlage 1 des BSIG-neu nennt folgende Sektoren:

- Energie
- Transport (Luft-, Schienen-, Straßen- und Wasserverkehr)
- Finanzwesen (Bankwesen und Finanzmarktinfrastruktur)
- Gesundheitswesen
- Trinkwasserversorgung (unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist)
- Abwasserbeseitigung
- Digitale Infrastruktur und Verwaltung von IKT- Diensten (Business-to-Business)
- Weltraum

Die genauere Betrachtung der Anlage 1 des BSIG-neu zeigt, dass soziale Träger zum allergrößten Teil nicht den genannten Sektoren unterfallen, da es hier in der Regel um Leistungen geht, die der Öffentlichkeit zur Verfügung gestellt werden, also um echte Infrastrukturleistungen. Gleichwohl ist eine Betroffenheit denkbar, etwa in den Bereichen Energie und Gesundheitswesen.

aa) Energie

Einer genaueren Prüfung sollte es etwa unterzogen werden, wenn z. B. eine Pflegeeinrichtung eine eigene Energiegewinnungsanlage betreibt, etwa ein Blockkraftwerk, und die überschüssige, nicht selbst verbrauchte Energie in das allgemeine Stromnetz einspeist und damit der Öffentlichkeit zur Verfügung stellt.

bb) Gesundheitswesen

Der Sektor, der offensichtlich für den sozialen Bereich relevant werden kann, ist das Gesundheitswesen.

Nach Pkt. 4.1.1 des Anhang 1 des BSIG-neu fallen hierunter u. a. Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie (EU) 2011/24 (abrufbar hier). Nach Artikel 3g) dieser Richtlinie sind „Gesundheitsdienstleister" jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines europäischen Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt. Gesundheitsdienstleistungen sind nach Artikel 3a) der Richtlinie Gesundheitsdienstleistungen, die von Angehörigen der Gesundheitsberufe gegenüber Patienten erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten. Nach Artikel 3f) der Richtlinie sind „Angehörige der Gesundheitsberufe": Ärzte, Krankenpfleger für allgemeine Pflege, Zahnärzte, Hebammen und Apotheker im Sinne der Richtlinie 2005/36/EG (abrufbar hier) oder andere Fachkräfte, die im Gesundheitsbereich Tätigkeiten ausüben, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1a) der Richtlinie 2005/36/EG vorbehalten sind, oder Personen, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gelten.

In Deutschland gehören zu den anerkannten Heilberufen und damit zu den Gesundheitsberufen z. B. Logopäden, Psychotherapeuten, Physiotherapeuten, Diätassistenten, Notfallsanitäter, Podologen und Pflegefachkräfte etc.:

https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/gesundheitsberufe/gesundheitsberufe-allgemein; jedenfalls in NRW auch Ergotherapeuten: https://www.mags.nrw/berufsbilder-von-a-bis-z.

Damit können eine Reihe von sozialen Trägern grundsätzlich dem Gesundheitswesen zugeordnet sein, so etwa Reha-Einrichtungen, Interdisziplinäre Frühförderzentren, Anbieter von Kurzzeitpflege und natürlich Krankenhäuser, wenn diese nicht ohnehin bereits als Betreiber kritischer Anlagen zu den besonders wichtigen Einrichtungen gehören, s.o.

Ausnahme: Langzeitpflege

Zu den Heilberufen in Deutschland gehören zwar auch Pflegefachkräfte, s. o. **Nach der Begründung des Gesetzesentwurfs für ein NIS2UmsuCG sind Einrichtungen der Langzeitpflege aber ausdrücklich keine Gesundheitsdienstleister im Sinne des BSIG-neu** (dort S. 197, Zu Anlage 1 des BSIG-neu).

Die Ausnahme erfolgt unter Bezugnahme auf Anhang I der NIS2-RL i.V.m. Artikel 3a) der Richtlinie (EU) 2011/24 (s.o.), in deren Anwendungsbereich Einrichtungen der Langzeitpflege ausdrücklich nicht fallen. Erwägungsgrund 14 der Richtlinie (EU) 2011/24 gibt Aufschluss, was mit Langzeitpflege gemeint ist. Zudem wirft er die Frage auf, ob noch weitere, der Langzeitpflege gleichwertige soziale Angebote vom NIS2-UmsuCG ausgenommen sein könnten. Erwägungsgrund 14 lautet:

„Diese Richtlinie sollte nicht für Dienstleistungen gelten, deren primäres Ziel darin besteht, Personen zu unterstützen, die auf Hilfe bei routinemäßigen alltäglichen Verrichtungen angewiesen sind. Diese Richtlinie sollte insbesondere nicht für jene Dienstleistungen der Langzeitpflege gelten, die als notwendig erachtet werden, um dem Pflegebedürftigen ein möglichst erfülltes und selbst bestimmtes Leben zu ermöglichen. Deshalb sollte diese Richtlinie beispielsweise nicht für Dienstleistungen der Langzeitpflege gelten, die von häuslichen Pflegediensten, im Rahmen von betreuten Wohnformen und in Wohnheimen oder -stätten („Pflegeheimen“) erbracht werden.“

Jedenfalls Leistungen der Langzeitpflege in diesem Sinne unterliegen damit keinen erhöhten Anforderungen an Cybersicherheit nach dem BSIG-neu.

b) Schwellenwerte

Wenn eine Organisation einem der genannten Sektoren zuzuordnen ist, ist sie aber nur dann eine besonders wichtige Einrichtung, wenn sie zudem mindestens 250 Mitarbeiter beschäftigt oder einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweist.

II. Wichtige Einrichtungen

Als wichtige Einrichtungen gelten nach § 28 Abs. 2 Nr. 3 BSIG-neu – was auch für soziale Träger relevant sein könnte – u. a.:

- natürliche oder juristische Personen des Privatrechts, die anderen Personen entgeltlich Waren oder Dienstleistungen anbieten,
- die einem Sektor der Anlagen 1 und 2 des BSIG zuzuordnen sind
- und die folgenden Schwellenwerte erreichen:
    - mindestens 50 Mitarbeiter beschäftigen oder
    - einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

Die wichtigen Einrichtungen müssen daher entweder einer der bereits o. g. Sektoren der Anlage 1 des BSIG-neu zuzuordnen sein. Hier kommt – wie schon bei den besonders wichtigen Einrichtungen – insbesondere der Gesundheitsbereich in Betracht, so dass z.B. die erwähnten Einrichtungstypen wie Reha-Einrichtungen, Interdisziplinäre Frühförderzentren, Krankenhäuser und Kurzzeitpflege (nicht aber Langzeitpflege) betroffen sein können.

Oder die wichtigen Einrichtungen sind einer der in der Anlage 2 des BSIG-neu genannten Sektoren zuzuordnen. Diese sind:

- Transport und Verkehr
  (Post- und Kurierdienste)

- Abfallbewirtschaftung
  (Unternehmen nach § 3 Abs. 14 KrWG, deren Hauptwirtschaftstätigkeit Abfallbewirtschaftung ist)
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
  (Lebensmittelunternehmen, die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind)
- Verarbeitendes Gewerbe/Herstellung von Waren
  (Herstellung von Medizinprodukten und In-vitro-Diagnostika, Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, Herstellung von elektrischen Ausrüstungen, Maschinenbau und Herstellung von Kraftwagen und Kraftwagenteilen)
- Anbieter digitaler Dienste
  (Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke)
- Forschungseinrichtungen

Auch die hier genannten Sektoren werden wohl überwiegend keine Rolle für soziale Einrichtungen spielen. Allerdings muss dies im Einzelfall geprüft werden. Etwa sollten Werkstätten für Menschen mit Behinderung prüfen, ob sie im Einzelfall nicht ausnahmsweise die Kriterien z.B. für ein „verarbeitendes Gewerbe“ oder ein „Lebensmittelunternehmen“ im o. g. Sinne erfüllen.

III. Auf welche wirtschaftliche Einheit ist bei den Schwellenwerten abzustellen?

Zu fragen ist ferner, auf welche wirtschaftliche Einheit es bei der Prüfung der Schwellenwerte ankommt. In Betracht kommt hier entweder die konkrete Einrichtung, deren Geschäftstätigkeit in einen der maßgeblichen Sektoren des BSIG-neu fällt. Also z. B. das einzelne Interdisziplinäre Frühförderzentrum oder der einzelne ambulante Dienst. Die zweite Möglichkeit ist, dass die Geschäftszahlen des gesamten Rechtsträgers zu berücksichtigen sind, also etwa des gesamten Vereins, der außer dem Interdisziplinären Frühförderzentrum noch weitere Einrichtungen (z.B. Wohnheime) betreibt, deren Tätigkeitsbereich nicht den maßgeblichen Sektoren zuzuordnen ist. Die dritte Möglichkeit ist, dass darüber hinaus noch die Geschäftszahlen von verbundenen und Partnerunternehmen einzubeziehen sind, welche (im Rahmen einer Konzernstruktur) Anteile an dem betreffenden Unternehmen in einer gewissen Größenordnung halten oder über dieses eine beherrschende Stellung ausüben, z.B. durch Stimmrechte in dessen Entscheidungsgremien, z. B. der Mitgliederversammlung.

§ 28 Abs. 3 BSIG-neu stellt klar, dass nur auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen ist. Nach der Begründung des Gesetzesentwurfs (dort S.

156) sind daher nur die Geschäftszahlen „der*jenigen Teile der Einrichtung einzubeziehen […], die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind. Querschnittsaufgaben wie beispielsweise Personal, Buchhaltung etc. sind lediglich anteilig zu berücksichtigen.*“ Im genannten Beispiel, in dem ein Verein neben einem Interdisziplinären Frühförderzentrum noch andere Einrichtungen mit anderen Tätigkeitsbereichen betreibt, die nicht den maßgeblichen Sektoren unterfallen, käme es also bei der Prüfung der Schwellenwerte nur auf die Geschäftszahlen des Interdisziplinären Frühförderzentrums an, nicht auf die Geschäftszahlen des Vereins insgesamt, wobei Zahlen des Overheads anteilig berücksichtigt würden.

Ferner sind nach § 28 Abs. 3 BSIG-neu die Daten von Partnerunternehmen oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG (dort Artikel 3 Absatz 2 und 3, abrufbar hier) bei der Schwellenprüfung außer Acht zu lassen, wenn das betroffene Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, die es für die Erbringung seiner Dienste nutzt, unabhängig von seinen Partner- oder verbundenen Unternehmen ist. Das bedeutet nach der Begründung (S. 156 f.), dass es nur auf die Geschäftszahlen des betroffenen Unternehmens ankommt, vorausgesetzt, dass es die grundsätzlichen Entscheidungen zur Beschaffung, zum Betrieb und zur Konfiguration der informationstechnischen Systeme, Komponenten und Prozesse eigenverantwortlich trifft.

IV. Wer ist in der Pflicht?

Entsprechend des zuvor Gesagten wird sich auch die Verpflichtung, die Vorgaben für eine erhöhte Cybersicherheit einzuhalten, auf die Einrichtung beschränken, deren Daten bei der Prüfung der Schwellenwerte zugrunde zu legen sind. Verpflichtet wird also die wirtschaftliche Einheit, die den bestimmenden Einfluss auf die eigenen informationstechnischen Systeme, Komponenten und Prozesse ausübt und somit die Macht hat, die relevanten Cyberangriffe abzuwehren. Dabei trifft die Verantwortung, die neuen Verpflichtungen einzuhalten, das Management, also Geschäftsführer und Vorstände, was zu einer Ausweitung der Managerhaftung führt.

Berlin, 26. Juli 2024
Anuschka Novakovic, LL. M. - Syndikusrechtsanwältin