Vorschlag für ein Konzept zur Identifizierung von Einrichtungen i. S. d. Art. 2 Abs. 2 f) ii) NIS-2-RL

Nachfolgend wird ein gemeinsamer Vorschlag für ein Konzept zur Identifizierung von Stellen der Landesverwaltung für die Zwecke der Umsetzung von Art. 2 Abs. 2 f) ii) NIS-2-RL vorgestellt.

Ausgangspunkt für die Entwicklung des Identifizierungskonzepts ist Art. 2 Abs. 2 f) ii) NIS-2-RL. Dieser erfordert ein risikobasiertes Identifizierungskonzept, das Dienste der öffentlichen Verwaltung auf regionaler Ebene ermittelt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte. Demnach erfordert Art. 2 Abs. 2 f) ii) NIS-2-RL ein dreistufiges Vorgehen:

- Im ersten Schritt muss der Begriff des Dienstes einer Einrichtung der öffentlichen Verwaltung auf regionaler Ebene definiert werden (nachfolgend auch „**Dienst**“).
- Im zweiten Schritt gilt es, solche Einrichtungen zu identifizieren, eine kritische gesellschaftliche Tätigkeit ausüben oder deren Dienste einen Bezug zu kritischen wirtschaftlichen Tätigkeiten haben.
- Im dritten Schritt müssen Einrichtungen identifiziert werden, bei denen die Störung eines Dienstes bei einer risikobasierten Betrachtung erhebliche Auswirkungen auf kritische wirtschaftliche Tätigkeiten hat (nachfolgend „**kritische Dienste**“). Diese unterfallen dann dem Anwendungsbereich der NIS-2-RL.

Neben diesen aus dem Wortlaut der Richtlinie ableitbaren Prüfungsschritten sind nachgelagert bei der Anwendung des Identifizierungskonzepts drei Durchführungsziele zu berücksichtigen:

- Erstens sollte eine wirtschaftliche und möglichst unbürokratische Anwendung des Identifizierungskonzepts gewährleistet sein.
- Zweitens sollten möglichst alle Behörden in der Landesverwaltung identifiziert werden, die wenigstens einen kritischen Dienst erbringen.
- Drittens soll ein möglichst bundeseinheitliches Identifizierungsergebnis erreicht werden.

Nachfolgend ist zwischen zwei Ebenen zu unterscheiden: Zuerst ist – entsprechend des oben skizzierten dreistufigen Prüfprogramms – ein Identifizierungskonzept zu entwickeln, das den Anforderungen des Art. 2 Abs. 2 f) ii) NIS-2-RL gerecht wird (I.). Anschließend stellt sich die Frage der Anwendung des Identifizierungskonzepts. Hierzu wird ein Vorschlag gemacht, der den drei vorgenannten Durchführungszielen im weitest möglichen Umfang Rechnung trägt (II.).

I. Identifizierungskonzept

Nachfolgend wird entsprechend den Vorgaben des Art. 2 Abs. 2 f) ii) NIS-2-RL dreistufig vorgegangen: Im ersten Schritt wird der Begriff des Dienstes der öffentlichen Verwaltung auf regionaler Ebene definiert. Im zweiten Schritt werden Dienste identifiziert, die eine kritische gesellschaftliche Tätigkeit darstellen oder einen Bezug zu kritischen wirtschaftlichen Tätigkeiten aufweisen. Im dritten Schritt

ist eine risikobasierte Bewertung dieser Dienste mit Bezug zu kritischen wirtschaftlichen Tätigkeiten durchzuführen, um kritische Dienste zu identifizieren.

1. Schritt: Definition des „Dienstes einer Einrichtung der öffentlichen Verwaltung auf regionaler Ebene“

Für die nähere Bestimmung des „Dienstes einer Einrichtung der öffentlichen Verwaltung auf regionaler Ebene“ sind dessen Tatbestandsmerkmale näher zu betrachten:

(1) regionale Ebene,

(2) Einrichtung der öffentlichen Verwaltung und

(3) Dienst.

Mit der regionalen Ebene ist die jeweilige Landesverwaltung gemeint. Welche Einrichtungen hierunter fallen, ist in Abgrenzung zu den Einrichtungen der Zentralregierung (Bundesverwaltung, Art. 2 Abs. 2 f) i) NIS-2-RL) und Einrichtungen der lokalen Ebene (Kommunalverwaltung, Art. 2 Abs. 5 a) NIS-2-RL) zu bestimmen. Jede Einrichtung der öffentlichen Verwaltung, die nicht entweder der Zentralregierung oder der lokalen Ebene zuzuordnen ist, fällt unter die regionale Ebene. Die Abgrenzung ist insbesondere zur Kommunalverwaltung diffizil. Hier bietet es sich an, unter Berücksichtigung von Art. 4 Abs. 2 Satz 1 EUV, auf das kommunale Selbstverwaltungsrecht (Art. 28 Abs. 2 GG) als Abgrenzungskriterium abzustellen. Dadurch sind beispielsweise die Kreisverwaltungsbehörden/ Landratsämter in BY und BW aufgrund der Organisationshoheit des Landrats nicht der „regionalen Ebene“, sondern der „lokalen Ebene“ zuzuordnen.

Einrichtungen der öffentlichen Verwaltung sind alle öffentlichen Einrichtungen der Landesverwaltung, welche die in Art. 6 Nr. 35 lit. a) – d) NIS-2-RL genannten Kriterien erfüllen. Erforderlich ist insbesondere, dass die jeweilige Einrichtung befugt ist, an natürliche oder juristische Personen Verwaltungs- oder Regulierungsentscheidungen zu richten (Art. 6 Nr. 35 lit. d) NIS-2-RL). Entscheidend ist hierbei die theoretische Möglichkeit hierzu, weshalb grundsätzlich alle Behörden i. S. d. § 1 Abs. 4 VwVfG unter den Begriff fallen. Ausgenommen sind diejenigen Einrichtungen, die in Art. 6 Abs. 35, Art. 2 Abs. 7 und 8 NIS-2-RL genannt sind (z. B. Justiz, Verteidigung, Öffentliche Sicherheit, Strafverfolgung, Parlamente und Zentralbanken). Für Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Eigenbetriebe, die einer wirtschaftlichen Tätigkeit nachgehen, bestimmt sich der Anwendungsbereich über die „Size-cap-rule“ und Sektorenangehörigkeit i. S. d. Art. 2 Abs. 1 NIS-2-RL. Diese Einrichtungen sollen nach Rechtsauffassung des BMI in den Anwendungsbereich des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes fallen und über das BSIG reguliert werden.

Der Begriff des Dienstes ist dem Zweck des Art. 2 Abs. 2 f) ii) NIS-2-RL nach weit zu verstehen. Demnach fällt hierunter jeder Vorgang innerhalb der vorgenannten Einrichtungen, durch den öffentliche Aufgaben erfüllt werden. Erfasst sind damit Verwaltungsleistungen gegenüber Dritten (z. B. Verwaltungsakte, Datenbereitstellung, Vollzug von Meldepflichten) sowie verwaltungsinterne Dienstleistungen (z. B. zentrale IT-Dienstleister).

Schritt 2: Identifizierung von kritischen gesellschaftlichen und wirtschaftlichen Tätigkeiten

Der Wortlaut des Art. 2 Abs. 2 f) ii) NIS-2-RL unterscheidet klar zwischen kritischen gesellschaftlichen und wirtschaftlichen Tätigkeiten. Insoweit sind innerhalb der von der NIS-2-RL erfassten Einrichtungen der Landesverwaltung anschließend diejenigen Dienste (z. B. Verwaltungsleistungen) zu

ermitteln, die eine kritische gesellschaftliche Tätigkeit darstellen oder einen Bezug zu kritischen wirtschaftlichen Tätigkeiten aufweisen.

Kritische gesellschaftliche Tätigkeiten sind die für die Aufrechterhaltung der Staats- und Regierungsfunktionen notwendigen Dienste der Verwaltung. In diesen Fällen ist der Dienst selbst die kritische Tätigkeit. Daher ist für diese Dienste die Identifizierung des jeweiligen Bezugs und die Risikobetrachtung (3. Schritt) bereits berücksichtigt, denn eine Störung des Dienstes hat stets das Potential, die kritische (gesellschaftliche) Tätigkeit – die ja im Erbringen des Dienstes selbst besteht – erheblich zu beeinträchtigen. Solche kritischen gesellschaftlichen Dienste sind insbesondere:

- Regierungsleitende Tätigkeiten (Oberste Landesbehörden),
- Leistungen der staatlichen IT-Dienstleister,
- sowie Dienste, die von nach Landesrecht identifizierten Einrichtungen erbracht werden. Anhaltspunkte können sich z. B. aus § 1 Abs. 4 Nds. SÜG oder einer vergleichbaren landesrechtlichen Regelung ergeben.

Hinsichtlich kritischer wirtschaftlicher Tätigkeiten ist der Bezug weit zu verstehen: Ausreichend ist es, wenn ein thematischer Bezug vorliegt. Ein solcher besteht, wenn zwischen der Störung des Dienstes auf staatlicher Seite und einer Störung bei einer kritischen wirtschaftlichen Tätigkeit eine objektive Kausalität erkennbar ist. Unerheblich ist an dieser Stelle dagegen, wie erheblich die Auswirkungen sind (diese Frage wird erst im nächsten Prüfungsschritt beantwortet).

Eine objektive Kausalität ist gegeben, wenn ein Dienst zwingend erforderlich ist, damit eine kritische wirtschaftliche Tätigkeit ausgeführt werden kann oder darf. Beispielsweise kann für die Tierschlachtung eine Genehmigung erforderlich sein. Sollte diese ausbleiben, könnten unter Umständen landesweit keine Schlachtungen mehr erfolgen. Im Gegensatz dazu dürfte die Messung von Pegelständen von Flüssen keinen Bezug zur Trinkwasserversorgung aufweisen, solange hierdurch die Entnahme von Wasser nicht direkt eingeschränkt wird.

Neben Diensten, die einen unmittelbaren Bezug zu kritischen wirtschaftlichen Tätigkeiten aufweisen (z. B. eine kritische wirtschaftliche Tätigkeit darf ohne hoheitliche Kontrolle nicht ausgeführt werden, ggf. Lebensmittelüberwachung, Kernreaktorfernüberwachung, …), existieren auch verwaltungsinterne Dienste mit einem mittelbaren Bezug zu kritischen wirtschaftlichen Tätigkeiten. Ein solcher mittelbarer Bezug liegt vor, wenn der Dienst notwendig ist, damit ein anderer kritischer Dienst[1] in

[1] Ein anderer Dienst mit unmittelbarem oder mittelbarem Bezug zu einer kritischen Tätigkeit, der bei einer risikobasierten Betrachtung erhebliche Auswirkungen auf eine kritische Tätigkeit hat.

seiner Funktion nicht eingeschränkt ist. Dieser verwaltungsinterne Dienst kann auch von einer anderen Behörde (insbesondere zentraler IT-Dienstleister) erbracht werden. Typischerweise handelt es sich hier um zentral für mehrere Behörden wahrgenommene Fachaufgaben.

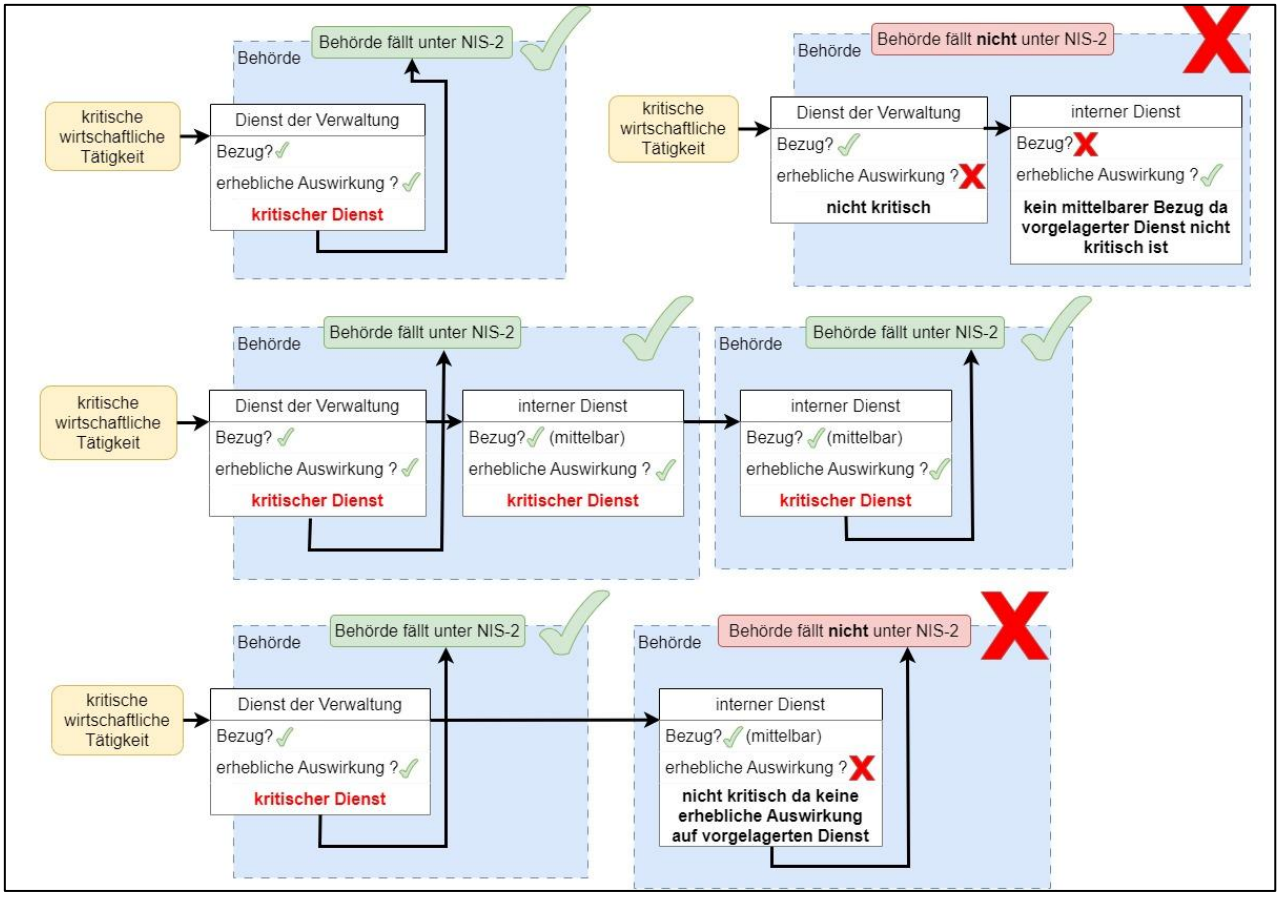

Abbildung 1 Veranschaulichung mittelbare und unmittelbare Bezüge

Zusammenfassend kann ein Bezug zu kritischen wirtschaftlichen Tätigkeiten somit beispielsweise vorliegen aufgrund von:

- Erlass von Verwaltungsakten, z. B. weil kritische Tätigkeiten nicht rechtskonform ausgeübt werden können, weil eine Genehmigung fehlt.
- Bereitstellung von Informationen, z. B. Bereitstellung von Geodaten.
- Entgegennahme von Meldungen, weil z. B. erhebliche Arbeitsrückstände bei einer kritischen wirtschaftlichen Tätigkeit drohen, wenn Meldeverfahren länger ausfallen.
- (Zentrale) Wahrnehmung von Fachaufgaben, wie Clientbetreuung, Fachverfahrensbetrieb, Laborleistungen usw.

Für die Identifizierung kritischer wirtschaftlicher Tätigkeiten bietet sich eine Orientierung am Begriff der Kritischen Infrastruktur nach § 2 Abs. 10 BSIG an[2]. Hierzu gehören insb. die in § 2 Abs. 10 Nr. 1 BSIG in der Fassung vom 23.6.2021 genannten Sektoren. Kritische wirtschaftliche Tätigkeiten sind demnach alle Tätigkeiten in den genannten Sektoren, die von hoher Bedeutung für das Funktionie-

[2] Entsprechend der Vorstellung des Entwurfs des NIS2UmsuCG des BMI in der Sitzung der LAG Cybersicherheit am 7.7.2023 zukünftig „Kritische Anlage“

ren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Ob der Dienst einer Einrichtung einen Bezug zu diesen Tätigkeiten hat, wird sich häufig bereits aus dem Fachrecht ergeben.

Im Fall des Bayerischen Landesamtes für Umwelt nach Art. 1 LfUG beispielsweise:

> ***Art. 1***
> ***Landesamt für Umwelt***
> *(1) Es besteht ein Landesamt für Umwelt mit Sitz in Augsburg.*
> *(2) [1]Nach Maßgabe gesonderter Vorschriften erfüllt es landesweit Fach- und Vollzugsaufgaben insbesondere*
>
> > *[…]*
> >
> > *3. der Abfallentsorgung,*
> >
> > *4. des Immissionsschutzes, insbesondere des Schutzes der Allgemeinheit vor Luftverunreinigungen, Lärm, Erschütterungen, der Gefahren der Kernenergie und vor ionisierender und nicht ionisierender Strahlung,*
> >
> > *5. der Wasserversorgung, des Gewässerschutzes und der Gewässerkunde einschließlich des Hochwassernachrichten- und Lawinenwarndienstes, […].*

3. Schritt: Risikobasierte Bewertung bei kritischen wirtschaftlichen Tätigkeiten

Im dritten Prüfungsschritt sind sodann die kritischen Dienste in der Landesverwaltung zu ermitteln. Das sind diejenigen Dienste, deren Störung bei einer risikobasierten Betrachtung erhebliche Auswirkungen auf kritische wirtschaftliche Tätigkeiten haben können. Dieser Prüfungsschritt ist nur für Einrichtungen durchzuführen, deren Dienste einen Bezug zu kritischen wirtschaftlichen Tätigkeiten haben (s.o.). Risiko ist grundsätzlich zu verstehen als das Multiplikationsergebnis von erwarteter Schadenshöhe und Eintrittswahrscheinlichkeit (so auch BSI-Standard 200-4, S. 205). Die NIS-2-Richtlinie fordert hingegen nur eine risikobasierte Bewertung. Daher soll die Eintrittswahrscheinlichkeit zunächst nicht herangezogen werden.

An dieser Stelle ist es wichtig zu betonen, dass der zu betrachtende Schaden in der risikobasierten Bewertung die Auswirkung einer Störung des jeweiligen Dienstes auf die jeweilige kritische wirtschaftliche Tätigkeit ist und zwar unabhängig von der Ursache dieser Störung. Sofern bei einem Dienst eine Störung gleichwelcher Art eine erhebliche Auswirkung auf eine kritische wirtschaftliche Tätigkeit hat, handelt es sich um einen kritischen Dienst.

Außer Betracht bleibt daher insbesondere das Risiko einer Störung der Netz- und Informationssysteme des jeweiligen Dienstes und die Frage, in welcher Weise eine solche Störung die Erbringung der Dienste beeinträchtigen könnte. Das ist für die Eröffnung des Anwendungsbereichs der NIS-2-RL erst einmal ohne Belang; hier ist nur von Bedeutung, ob der Dienst an sich als kritisch einzustufen ist. Das zeigt zum einen ein Vergleich mit den in Art. 2 Abs. 1, 2 lit. a) – e) NIS-2-RL genannten Einrichtungen. Diese fallen unabhängig von der Frage nach ihrer Anfälligkeit für Störungen ihrer IT-Systeme, sondern allein aufgrund ihrer allgemeinen Kritikalität in den Anwendungsbereich der Richtlinie. Zum anderen ist zu beachten, dass die Risiken, die für den jeweiligen Dienst aufgrund einer Störung der Netz- und Informationssysteme ausgehen, im Rahmen der Risikomanagementmaßnahmen nach Art. 21 NIS-2-RL betrachtet werden. Diese Prüfung sollte nicht in die Frage der Anwendbarkeit der NIS-2-RL vorverlagert werden. Dafür spricht letztlich auch, dass andernfalls eigentlich

kritische Dienste, die derzeit weniger auf IT-Systeme angewiesen sind, aus dem Anwendungsbereich fallen würden. Das birgt die Gefahr, dass diese zukünftig unbeachtet bleiben, auch wenn sich ihre IT-Abhängigkeit steigert.

Zentral ist die Frage nach dem Schadenspotential, d. h. der Auswirkung, die eine Störung des jeweiligen Dienstes auf die kritische wirtschaftliche Tätigkeit haben könnte[3]. Die NIS-2-RL fordert an dieser Stelle, dass der Schaden bzw. die Auswirkung „erheblich" ist. Um die Erheblichkeit einer Auswirkung zu bewerten, bietet es sich an, eine Business-Impact-Analyse (BIA) durchzuführen. Dies könnte z. B. entsprechend des Auswertungsbogens des BSI zum Standard 200-4 erfolgen[4]. Daraus ergeben sich die folgenden Schadenskategorien:

Auswirkung	**Beschreibung** *Betrachtete Schadenszenarien: Die Beeinträchtigung der Durchführung der kritischen Tätigkeit, Verstöße gegen Gesetze, Vorschriften und Verträge, Ansehensbeeinträchtigungen, finanzielle Schäden, Beeinträchtigungen der persönlichen Unversehrtheit Einzelner (körperliche Unversehrtheit und Persönlichkeitsrechte).*
vernachlässigbar	Die Störung hat geringe, kaum spürbare Auswirkungen auf die kritische Tätigkeit: Die Durchführung der kritischen Tätigkeit wird unwesentlich beeinträchtigt. Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten. Der finanzielle Schaden ist unerheblich. Eine Beeinträchtigung der persönlichen Unversehrtheit Einzelner ist ausgeschlossen.
begrenzt	Die Störung hat spürbare Auswirkungen auf die kritische Tätigkeit: Die Störung hat spürbare Auswirkungen auf die Durchführung der kritischen Tätigkeit; mit Arbeitsrückständen ist zu rechnen. Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen. Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. Der finanzielle Schaden ist tolerabel. Eine Beeinträchtigung Einzelner ist unwahrscheinlich.
beträchtlich	Die Störung hat nicht tolerierbare Auswirkungen auf die kritische Tätigkeit: Die Durchführung der kritischen Tätigkeit ist massiv eingeschränkt; Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren. Es wird gegen Gesetze verstoßen. Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten. Der finanzielle Schaden ist erheblich und nachhaltig. Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
existenzbedrohend	Die Störung führt zu existentiell bedrohlichen Auswirkungen für die kritische Tätigkeit: Die Störung hat fundamentale und langfristige Auswirkungen auf die kritische Tätigkeit; Arbeitsrückstände können nicht mehr aufgeholt werden. Es wird im hohen Maß gegen Gesetze verstoßen, sodass erhebliche Konsequenzen drohen, z. B. strafrechtlicher Art oder Bußgelder. Eine fundamentale, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. Der finanzielle Schaden hat existenzbedrohende Ausmaße. Es besteht akute Gefahr für Leib und Leben oder gravierende Beeinträchtigungen von Persönlichkeitsrechten Einzelner.

Dabei sollten Auswirkungen einer Störung des Dienstes nicht beachtet werden, die allein durch Erlass von Verordnungen oder Verwaltungsvorschriften durch die zuständige oberste Landesbehörde beseitigt oder reduziert werden könnten. Dadurch wird vermieden, dass Dienste aufgenommen werden, bei denen die Auswirkung in einem „bloßen Rechtsverstoß" besteht, obwohl diese Auswirkung z. B. durch Senkung bürokratischer Anforderungen minimiert werden könnte (z.B. indem Bewilligungen vorübergehend durch Allgemeinverfügung erteilt werden).

Ist im Ergebnis ein beträchtlicher oder existenzbedrohender Schaden anzunehmen, sollte von einer erheblichen Auswirkung im Sinne des Art. 2 Abs. 2 f) ii) NIS-2-RL ausgegangen werden.

---

[3] Die Auswirkung bzw. Schäden auf Seiten der Verwaltung sind hingegen für diese Betrachtung unbeachtlich. Insoweit ist das Vorgehen von einem Risikomanagement für die Verwaltung abzugrenzen.

[4] Der Auswertungsbogen findet sich unter <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BIA_Auswertungsbogen_mit_BSP.xlsx?__blob=publicationFile&v=2>.

Bei der Bewertung der möglichen Auswirkungen einer Störung stellt sich auch die Frage des Zeithorizonts für die Störung des Dienstes. Ein solcher muss festgelegt werden, denn auch die für sich gesehen geringfügige Störung eines Dienstes über einen längeren Zeitraum wird irgendwann zu einer erheblichen Auswirkung führen. In Anlehnung an den vorgenannten Auswertungsbogen des BSI sollten wenigstens die Auswirkungen eines Ausfalls des Dienstes in einem Zeitraum von 30 Tagen betrachtet werden. Damit haben alle Dienste eine erhebliche Auswirkung, deren Störung über einen Zeitraum von 30 Tagen oder kürzer zu einem beträchtlichen oder existenzbedrohenden Schaden bei der Durchführung der kritischen wirtschaftlichen Tätigkeit führt.

Wie erwähnt, soll bei der Beurteilung der erheblichen Auswirkung die Eintrittswahrscheinlichkeit einer Störung keine Berücksichtigung finden. Eine solche Bewertung ist mit Art. 2 Abs. 2 f) ii) NIS-2-RL vereinbar, da die Richtlinie für Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene eine „risikobasierte Bewertung“ fordert. Gegen eine Berücksichtigung der Eintrittswahrscheinlichkeit spricht erstens, dass die Bewertung der Eintrittswahrscheinlichkeit einer Störung des jeweiligen Dienstes schwer durchführbar sein wird, da hierfür eine Vielzahl an Ursächlichkeiten betrachtet werden müsste. Dadurch entsteht unnötige Komplexität. Zweitens wird es kaum Dienste mit Bezug zu kritischen Tätigkeiten geben, bei denen eine erhöhte Wahrscheinlichkeit für eine Störung vorliegt. Entscheidend ist drittens, dass die Berücksichtigung der Eintrittswahrscheinlichkeit zur Folge hätte, dass durch die Ergreifung von Maßnahmen, welche die Wahrscheinlichkeit einer Störung senken, ein Dienst aus dem Anwendungsbereich der NIS-2-RL fiele. Die Eröffnung des Anwendungsbereichs der NIS-2-RL kann aber nicht davon abhängen, welche risikoverringernden Maßnahmen die jeweilige Einrichtung ergreift. Viertens wird die Frage nach der Wahrscheinlichkeit und den Auswirkungen eines Ausfalls der Netz- und Informationssysteme ohnehin im Rahmen der Risikomanagementmaßnahmen beantwortet (vgl. Art. 21 Abs. 1 UAbs. 2 NIS-2-RL).

Demnach ist die Einordnung als kritischer Dienst allein von dem erwarteten Schadenspotential für den Fall einer Störung über einen bestimmten Zeitraum (30 Tage) abhängig. Jedenfalls bei einem beträchtlichen oder existenzbedrohenden Schaden ist von einer erheblichen Auswirkung auszugehen.

Ein kritischer Dienst im Sinne des Art. 2 Abs. 2 f) ii) NIS-2-RL liegt demnach dann vor, wenn der Ausfall des Dienstes in einem Zeitraum von bis zu 30 Tagen einen beträchtlichen oder existenzbedrohenden Schaden und damit eine erhebliche Auswirkung für die jeweilige kritische wirtschaftliche Tätigkeit zur Folge hätte.

II. Anwendung des Identifizierungskonzepts

Bei der Anwendung des oben entwickelten Identifizierungskonzepts sollten die einleitend genannten Durchführungsziele berücksichtigt werden. Die Anwendung sollte wirtschaftlich und unbürokratisch sein und möglichst sämtliche kritischen Dienste in der Landesverwaltung erfassen. Außerdem sollte ein bundesweit möglichst homogenes Identifikationsergebnis angestrebt werden.

Grundlegend sind zwei Anwendungsmethoden denkbar: Bei einer formalen Anwendung werden die kritischen Dienste anhand einer abstrakten Bewertung ihrer potentiell erheblichen Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten vorab identifiziert und z. B. durch Gesetz oder Rechtsverordnung festgelegt. Denkbar wäre es z. B. die obersten Landesbehörden und die zentralen IT-Dienstleister als Einrichtungen mit kritischen Diensten abstrakt zu identifizieren. Die formale Anwendung hat den Vorteil, dass sie mit einem vergleichsweise geringen wirtschaftlichen Aufwand verbunden ist und ein bundeseinheitliches Identifizierungsergebnis gewährleistet. Sie läuft aber Gefahr, den besonderen Verwaltungsstrukturen einzelner Länder nicht ausreichend Rechnung

zu tragen; bestimmte kritische Dienste könnten in diesem Zuge übersehen werden (z. B. die Landestalsperrenverwaltung Sachsen oder der Niedersächsischer Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz).

Dem gegenüber steht eine funktionale Anwendung. Hierbei bewerten die jeweiligen Einrichtungen ihre Dienste individuell und in eigener Verantwortung. Der Vorteil dieser Anwendung ist eine passgenaue, auf die jeweilige Einrichtung zugeschnittene risikobasierte Bewertung. Ihr Nachteil ist aber, dass die individuelle risikobasierte Bewertung mit einem erheblichen wirtschaftlichen und bürokratischen Aufwand einhergeht und zwischen den Ländern ein uneinheitliches, heterogenes Identifizierungsergebnis droht.

Es wird vorgeschlagen, die Behörden mit gesellschaftlich kritischen Tätigkeiten formal und die Einrichtungen mit Bezug zu kritischen wirtschaftlichen Tätigkeiten funktional zu identifizieren. Um eine möglichst wirtschaftliche Anwendung zu gewährleisten, bietet es sich an, das Verfahren ausgehend von den obersten Landesbehörden durchzuführen:

1. Formale Identifizierung: Die obersten Landesbehörden, zentrale IT-Landesdienstleister und ggf. weitere, nach Landesrecht identifizierte Einrichtungen werden formal als Erbringer kritischer gesellschaftlicher Tätigkeiten[5] identifiziert.
2. Funktionale Identifizierung: Die obersten Landesbehörden prüfen für jede Behörde oder Einrichtung in ihrem Geschäftsbereich zunächst, ob diese einen unmittelbaren oder mittelbaren Bezug zu einer kritischen wirtschaftlichen Tätigkeit hat. Ggf. ist hierfür auch eine Subdelegation an Mittelbehörden erforderlich. Besteht kein unmittelbarer oder mittelbarer Bezug, entfällt für diese Behörde oder Einrichtung die Ermittlung und Prüfung der Dienste bereits.
3. Für jede nicht formal identifizierte Einrichtung, die generell einen Bezug zu einer kritischen wirtschaftlichen Tätigkeit hat, werden Dienste[6] im Sinne von Schritt 2 und 3 geprüft. Sobald ein kritischer Dienst festgestellt wurde, kann die Prüfung beendet werden, da die Einrichtung dann in den Anwendungsbereich der Regelung fällt.

Diese Abfolge des Identifizierungsprozesses ist in Abbildung 2 dargestellt. Damit sind alle kritischen Dienste bekannt, entweder selbst eine kritische gesellschaftliche Tätigkeit darstellen oder die in einer obersten Landesbehörde und dessen Geschäftsbereich einen mittelbaren oder unmittelbaren Bezug zu kritischen wirtschaftlichen Tätigkeiten haben. Für eine Einrichtung, die diese Dienste erbringt, muss dann landesrechtlich eine Umsetzung der NIS-2-RL erfolgen.

[5] Die genannten Einrichtungen können darüber hinaus auch Dienste mit Bezug zu kritischen wirtschaftlichen Tätigkeiten aufweisen. Diese ist bei Vollzug der NIS-2-RL in der Einrichtung zu beachten.
[6] Hier könnte insbesondere bei verwaltungsinternen Dienstleistungen eine hohe Abstraktionsebene gewählt werden, um den Aufwand für die Identifizierung niedrig zu halten.

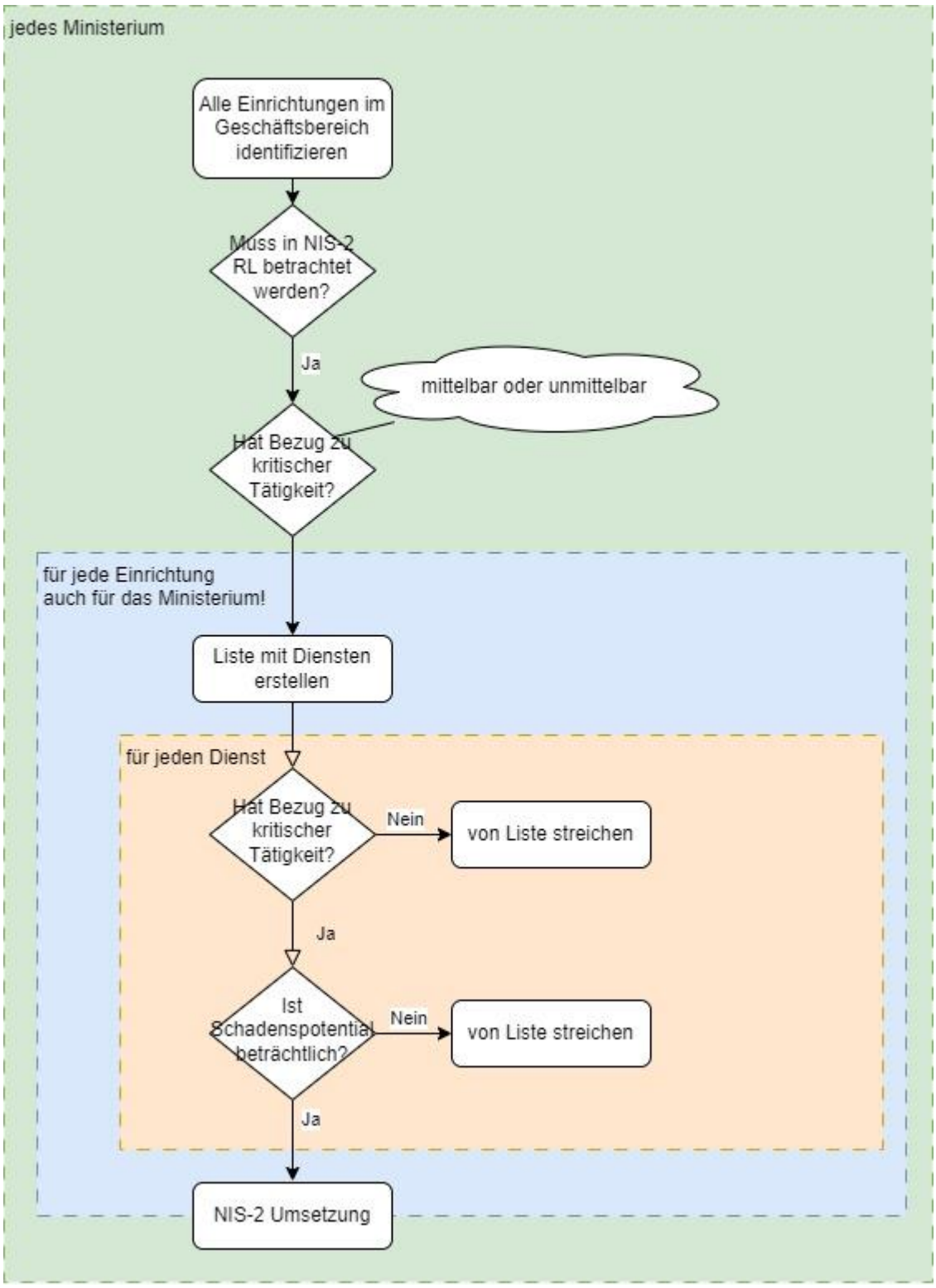

Abbildung 2 Prozess zur Identifizierung

Fiktives Beispiel für das Nds. Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz:

Das Nds. Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz hat im nachgeordneten Bereich das Landesamt für Verbraucherschutz und Lebensmittelsicherheit. Für dieses wird ein Bezug zu kritischen Tätigkeiten (§ 2 Abs. 10 Nr. 1 BSIG i. V. m. § 3 Abs. 1 Nr. 1 BSI-KritisV (Trinkwasserversorgung)) festgestellt. Es wird eine Liste mit allen in Zusammenhang mit Trinkwasser stehen-

den Verwaltungsleistungen erstellt. Unter den Verwaltungsleistungen gibt es z. B. den Dienst „Trinkwasserkontrolle“. Für diesen Dienst wird ein direkter Bezug zu einer kritischen wirtschaftlichen Tätigkeit festgestellt. Das Schadenspotential wird als erheblich bewertet, da ein Ausbleiben der Trinkwasserkontrolle die Trinkwasserversorgung wenigstens beträchtlich gefährden kann. Nun werden die für den Dienst benötigten verwaltungsinternen Dienstleistungen bestimmt. Hier findet sich unter anderem die Bereitstellung der IT für einen Standard-Arbeitsplatz (PC, Telefonie, E-Mail, Officeanwendungen, …) sowie ein spezielles Onlinetool zur Kommunikation der Ergebnisse mit den Trinkwasserversorgern. Beides wird von einem zentralen IT-Dienstleister bereitgestellt. Sowohl das Landesamt für Verbraucherschutz und Lebensmittelsicherheit als auch der zentrale IT-Dienstleister fallen somit in den Anwendungsbereich der NIS-2-RL.

III Synergie mit dem IT-Notfallmanagement/ BCM

Bei der Identifizierung von Diensten im Rahmen der NIS-2-RL und notwendigen Schritten beim Ausbau und Betrieb eines IT-Business Continuity Management (IT-BCM) besteht ein hohes Synergiepotential. Da sich der IT-Planungsrat in der 28. Sitzung mit Beschluss 2019/04 darauf geeinigt hat, dass alle Länder ein IT-Notfallmanagement aufbauen müssen, sei an dieser Stelle auf eine mögliche Verbindung hingewiesen. Auch im Rahmen eines BCM müssen Dienste (Geschäftsprozesse) erhoben und auf ihre Kritikalität hin geprüft werden. Die Schadensszenarien, die geprüft werden, sind nicht festgelegt. Typischerweise enthalten diese z. B. Imageschaden oder finanziellen Schaden. Fügt man den zu betrachtenden Szenarien „Auswirkungen auf kritische wirtschaftliche Tätigkeiten gem. NIS-2-RL“ hinzu, so lassen sich auf einfache Weise im Rahmen des BCM auch alle Dienste ermitteln, die unter die NIS-2-RL fallen. Das weitere Vorgehen im Rahmen des BCM (nach BSI 200-4) stellt sicher, dass die Erfordernisse, wie in diesem Identifizierungskonzept beschrieben, sichergestellt und durchgeführt werden (z. B. die Risikoanalyse).

Darüber hinaus bietet die Integration der NIS-2-RL relevanten Dienste in ein bestehendes BCM noch weitere Vorteile. So wird durch das BCM z. B. Art. 21 Abs. 2 c) NIS-2-RL abgedeckt. Außerdem wird das BCM regelmäßig überprüft und aktualisiert.