CERT.at GmbH
Karlsplatz 1/2/9
1010 Wien · Austria

CERT.at

Stellungnahme zum Entwurf des NISG 2024

BKA-Geschäftszahl
2024-0.220.735

Dokumenttyp:	**Autor:** Otmar Lendl	**Version:** 1.0
Evaluierung / Assessment	**Erstellung/Änderung** am 20240417	**Status:** Final
Klassifikation:	**T** +43 1 505 64 16 78	**Gültig von:** 20240417
öffentlich	**Mail:** lendl@cert.at	**Gültig bis:** -
Adressatenkreis:	NIS Behörden, Nationalrat, Öffentlichkeit	

1 Vorbemerkungen

Wir begrüßen die Chance, den Entwurf zum NIS-Gesetz 2024 begutachten und kommentieren zu können.

Wir haben keine groben Bedenken gegen dieses Gesetz, es setzt in vielen Bereichen die EU-Richtlinie direkt um. Trotzdem gibt es im vorliegenden Text einige Unstimmigkeiten, die sich unseres Erachtens leicht korrigieren lassen. Der Großteil der folgenden Kommentare sind in diesem Sinn zu lesen: es geht nicht um grobe Änderungsvorschläge im Inhalt, sondern um **Klarstellungen und sprachliche Verbesserungen** in Details.

Dieses Dokument erwähnt nur die Punkte, wo wir Verbesserungspotential sehen, nicht aber die Punkte, wo wir den Entwurf für richtig und wichtig halten (etwa §8 Abs. 11).

2 Begriffsbestimmungen

Die Definitionen sind weitgehend verständlich. Zwei gute Ansätze sind leider nicht konsequent durchgezogen:

1. Abkürzungen / Akronyme werden manchmal bei der ersten Verwendung erklärt (Beispiel „Top Level Domain – TLD“`), aber nicht immer, etwa bei „IKT“ oder „DNS“.
2. Manche sperrigen deutschen Formulierungen werden durch ihre bekannteren, englischen Pendants ergänzt, etwa bei 23. „Anbieter verwalteter Dienste“ (Managed Service Provider). oder 29. „Beinahe-Cybersicherheitsvorfall“ (Near Miss). Das wäre auch bei 24. hilfreich, optimalerweise auch gleich mit der geläufigen Abkürzung, also „Anbieter verwalteter Sicherheitsdienste“ (Managed Security Service Provider – MSSP)

Verbesserungsbedarf sehen wir daher bei:

- *12 „DNS-Diensteanbieter“ vs. §24 „*Domänennamensystem-Diensteanbieter“

  In §3 Z. 12 wird der Begriff „DNS-Diensteanbieter“ bestimmt und mehrfach im NISG 2024 entsprechend verwendet. In §24 wird einmalig der Begriff „Domänennamensystem-Diensteanbieter“ verwendet. Wir vermuten, dass dies dieselbe Funktion beschreiben soll und empfehlen daher die Verwendung des Begriffs „DNS-Diensteanbieter“. Andernfalls bräuchte es für „Domänennamensystem-Diensteanbieter“ eine eigene Begriffsbestimmung.
  Auch wäre es sinnvoll, analog zu („Top Level Domain – TLD“`) von 13. hier ein „(Domainnamensystem – DNS)“ einzufügen.

- *12 b) autoritative Dienste zur Auflösung von Domänennamen zur Nutzung durch **Dritte**, mit Ausnahme von Root-Namenservern, anbietet;*

  „Dritte“ ist hier nicht eindeutig definiert. Es könnte sich auf Domaininhaber beziehen, die ihre Domains auf den autoritative Nameservern eines DNS-Diensteanbieters hosten lassen, oder auf die Personen, die Anfragen an diese Nameserver stellen. Die erstere Deutung ist hoffentlich die gewünschte, wenn man „Dritte“ durch „Domaininhaber“ ersetzt, ist das eindeutig. Alternativ könnte man das in den EB ausführen.

- *14 „Einrichtung, die Domänennamen-Registrierungsdienste erbringt“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa ein Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten;*

  Hier ist schon in der deutschen Version der NIS-2-Richtlinie ein Übersetzungsfehler passiert, da die Begriffe „Anbieter“ und „Wiederverkäufer“ vertauscht wurden. Das Englische *„(22) ‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;“* muss auf Deutsch korrekterweise lauten:

  *„Einrichtung, die Domänennamen-Registrierungsdienste erbringt“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa ein Anbieter von Datenschutz- oder Proxy-Registrierungsdiensten **oder Wiederverkäufer**;“*,

  oder (besser)

  *„Einrichtung, die Domänennamen-Registrierungsdienste erbringt“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa **Wiederverkäufer oder Anbieter** von Datenschutz- oder Proxy-Registrierungsdiensten;*

- 25 *„ein CSIRT“*, 33 *„… den Computer-Notfallteams (CSIRTs)“*

  Das Akronym „CSIRT“ ist ein generischer Begriff, im Rahmen dieses Gesetzes sind aber nur die CSIRTs gemeint, die laut §8 Abs. 2 – 4 eingerichtet oder ermächtigt wurden. Eine Klarstellung dazu in den Begriffsbestimmungen wäre willkommen.

- 35. *„CSIRTs-Netzwerk“ ein gemäß Art. 15 NIS-2-Richtlinie errichtetes Gremium zum Aufbau von Vertrauen zwischen den Mitgliedstaaten der Europäischen Union und zur Förderung einer raschen und wirksamen operativen Zusammenarbeit zwischen ihnen;*

  Das ist so nicht korrekt und leider ist hier bereits die NIS-2-Richtlinie nicht konsistent formuliert. (Siehe https://cert.at/en/blog/2021/11/an-update-on-the-state-of-the-nis2-draft Article 13). Das CSIRTs Netzwerk ist in der Praxis kein Gremium, in das die Mitgliedstaaten der EU ihre Vertreter entsenden, sondern es ist das Netzwerk, das alle (NIS-)CSIRTs der Mitgliedsstaaten als Mitglieder hat. Besser wäre daher einfach:

  35. „CSIRTs-Netzwerk“ das gemäß Art. 15 NIS-2-Richtlinie errichtetes Netzwerk der CSIRTs der Mitgliedstaaten der Europäischen Union;

3 Strukturen

- *§ 5 (1) Die Cybersicherheitsbehörde hat eine zentrale Anlaufstelle zu betreiben, die als operative Verbindungsstelle der Gewährleistung der Sicherheit von Netz- und Informationssystemen, der grenzüberschreitenden Zusammenarbeit und Kommunikation mit den zuständigen Stellen in den anderen Mitgliedstaaten der Europäischen Union sowie der Kooperationsgruppe, EU-CyCLONe und dem CSIRTs-Netzwerk dient.*

  In der NIS-2-Richtlinie gibt es in den Bestimmungen, die die Kooperationsgruppe, EU-CyCLONe und

das CSIRTs Network beschreiben, (Art. 14, 15 und 16) keinen Verweis auf die zentrale Anlaufstelle (SPOC), hingegen ist in Artikel 13 die Zusammenarbeit auf nationaler Ebene geregelt. Auch in Art.23 (6) geht es um eine nationale Kooperation zwischen CSIRT und SPOC. Konkret hat das CSIRTs Netzwerk daher keinerlei Mandat und auch keine Prozesse, um direkt mit den SPOCs zu kommunizieren, das ist immer die Aufgabe der jeweiligen CSIRTs.

Der Absatz sollte daher heißen:

*§ 5 (1) Die Cybersicherheitsbehörde hat eine zentrale Anlaufstelle zu betreiben, die als operative Verbindungsstelle der Gewährleistung der Sicherheit von Netz- und Informationssystemen, der grenzüberschreitenden Zusammenarbeit und Kommunikation mit den zuständigen Stellen in den anderen Mitgliedstaaten der Europäischen Union sowie **den österreichischen Mitgliedern** der Kooperationsgruppe, EU-CyCLONe und dem CSIRTs-Netzwerk dient.*

- *§8 (1) 1. die Überwachung und die Analyse von Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfällen auf nationaler Ebene und gegebenenfalls die Unterstützung betreffender wesentlicher und wichtiger Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit;*

  Bereits in der deutschen Version der NIS-2-Richtliniewurde das schon holprige englische „*concerned*“ als „*betreffende*“ übersetzt. Sprachlich richtig ist hier jedoch „***betroffener***“: damit sind klar die Einrichtungen gemeint, die von den Bedrohungen, Schwachstellen und Vorfällen betroffen sind.

  Der Absatz sollte daher heißen:

  *§8 (1) 1. die Überwachung und die Analyse von Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfällen auf nationaler Ebene und gegebenenfalls die Unterstützung **betroffener** wesentlicher und wichtiger Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit;*

- *§8 (1) 6. die Beteiligung am CSIRTs-Netzwerk (§ 3 Z 35) und die auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des CSIRTs-Netzwerks;*

  Besser wäre hier „*Teilnahme am*“ oder „*Mitgliedschaft im*“ statt „*Beteiligung am“.*

- *§8 (6) Dem nationalen CSIRT gebührt vom Bund ein pauschalierter Ersatz für die bei Erfüllung ihrer Aufgaben gemäß Abs. 1 entstandenen Aufwendungen.*

  Das sollte grammatikalisch richtig „***seiner** Aufgaben*“ heißen.

- *§9 (1) Die CSIRTs (§ 8 Abs. 2 bis 4) haben die zur Erfüllung der Aufgaben gemäß § 8 Abs. 1 erforderlichen technischen und organisatorischen Fähigkeiten aufzuweisen und müssen zur Gewährleistung einer angemessenen Personalausstattung über ausreichende Ressourcen und geeignetes Personal verfügen. Die Ermächtigung darf nur vertrauenswürdigen Personen verliehen werden.*

Wenn sich der zweite zitierte Satz auf natürliche Personen, also das Personal des CSIRTs, beziehen soll, dann könnte man diesen Satz entweder weglassen, weil diese Voraussetzung durch §9(1)7 auch festgeschrieben ist, oder alternativ das vertrauenswürdig in den vorhergehenden Satz mit einbauen, etwa:

Die CSIRTs (§ 8 Abs. 2 bis 4) haben die zur Erfüllung der Aufgaben gemäß § 8 Abs. 1 erforderlichen technischen und organisatorischen Fähigkeiten aufzuweisen und müssen zur Gewährleistung einer angemessenen Personalausstattung über ausreichende Ressourcen und geeignetes ***und vertrauenswürdiges*** *Personal verfügen.*

Wenn sich der zweite Satz auf juristische Personen bezieht, dann sollte in den EBs beschrieben werden, wie die Vertrauenswürdigkeit dieser nachgewiesen werden kann.

Anmerkung: hier wird *„CSIRTs (§ 8 Abs. 2 bis 4)"* benutzt, an anderen Stellen nur *„CSIRTs".* Eine Vereinheitlichung, am besten mit einer Begriffsbestimmung von „CSIRTs", wäre hilfreich.

- *§9 (1) 7. ihre Mitarbeiter müssen sich einer Sicherheitsüberprüfung nach §§ 55 ff SPG für den Zugang zu geheimer Information unterzogen haben. Die Sicherheitsüberprüfung ist alle fünf Jahre zu wiederholen.*

  Eine genaue Auslegung dieses Punktes heißt, dass CSIRTs neues Personal erst nach erfolgter Sicherheitsüberprüfung – die Monate dauern kann – einstellen können. Das ist nicht praktikabel. Außerdem ist der Punkt zu weit gefasst, da nicht jeder Mitarbeiter unbedingt Zugang zu sensitiven Daten hat bzw. braucht, um seiner Tätigkeit nachzukommen. Besser daher:

  ihre Mitarbeiter, ***welche Zugang zu sensitiven Informationen haben,*** *müssen sich einer Sicherheitsüberprüfung nach §§ 55 ff SPG für den Zugang zu geheimer Information unterzogen haben. Die Sicherheitsüberprüfung ist alle fünf Jahre zu wiederholen.*

- *§11 CVD*

  Es wäre wichtig, die Ziele der koordinierten Offenlegung von Schwachstellen explizit auszuführen, damit Missverständnisse in der Art von „Der Staat will die 0-days haben, damit er sie selbst ausnutzen kann" von vorneherein aus dem Weg geschafft werden können.

  Unserer Meinung nach sollten diese Ziele sein:
  - Minimierung der Wahrscheinlichkeit, dass die Schwachstellen ausgenutzt werden
  - Schutz des Meldenden vor negativen Folgen durch den Fund (etwa Klagen des Herstellers)
  - Schutz der Hersteller vor voreilig einseitiger Veröffentlichung von Schwachstellen

  Daher braucht es einen klaren Rahmen, welche Tests und Analysen zulässig sind und wo die Grenze zum illegalen Handeln liegt. Ob das im NISG 2024 zu regeln ist oder ggf. im Rahmen einer Verordnung erfolgen sollte, können wir nicht beurteilen.

  Die NIS-Kooperationsgruppe hat Empfehlungen für eine nationale CVD Policy veröffentlicht[1], die mehrere Punkte aufzählt, die die EU Mitgliedstaaten adressieren sollten. Der §11 ist hier bei weitem

[1] https://ec.europa.eu/newsroom/dae/redirection/document/99973

nicht ausreichend, um diese abzudecken. Das Thema umfassend im NISG2024 zu regeln, mag nicht möglich sein, eine Verordnungsermächtigung, damit der CVD-Prozess ausdefiniert werden kann, wäre hier aber sinnvoll.

Eine entsprechende Verordnungsermächtigung könnte daher in etwa lauten:

Der Bundesminister für Inneres hat in Abstimmung mit dem nationalen CSIRT in einer Verordnung festzulegen, wie sich Sicherheitsforscher beim Fund von Schwachstellen verhalten sollten, wie die Meldung an das CSIRT erfolgen soll und welche Zeitrahmen für die Offenlegung einzuhalten sind.

- §14 (1) „*und den CSIRTs*“

  Siehe Anmerkung zur Begriffsbestimmung von CSIRTs. Es sollte klargestellt werden, dass damit die CSIRTs laut §8 Abs 2 – 4 gemeint sind.

- *§14 (2) Die OpKoord kann um Vertreter von wesentlichen und wichtigen Einrichtungen sowie sonstigen Einrichtungen erweitert werden, wenn deren Wirkungsbereich von einem Cybersicherheitsvorfall, einer Cyberbedrohung oder einem Beinahe-Vorfall betroffen ist („erweiterter OpKoord“).*

  Grammatik: Es die OpKoord, daher „***erweiterte** OpKoord*“.

- §17 (2)

  Die in den EBs erwähnte „Threat Intelligence“ (TI), die als Datenbank bezeichnet wird, sollte besser „Threat Intelligence Platform – TIP“ genannt werden[2] - „Threat Intelligence“ ist die Information, die dort gespeichert wird. Es bietet sich hier ein Verweis auf §36 an: diese TIP könnte die IKT-Plattform sein, über die Einrichtungen Informationen zu Bedrohungen austauschen.

- §18 (1)

  Hier sollte auch das BMEIA, das derzeit auch Teil des IKDOKs ist, aufgelistet werden.

4 Pflichten

- *§29 (2) 3. den Sektor, Teilsektor und die Art der Einrichtung gemäß Anlage 1 oder 2;*

  Es ist zu erwarten, dass viele Einrichtungen in mehr als einem Sektor / Teilsektor aktiv sind, bzw. mehrfache „Art[en] der Einrichtung“ zutreffen werden. Diese Punkt muss daher auch Mehrfachnennungen erlauben.

- *§30 (1) Die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, haben in einer eigenen Datenbank **genaue und vollständige** Domänennamen-Registrierungsdaten zu sammeln*

  In der englischen Direktive steht hier „*accurate and complete*“, was besser mit „***korrekt und***

[2] https://en.wikipedia.org/wiki/Threat_Intelligence_Platform

vollständig“ zu übersetzen wäre. Das Wort „genau“ hat zwei Bedeutungen: es kann „exakt richtig“ meinen, aber auch nur dass die Angabe sehr spezifisch – aber nicht notwendigerweise korrekt – ist. Da mit dem zweiten Adjektiv „vollständig“ klar ist, dass etwa nur die Angabe des Nachnamens nicht reicht, ist bei „genau“ die Bedeutung „korrekt“ die relevante, worauf es mehr Sinn macht, gleich dieses Wort zu verwenden.

- *§34 (1) Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen CSIRT, andernfalls dem nationalen CSIRT, unverzüglich jeden erheblichen Cybersicherheitsvorfall (§ 35) zu melden.*

  Der Satz ist nicht konsistent, er sollte entweder

  „*Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen **sektoralen** CSIRT, andernfalls dem nationalen CSIRT, unverzüglich jeden erheblichen Cybersicherheitsvorfall (§ 35) zu melden.“*

  oder

  *„Wesentliche und wichtige Einrichtungen haben dem für **sie zuständigen CSIRT** unverzüglich jeden erheblichen Cybersicherheitsvorfall (§ 35) zu melden.“*

  heißen. Gibt es kein passendes sektorales CSIRT ist das nationale zuständig, d.h. es gibt immer ein „zuständiges CSIRT“.

- *§34 (2) 5. im Falle eines andauernden Cybersicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts gemäß Z 4 haben die betreffenden Einrichtungen zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Cybersicherheitsvorfalls zu übermitteln.*

  Hier ist schon die Textvorlage der NIS-2-Richtlinie nicht verständlich formuliert („*Behandlung des Cybersicherheitsvorfalls*“ ist kein Zeitpunkt, sondern ein lange dauernder Vorgang). Eine bessere Formulierung wäre etwa

  *Falls der Cybersicherheitsvorfall zum Zeitpunkt der Fälligkeit der Vorlage des Abschlussberichts gemäß Z 4 noch andauert, haben die betreffenden Einrichtungen bis zu diesem Zeitpunkt einen Fortschrittsbericht zu übermitteln. Der Abschlussbericht muss bis maximal ein Monat nach **Beendigung der Vorfallsbehandlung** übermittelt werden.*

  Oder aber (ganz verstehen wir die Intention hinter der Formulierung in der NIS-2-Richtlinie nicht):

  *Falls der Cybersicherheitsvorfall zum Zeitpunkt der Fälligkeit der Vorlage des Abschlussberichts gemäß Z 4 noch andauert, haben die betreffenden Einrichtungen bis zu diesem Zeitpunkt einen Fortschrittsbericht zu übermitteln, **wodurch sich die Frist für die Vorlage des Abschlussberichts um ein Monat nach hinten verschiebt**.*

  Welche Berichte sind etwa bei einem Cybersicherheitsvorfall, der mehr als 3 Monate andauert, zu liefern?

- *§34 (fehlt)*

  Bei der freiwilligen Meldung gilt: *§37 (3) Die Meldung kann personenbezogene Daten gemäß § 42 Abs. 2 enthalten.*

  Eine äquivalente Freigabe für die Pflichtmeldung fehlt.

5 Informationsaustausch

- §36

  Uns ist keine Rechtsvorschrift bekannt, die den in §36 definierten Informationsaustausch zwischen Einrichtungen aktuell unterbindet. Erst wenn PII Daten involviert wären, dann beschränkt die DSGVO den Datenaustausch. Wenn der Sinn hinter §36 eine Motivation für eine engere Kooperation der Einrichtungen ist, dann sollte die dadurch gegebene Datenschutzfreigabe klarer beschrieben werden, etwa durch einen Verweis auf §42 Abs. 2.

  Es sollte einen klaren Vorteil für die Einrichtungen geben, wenn sie ihre Kooperation in den Rahmen des §36 Schemas stellen. Der ist aus dem aktuellen Text nicht ersichtlich. Das könnte man etwa mit folgendem Text erreichen:

  (3) Die Cybersicherheitsbehörde unterstützt die Einrichtungen bei der Ausarbeitung von Vereinbarungen gemäß Abs. 2, insbesondere hinsichtlich der Anwendung der in § 15 Abs. 4 Z 8 genannten Konzepte. ***Wenn die verwendeten IKT-Plattformen von einem CSIRT betrieben wird, so können auch die in §42 Abs. 2 genannten Daten, wenn das zur Erreichung der in Abs. 1 genannten Ziele nötig ist, übermittelt werden.***

  Das Aufsichtsrecht des Innenministers über die CSIRTs stellt sicher, dass der Informationsaustausch kontrolliert abläuft.

- §37 (1)

  Gleicher Kommentar wie zu §34 (1): Es gibt immer ein zuständiges CSIRT. In Abs. 2 ist es richtig formuliert.

- *§37 (1) vs (2)*

  Abs. 2 enthält den Halbsatz „*das die Meldungen zusammenfasst*“, Abs. 1 aber nicht. Das sollte für alle freiwilligen Meldungen gelten.

- *§37 (2) Einrichtungen, die nicht in den Anwendungsbereich dieses Bundesgesetzes fallen, …*

  Im Gegensatz zum alten NISG ist die Formulierung hier so, dass auch Meldungen zu Vorfällen bei anderen Einrichtungen gemacht werden können. Beispiel: Es gibt einen DDoS auf Firma X, ein Kunde bemerkt das und will das melden. Das ist gut so, die Einschränkung im NISG von 2018 war ein Fehler. Damit muss der Melder aber keine Einrichtung sein, sondern könnte auch eine Privatperson sein. Damit ist eine Formulierung analog zu §8(11) angebracht.

Das zuständige CSIRT ist nicht notwendigerweise das, das für den Melder zuständig ist, sondern das, in dessen Verantwortungsbereich der Vorfall passiert ist. Das muss auch nicht notwendigerweise in einem der NIS2 Sektoren liegen. Eine Meldung zu einem Vorfall bei Dritten ist sehr nahe an einer Meldung zu einer Schwachstelle bei Dritten, daher könnte hier das nationale CSIRT – analog zur Rolle als CVD-Koordinator – mehr Sinn machen, als das „zuständige CSIRT". Etwa:

Personen und Einrichtungen, die nicht in den Anwendungsbereich dieses Bundesgesetzes fallen, können ebenfalls auf freiwilliger Basis Cybersicherheitsvorfälle, Cyberbedrohungen und Beinahe-Cybersicherheitsvorfälle an das nationale CSIRT, melden, das die Meldungen zusammenfasst und an die Cybersicherheitsbehörde weiterleitet.

In dem Zusammenhang könnte man in §37 Abs. 1 die Einschränkung auf die wesentlichen und wichtigen Einrichtungen fallen lassen, und stattdessen schreiben: *„Einrichtungen in den Sektoren laut Anlagen 1 und 2 können …"*

- *§37 (3) § 34 Abs. 2 gilt sinngemäß.*

  Das starre Meldeschema mit Fristen macht für die freiwillige Meldung, die noch dazu anonym erfolgen kann, keinen Sinn. Dieser Satz ist daher ersatzlos zu streichen.

6 Aufsicht und Durchsetzung

- *§40. Die Cybersicherheitsbehörde kann wesentliche und wichtige Einrichtungen dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Art. 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in § 32 genannter Anforderungen nachzuweisen.*

  Hier ist bereits der Text der NIS-2-Richtlinie nicht klar formuliert. Ist mit „spezielle" gemeint, dass die Behörde die Verwendung konkreter Produkte vorschreiben kann, oder ist mit „spezielle" gemeint, dass für genau genannte Zwecke Produkte/Dienste/Prozesse verwendet werden müssen, die zertifiziert sind?

  Vorschlag: *Die Cybersicherheitsbehörde kann wesentliche und wichtige Einrichtungen dazu verpflichten,* ***für spezielle Zwecke*** *IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Art. 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in § 32 genannter Anforderungen nachzuweisen.*

  Weiters, es fehlt hier ein Gebot der Verhältnismäßigkeit: wenn es etwa in einem Bereich nur ein zertifiziertes Produkt gibt, und dieses vorgeschrieben ist, wie wird hier eine Monopolisierung verhindert, die negative wirtschaftliche und sicherheitstechnische Konsequenzen hätte?