ANGA
Der Breitbandverband

Stellungnahme der ANGA zur Bundesnetzagentur Handreichung zur Resilienz

Die ANGA bedankt sich für die Zusendung der Handreichung und die Möglichkeit diese Handreichung kommentieren zu können.

Die ANGA bedankt sich zudem bei der Bundesnetzagentur für die Beantwortung der gestellten Fragen. Die Antworten auf die gestellten Fragen hilft bei der Kommentierung einzuordnen, welche Ziele mit der Handreichung verfolgt werden sollen. Wir haben versucht, dies im Rahmen der Möglichkeiten einer Handreichung aufzugreifen.

Hierfür jedoch sollte die Handreichung zunächst um einen Scope erweitert werden, der die Aufgabe der Handreichung präzise beschreibt. Dies würde die Arbeit mit dieser Handreichung und die möglichen Diskussionen zur Handreichung mehr fokussieren.

Vorab gestellte Fragen der ANGA an die BNetzA und die Antworten der BNetzA dazu:

Frage 1: Welches Schutzziel soll die Handreichung abdecken?
Antwort der BNetzA: Die Handreichung soll kein konkretes Schutzziel abdecken. Die im Katalog der Sicherheitsanforderungen aufgeführten Schutzziele sollten durch die Umsetzung des Kataloges in den Unternehmen bereits erfüllt sein (zum Ziel und dem Charakter der Handreichung s. Antworten auf Frage 5, 6 und 8).

Frage 2: Wie werden kleine und mittlere Unternehmen definiert. Welche verpflichtende Schwellwerte ziehen Sie zu der Definition heran?
Antwort der BNetzA: Hier verweisen wir auf die Definition der EU-Kommission: Kleinstunternehmen: weniger als 10 Mitarbeiter und ein Jahresumsatz (der Geldbetrag, der in einem bestimmten Zeitraum eingenommen wurde) bzw. eine Jahresbilanz (eine Aufstellung der Vermögenswerte und Verbindlichkeiten eines Unternehmens) von unter 2 Mio. EUR. Kleines Unternehmen: weniger als 50 Mitarbeiter und ein Jahresumsatz bzw. eine Jahresbilanz von unter 10 Mio. EUR. Mittleres Unternehmen: weniger als 250 Mitarbeiter und ein Jahresumsatz von unter 50 Mio. EUR bzw. eine Jahresbilanz von unter 43 Mio. EUR (Quelle: Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen).

Frage 3: Welche KRITIS-Sektoren sollen durch die Handreichung abgedeckt werden?
Antwort der BNetzA: Die Handreichung richtet sich an Unternehmen des TK-Sektors, also Betreiber von TK-Netzen und Anbieter von TK-Diensten.

Frage 4: Bezogen auf die Handreichung - wie werden Auswirkungen von Betriebsstörungen betrachtet? Welche Schwellwerte werden hier herangezogen?
Antwort der BNetzA: Das Melden der Sicherheitsvorfälle mit beträchtlichem Ausmaß gemäß dem Meldekonzept der BNetzA ist im § 168 TKG geregelt und bleibt durch die Handreichung unberührt.

Frage 5: Wie ist die Handreichung zu der derzeitigen Erstellung des Sicherheitskatalogs einzuordnen und wie wird hier eine Einbindung in die Gesetzgebungsverfahren gesehen?
Antwort der BNetzA: Die Handreichung ist als eigenständiges Dokument anzusehen. Dieses steht nicht im direkten Zusammenhang mit dem Katalog für Sicherheitsanforderungen.

Frage 6: Welchen Stellenwert wird die Handreichung im Vergleich zu dem Sicherheitskatalog haben? Wird der Sicherheitskatalog die Inhalte der Handreichung noch zukünftig beeinflussen?
Antwort der BNetzA: Der Katalog von Sicherheitsanforderungen ist durch die Allgemeinverfügung vom 29.04.2020 erlassen worden, deren Charakter ist rechtsbindend. Die Handreichung enthält lediglich Handlungsempfehlungen, um kleineren und mittleren Unternehmen gesammelt Informationen zu der Thematik Resilienz zur Verfügung zu stellen. Die gesetzlichen Anforderungen und die Anforderungen des Sicherheitskataloges sind zwingend zu erfüllen, die Handreichung wird keinen rechtsbindenden Charakter haben und wird in keinster Weise die Verfügungen des Kataloges für Sicherheitsanforderungen oder Forderungen aus dem TKG berühren.

Frage 7: Soll die Handreichung a) Risikomanagement und b) Krisenmanagement gemeinsam behandeln oder nur eines von beiden?
Antwort der BNetzA: Da das Risikomanagement eng mit dem Krisenmanagement verzahnt ist, sollten beide Bereiche zumindest in groben Zügen behandelt werden.

Frage 8: Die Handreichung soll ein Risikomanagement für kleinere und mittlere Unternehmen vornehmen und dann auf praktikable und sinnvolle Maßnahmen verweisen? Ist das Ziel der Handreichung richtig erfasst?
Antwort der BNetzA: Das Ziel der Handreichung ist korrekt erfasst. Insgesamt soll die Handreichung eine Hilfestellung und einen Überblick verschaffen. Das Thema Resilienz ist sehr breit gefächert und in der Regel ist das Studium von zahlreichen umfangreichen Dokumenten notwendig. Hier soll die Handreichung Abhilfe schaffen und kurz und prägnant Informationen liefern und Verweise auf tiefergehende Quellen enthalten.

Frage 9: Welcher genaue Anwendungsbereich im Zusammenhang mit NIS2 soll durch die Handreichung abgedeckt werden?
Antwort der BNetzA: Das Ziel und der Zweck der Handreichung ist es nicht, die Anforderungen der NIS2 Richtlinie umzusetzen. Die Umsetzung der NIS2 Richtlinie in nationales Recht ist nicht Aufgabe der BNetzA, sondern wird durch das NIS2UmsuCG geregelt.

Anregungen:

1.

Zunächst sollte deutlich gemacht werden, mit welchen Verbänden und Unternehmen aus dem TK-Sektor sowie Behörden die Handreichung erstellt wurde. Dies gibt dem Leser vor allem Rechtssicherheit.

2.

Hinsichtlich der erfassten Unternehmen sollte mehr ins Detail gegangen werden. Grundsätzlich sind – auch entsprechend der obigen Antwort – folgende grundlegenden Kriterien relevant:

Größenklasse	Beschäftigte	Jahresumsatz	Jahresbilanzsumme
Kleines Unternehmen (KU)	< 50 und	≤ 10 Mio. Euro oder	≤ 10 Mio. Euro
Mittleres Unternehmen (MU)	< 250 und	≤ 50 Mio. Euro oder	≤ 43 Mio. Euro
Großes Unternehmen (GU)	≥ 250 oder	> 50 Mio. Euro und	> 43 Mio. Euro

Allerdings sollte darauf hingewiesen werden, dass bei Unternehmen mit einer komplexeren Struktur (z.B. Tochtergesellschaft im Konzern) eine Einzelfallprüfung erforderlich ist. Für die Beurteilung wird neben der Unternehmensgröße (d.h. Mitarbeiterzahl und Umsatz- bzw. Bilanzzahl) berücksichtigt, ob es sich um ein eigenständiges Unternehmen, Partnerunternehmen (Beteilungen an anderen Unternehmen ab 25 % bis 50 %) oder verbundenes Unternehmen (Beteiligungen an anderen Unternehmen über 50 %) handelt.

Umgekehrt sollte klar werden, dass es von dieser Beurteilung Ausnahmen gibt, da bestimmte Unternehmen unabhängig von ihrer Größe in den Anwendungsbereich fallen:

- Vertrauensdiensteanbieter
- Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
- TLD-Namenregister und DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern
- Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essenziell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.

Zusätzlich müssen auch Dienstleister und Lieferanten von betroffenen Unternehmen Sicherheitsvorkehrungen einhalten. Gerade dieser Punkt der Betroffenheit der Dienstleister und Lieferanten müsste in der Handreichung deutlicher herausgestellt werden. Service Unternehmen, die die Wartung und Störbeseitigung in den Netzen vornehmen, müssten im gleichen Maße geprüft werden wie die eigenen Mitarbeiter. Ebenfalls müssten dort entsprechende Bereiche eingeführt werden. Hierbei ist aber darauf zu achten, dass die Kosten in einem überschaubaren Rahmen bleiben. Die Listung der Vermögenswerte/Inventar müsste auf jeden Fall mit der Liste des Netzbetreibers abgeglichen sein.

In der Definition der Betroffenheit fehlt zudem die Liste der wesentlichen Einrichtungen:

Als wesentliche Einrichtungen gelten große Unternehmen aus den Sektoren

- Energie
- Verkehr
- Bankwesen
- Finanzmarkt
- Gesundheit
- Trinkwasser
- Abwasser
- Verwaltung von IKT-Diensten
- Weltraum

In diesem Zusammenhang wäre denn auch eine Erläuterung hilfreich, was die Rolle der IKT-Anbieter in Bezug auf die Sektoren ist. Es ist in der Handreichung insbesondere nicht klar, welche Rolle hier Verbände übernehmen sollen.

Es wird zudem unerlässlich sein, die Forderungen aus der Handreichung mit der nationalen KRITIS-Resilienz-Strategie zu synchronisieren.

Um die gesamtstaatlichen strategischen Ziele und politischen Maßnahmen zur Stärkung der Resilienz kritischer Infrastrukturen festzulegen, wird gemäß Artikel 4 der Richtlinie (EU)

2022/2557 bis 17. Januar 2026 eine nationale Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen (Nationale KRITIS-Resilienzstrategie) verabschiedet. Mit der Umsetzung der NIS 2 Richtlinie wird ebenfalls die Definition von kleinen, mittleren und großen Unternehmen veröffentlicht, an der sich auch die Handreichung zu orientieren hätte.

Die Handreichung unterscheidet auch nicht, ob ein Unternehmen wesentlich oder wichtig ist, wie dies die NIS-2-Richtlinie tut. Der Unterschied ist für das TK Unternehmen sehr entscheidend, da die Bußgelddrohungen deutlich unterschiedlich sind. Bezüglich der digitalen Infrastruktur unterscheidet die NIS-2-Richtlinie noch einmal, was ein wichtiges und ein wesentliches Unternehmen ist.

Aus der Handreichung wird jedenfalls nicht klar, wie sich die Begriffe wichtig und wesentlich auf die Unternehmen in der Lieferkette beziehen. Gerade auch für Kooperationen zwischen TK-Betreibern, wie z.B. im Kontext von Open Access sind die Anforderungen entsprechend herauszustellen. Das Gigabitforum der BNetzA ist hier sehr aktiv und die Ergebnisse sollten hier gemeinsam abgestimmt sein. Für die praktische Arbeit und die Abwägung der erforderlichen Maßnahmen wäre dieser Punkt wichtig.

Anbieter öffentlicher elektronischer Kommunikationsnetze oder elektronischer Kommunikationsdienste werden bei „groß“ und „mittel“ als wesentlich eingestuft, während „kleine“ Unternehmen nur als wichtig eingestuft werden. Bei Anbietern von Internet-Knoten, Cloud Computing Diensten, Rechenzentrumsdiensten und Content Delivery Networks wird die Einteilung noch detaillierter, da es dort keine kleinen Unternehmen mehr gibt. Um dem Praxisbezug der Handreichung gerecht zu werden, sollte es in der Handreichung einen Hinweis auf den möglichen Umgang mit der Einstufung geben.

3.

Es erscheint, dass der Zeitpunkt der Veröffentlichung der Handreichung unglücklich gewählt wurde, da derzeit die NIS-2-Richtlinie in nationales Recht umgesetzt wird und gleichzeitig das KRITIS-Dach-Gesetz zur Anhörung verteilt wurde. Zusätzlich soll bis zum 17. Januar 2024 eine nationale Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen verabschiedet werden.

4.

Die Handreichung verweist auch nicht auf die Risikomanagementmaßnahmen, die nach NIS-2 durchzuführen sind. Auch der Unterschied zwischen Risikomanagement und Risikoanalyse wird nicht erläutert. Dies sind aber Punkte, unter welche die empfohlenen Maßnahmen in der Handreichung eingeordnet werden müssen. Gerade wenn die nationale Umsetzung der NIS-2-Richtlinie in Deutschland kommt, werden diese Punkte immer wichtiger und die Handreichung sollte hier einen praktikablen Hinweis geben, der auch Bestand hat.

5.

Die Sicherheit der Lieferketten in der Telekommunikation und die sicherheitsbezogenen Aspekte der Beziehungen spielen eine große Rolle, da in der vernetzten Welt der

Telekommunikation über schädliche Software großer Schaden angerichtet werden kann. (NIS-2 geht auf diese Szenarien ein). Die Handreichung hat dazu keine Empfehlungen. Es muss jedoch Ziel der Handreichung sein, dass jemand, der die Handreichung in seinem Unternehmen vollständig umsetzt, keine weiteren Maßnahmen treffen muss, wenn die NIS-2-Richtlinie in deutsches Recht umgesetzt wird oder das KRITIS-DachG in Kraft tritt. Der einfache Satz, dass die gesetzlichen Vorgaben grundsätzlich einzuhalten sind, genügt dafür sicherlich nicht.

6.

Es wäre hilfreich, wenn in der Handreichung Hinweise zur Berichtspflicht nach NIS-2 zu den zuständigen CSIRT (Cybersecurity Incident Response Team) gegeben würde.

Hier wäre es hilfreich mitzuteilen, welche Dokumente zu liefern und, welche Aufstellungen und Zahlen notwendig sind. Dies würde die Arbeit sowohl für Unternehmen als auch CSIRT vereinfachen. Gerade bei den kurzen Fristen der Berichtspflicht (wir reden hier über Stunden) wäre eine solche Empfehlung wichtig. Es wäre auch hilfreich zu wissen, welche zusätzlichen Statusberichte das CSIRT abfragen darf und wird. Auch hierzu sollte es eine Empfehlung geben. Gerade im Hinblick auf die Informationen an weitere Betreiber, wäre es wichtig, aus der vergangenen Erfahrung der CSIRT Kommunikation zu lernen, um Informationen zielgerichtet verfassen zu können. Damit kann das Gesamtsystem verbessert werden.

Das Thema DATA BREACH (Verletzung des Schutzes personenbezogener Daten) mit seinen Auswirkungen auf die DGSVO und deren Berichtspflichten muss hier ebenfalls einbezogen werden. Wenn nationale Risikoanalysen und Risikobewertungen für kritische Dienstleistungen durchgeführt werden, sollte die Handreichung hierzu Hinweise geben, damit sich betroffene Betreiber sinnvoll daran beteiligen können. Da die Handreichung auch dazu beitragen soll, dass nicht-IT-bezogene Maßnahmen zur Stärkung der Resilienz der Betreiber kritischer Anlagen erstmals in einem einheitlichen, sektorenübergreifenden Standard mit Mindestvorgaben normiert werden kann, sind diese Punkte unbedingt einzubinden.

Der Stand der Technik soll möglichst einen praktikablen Stand reflektieren; die normalen Aufgaben der Netzbetreiber, wie Lawful Interception dürfen mit den Maßnahmen aber nicht negativ beeinflusst werden. Hier wäre zu klären, welche Resilienz-Anforderungen an diese Netzzugänge gestellt werden. Insbesondere wäre zu betrachten, ob dazu TR TKÜV überarbeitet werden muss.

7.

In dem Zusammenhang muss auch auf die Haftung der Geschäftsführung hingewiesen werden, wenn essenzielle Risikoabwägungen vernachlässigt oder ignoriert wurden. Das Thema Resilienz bedarf einer konkreten Budgetplanung und einer Planung von personellen Ressourcen, die wahrscheinlich einer entsprechenden Schulung bedürfen. Damit kommen Faktoren wie Budget und Zeit zur Umsetzung der Maßnahmen ins Spiel. Hier kann die schon vorliegende Handreichung entsprechend erweitert werden und einen wertvollen Beitrag zur Umsetzungsplanung liefern.

Es ist für die ANGA klar, dass derzeit bei der NIS 2 nicht nur die aufkommenden Kosten betrachtet werden dürfen und diese als eine Hürde angesehen werden, sondern diese Kosten denen eines möglichen Cyber-Angriffs gegenübergestellt werden müssen. Ein Cyberangriff

wird durch Vertrauensverlust und Produktionsausfälle einen sehr viel höheren finanziellen Schaden verursachen. Daher unterstützt die ANGA mit Ihren Mitgliedern die Handreichung und möchte einer breiten Öffentlichkeit eine routinemäßige Handhabung bei möglichen Vorfällen an die Hand geben, damit ein möglicher Schaden gar nicht auftritt oder die Auswirkung, auch auf die Lieferkette, gering bleibt.

8.

Da die Handreichung sich nur auf die TK Unternehmen bezieht, wäre die mögliche Beschreibung von Schnittstellen zu den anderen Sektoren wichtig, da in allen Fällen die TK-Infrastruktur auch für diese Sektoren eine Rolle spielt.

Das KritisDach G postuliert dazu folgenden Punkt: [..] *Zur weiteren Konkretisierung von sektorübergreifenden Resilienzmaßnahmen wird das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe einen Katalog mit Mindestanforderungen erarbeiten.* [..]

Gerade die sektorübergreifende Resilienz-Maßnahmen sollten der Mindestanforderung entsprechen und diese Mindestanforderungen des Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sollten in die Handreichung einfließen.

Hier empfiehlt die ANGA einen engen Schulterschluss zwischen der BNetzA und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, damit Empfehlungen an die Netzbetreiber nicht durch widersprüchliche Regeln entkräftet werden. Dies kommt auch der Forderung aus der RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 nach, die postuliert: [..] *es von wesentlicher Bedeutung, einen Unionsrahmen zu schaffen, der sowohl darauf abzielt, die Resilienz kritischer Einrichtungen im Binnenmarkt durch die Festlegung harmonisierter Mindestverpflichtungen zu verbessern, als auch darauf, diesen Einrichtungen durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu helfen.* [..]

Die Schaffung und Beachtung des Unionsrahmens ist bei der Verwobenheit der Sektoren ein ganz wichtiger Punkt. Die ANGA sieht diese Handreichung als einen Teil der Unterstützungsmaßnahmen gemäß Richtlinie . Dennoch sieht die ANGA hier den globalen Ansatz, da Endgeräte meist auf dem globalen Markt erworben werden, der über den Binnenmarkt hinausgeht, die funktionsbedingt einen sehr engen Kontakt zum Netzwerk pflegen.

9.

Zu klären wäre insbesondere, welche Aufgaben der Marktaufsicht und den entsprechenden harmonisierten Standards zukommen. In diesem Kontext wäre zudem ein praktikabler Hinweis für kundeneigene Endgeräte von besonderer Bedeutung.

Bei kundeneigenen Endgeräten kann der Netzbetreiber nicht Einfluss auf die genutzte Firmware nehmen und auch nicht im Sinne der Resilienz die Verantwortung übernehmen. Hierzu wäre ein klarer Hinweis in der Handreichung wichtig. Die geforderte Resilienz darf durch solche Endgeräte nicht aufgebrochen werden. Dieses Szenario wird weder in der EU Richtlinie 2022/2557 betrachtet, noch schreibt die Handreichung etwas zum deutschen Sonderweg.

Berlin, 16. Januar 2024

ANGA Der Breitbandverband e.V. vertritt die Interessen von mehr als 200 Unternehmen der deutschen Breitbandbranche. Die Unternehmensvereinigung setzt sich gegenüber Politik, Behörden und Marktpartnern für investitions- und wettbewerbsfreundliche Rahmenbedingungen ein.

Zu den Mitgliedsunternehmen zählen Netzbetreiber wie Vodafone, Tele Columbus (PYUR), EWE TEL, NetCologne, M-net, wilhelm.tel und eine Vielzahl von Technologieausrüstern. Sie versorgen insgesamt mehr als 20 Millionen Kunden mit Fernsehen und Breitbandinternet.

Neben der politischen und regulatorischen Interessenvertretung zählt zu den satzungsmäßigen Aufgaben des Verbandes die Verhandlung mit den urheberrechtlichen Verwertungsgesellschaften. Die Mitgliedsunternehmen erhalten dadurch kostengünstige Musterlizenzverträge für die Weitersendung von Fernseh- und Hörfunkprogrammen.