Rechnungshof
Österreich
Unabhängig und objektiv für Sie.

Bundeskanzleramt
Ballhausplatz 2
1010 Wien

Wien, 29. April 2024
GZ 2024-0.259.166

Entwurf eines Bundesgesetzes, mit dem das Netz– und Informationssystemsicherheitsgesetz 2024 – NISG 2024 erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden

Sehr geehrte Damen und Herren,

der Rechnungshof (RH) dankt für den mit Schreiben vom 3. April 2024, GZ: 2024-0.220.735, übermittelten, im Betreff genannten Entwurf und nimmt zu diesem im Rahmen des Begutachtungsverfahrens aus Sicht der Rechnungs– und Gebarungskontrolle wie folgt Stellung:

1. Allgemeine Anmerkungen

1.1 Ziel und Inhalt des Entwurfs

Mit dem vorliegenden Entwurf soll die Umsetzung der Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS–2–Richtlinie) durch Erlassung des NISG 2024 erfolgen und das bisher geltende Netz– und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018 außer Kraft treten. Die NIS–2–Richtlinie sieht dabei eine Steigerung der zu beaufsichtigenden Entitäten durch Ausweitung der betroffenen Sektoren (beispielsweise die öffentliche Verwaltung inklusive Einrichtungen der Landesverwaltung, Abwasser, Verwaltung von IKT–Diensten sowie Abfallbewirtschaftung) vor.

Der RH wertet einleitend als positiv, dass mit dem Entwurf auch eine Zusammenführung der *„derzeit extrem stark fragmentierten“*, *„auf eine Vielzahl an Ressorts aufgeteilten“* Kompetenzen zur Cybersicherheit erfolgen soll (WFA S. 4). Dabei sollen – nach den Erläuterungen – unter anderem problematische Auswirkungen auf den Verwaltungsoverhead (ressortübergreifende Prozesse durch die derzeitige Aufteilung auf mehrere Ministerien) und – da Cybersicherheit eine Querschnittsmaterie ist, die zahlreiche unterschiedliche Materien berühren kann – insbesondere negative Kompetenzkonflikte vermieden werden.

Dampfschiffstraße 2
1030 Wien

Tel.: +43 (0)1 711 71–0
office@rechnungshof.gv.at
www.rechnungshof.gv.at
Twitter: @RHSprecher
/RechnungshofAT

Kerninhalte des Entwurfs sind u.a.

- die gesetzliche Verankerung der bisher nur in der ÖSCS 2021 erwähnten Cyber Sicherheit Steuerungsgruppe als strategisches Gremium (nunmehr unter dem Vorsitz des BMI statt BKA),
- die Zusammenführung der strategischen (bisher BKA) und operativen (bisher BMI) NIS–Behörde in eine Cybersicherheitsbehörde im BMI,
- die Einführung einer Registrierungspflicht für die betroffenen wesentlichen und wichtigen Einrichtungen (an Stelle des bisherigen behördlichen Ermittlungsverfahrens) sowie
- die Verfassungsbestimmungen in den §§ 1 und 46, um die nach der Richtlinie notwendige Einbeziehung der Länder erreichen zu können.

Der RH weist einleitend darauf hin, dass der Entwurf einerseits eine Reihe von RH–Empfehlungen aus vorangegangenen Prüfungen, insbesondere aus der Prüfung „Koordination der Cybersicherheit" (Reihe Bund 2022/13) berücksichtigt. Andererseits lässt er auch eine Reihe von RH–Empfehlungen aus dem angesprochenen Bericht unberücksichtigt.

Im Einzelnen nimmt der RH wie folgt Stellung:

1.2 Zum Anwendungsbereich des NISG 2024 – § 24 des Entwurfs

(1) Gemäß der Definition der wesentlichen und wichtigen Einrichtungen in § 24 des Entwurfs sollen nach Abs. 6 dieser Bestimmung neben weiteren Einrichtungen im Sektor der öffentlichen Verwaltung (des Bundes und der Länder) auch Einrichtungen der Gesetzgebung, einschließlich der Parlamentsdirektion nicht als wesentliche oder wichtige Einrichtungen gelten, und damit vom Anwendungsbereich ausgenommen sein. Die Richtlinie (EU) 2022/2555 enthält die Möglichkeit für diese Ausnahmen in Art. 2 Abs. 7, Art. 6 Z 35 und Z 41.

Der RH ist aufgrund seiner Einrichtung als Organ des Nationalrates in Art. 122 Abs. 1 B–VG der Legisla-tive zugeordnet. Aufgrund dieser Zuordnung geht der RH davon aus, dass Rechnungshof und Volksanwaltschaft vom Anwendungsbereich des Entwurfs ausgenommen sind und regt an, eine diesbezügliche Klarstellung in den Erläuterungen vorzunehmen.

Ungeachtet dessen hält der RH fest, dass er selbstverständlich bestrebt ist, die sich aus der NIS–2–Richtlinie ergebenden notwendigen Sicherheitsmaßnahmen unter Wahrung seiner verfassungsgesetzlich vorgesehenen Unabhängigkeit zu beachten.

(2) Der RH empfahl in TZ 29 (Schlussempfehlung (SE) 38) des Berichts „Koordination der Cybersicherheit", Reihe Bund 2022/13, *„im Rahmen der Aufgaben der strategischen Koordination der Cyber–Sicherheit auf eine wirksame Einbeziehung der Länder in die gesetzlichen Verpflichtungen zur Netz– und Informationssystemsicherheit hinzuwirken*".

Gemäß § 24 Abs. 2 Z 2 des Entwurfs umfasst der Anwendungsbereich des NISG 2024 auch die Einrichtungen der öffentlichen Verwaltung auf Landesebene, die in Abs. 5 näher definiert werden. Es handelt sich jedenfalls um die Ämter der Landesregierungen und Bezirkshauptmannschaften sowie

um Einrichtungen der öffentlichen Verwaltung mit Bescheiderlassungskompetenz, die Angelegenheiten der Landesverwaltung besorgen und Rechtspersönlichkeit besitzen (ausgegliederte Einrichtungen, die hoheitlich tätig werden).

Die so vorgeschlagene Regelung wird daher im Sinn einer Berücksichtigung der genannten Empfehlung positiv bewertet.

(3) Weiters wird ausdrücklich normiert, dass Gemeinden (und Gemeindeverbände) vom Anwendungsbereich des NISG 2024 ausgeschlossen sind (§ 24 Abs. 3). Die Erläuterungen führen dazu keine Begründung an. Der Ausschluss entspricht der Richtlinie 2022/2555, die zwar die Möglichkeit, aber keine Pflicht zur Aufnahme der Einrichtungen im Sektor der öffentlichen Verwaltung „*auf lokaler Ebene*“ vorsieht.

Der RH weist dazu jedoch darauf hin, dass auf Landesebene die Bezirkshauptmannschaften (so wie auch die Ämter der Landesregierungen) per se als wichtige Einrichtungen festgelegt werden und diese bei der Wahrnehmung von Angelegenheiten der Bundesverwaltung (mittelbare Bundesverwaltung) und der Landesverwaltung die Anforderungen nach dem NISG 2024 zu erfüllen haben. Infolge der Ausnahme der Gemeinden vom Anwendungsbereich des NISG 2024 unterliegen aber Statutarstädte, die dieselben Aufgaben wie Bezirkshauptmannschaften wahrnehmen, nicht diesen Anforderungen, da sie daneben auch Gemeindeaufgaben wahrnehmen und vorrangig als Einrichtungen auf Gemeindeebene gelten.

Der RH regt daher an, die Sonderstellung der Statutarstädte zumindest in den Erläuterungen darzustellen bzw. klar darzulegen.

2. Zur Berücksichtigung von Empfehlungen des Rechnungshofes

Insbesondere vor dem Hintergrund des Berichts „Koordination der Cybersicherheit“ (Reihe Bund 2022/13) nimmt der RH zu folgenden inhaltlichen Aspekten des Entwurfs Stellung:

2.1 Einrichtung eines Cyber–Lagezentrums

Der RH empfahl in TZ 14 (SE 13) des o.a. Berichts, ein Cyber–Lagezentrum mit der für die Zwecke der Erfüllung der Aufgaben erforderlichen Infrastruktur unter Beachtung von Kosten–Nutzen–Aspekten einzurichten und dem IKDOK (und der OpKoord) zur Verfügung zu stellen. Dieses sollte aufgrund der dem Bundesminister für Inneres zukommenden Leitungsaufgaben im IKDOK (und der OpKoord) beim Bundesministerium für Inneres eingerichtet werden.

Der RH weist darauf hin, dass der Entwurf keine Bestimmungen zur Einrichtung bzw. Vorhaltung eines eigenen, dauerhaft eingerichteten und jederzeit benutzbaren Cyber–Lagezentrum für die Aufgabenerfüllung durch den IKDOK enthält. Das im Entwurf vorgesehene nationale Koordinierungszentrum (§ 6) hat hauptsächlich präventive Aufgaben im Vorfeld von Cybersicherheitsvorfällen und damit andere Aufgaben als ein Cyber–Lagezentrum, dessen Hauptaufgabe die regelmäßige Erstellung eines Lagebildes sowie die Bearbeitung von Cybersicherheitsvorfällen sein sollte.

Derzeit stehen Räumlichkeiten in einem Amtsgebäude des BMI für Lagebesprechungen des IKDOK und der OpKoord zur Verfügung und auch nach der wirkungsorientierten Folgenabschätzung (WFA) wurden Vorkehrungen für Räumlichkeiten und Ausstattung getroffen (S. 37 f) und eine Organisationseinheit mit der Aufgabe Cyber–Lagezentrum vorgesehen (S. 31 f).

Auch wenn – faktisch – die o.a. Empfehlung im Hinblick auf die Infrastruktur berücksichtigt wurde, regt der RH dennoch eine gesetzliche Festlegung eines umfassenden Cyber–Lagezentrums (Infrastruktur, erweiterte Aufgaben, siehe TZ 25 und TZ 26 des Berichts 2022/13; siehe auch Bundeslagezentrum nach § 6 Bundes–Krisensicherheitsgesetz) oder zumindest eine Klarstellung des Verhältnisses zum Bundeslagezentrum in den Erläuterungen an.

2.2 Regelmäßige Auditierung von Sicherheitsvorkehrungen

In SE 3 und 4 des o.a. Berichts empfahl der RH, die von den Bundesministerien getroffenen Sicherheitsvorkehrungen insbesondere betreffend die wichtigen Dienste regelmäßig, vergleichbar mit den Vorschriften des Netz– und Informationssystemsicherheitsgesetzes für die Betreiber wesentlicher Dienste, zumindest alle drei Jahre zu auditieren. Im Gremium Operative Koordinierungsstruktur (OpKoord) wären auch die übrigen Bundesministerien und die Länder auf die Bedeutung der regelmäßigen Sicherheitsüberprüfung ihrer wichtigen Dienste hinzuweisen.

§ 33 Abs. 2 des Entwurfs sieht nunmehr für alle wesentlichen Einrichtungen (also auch die Einrichtungen der öffentlichen Verwaltung auf Bundesebene) eine Prüfung der Umsetzung der Risikomanagement-maßnahmen (Sicherheitsvorkehrungen) durch eine unabhängige Stelle vor. Diese hat innerhalb von 2,5 bis 3,5 Jahren nach Aufforderung durch die Cybersicherheitsbehörde zu erfolgen.

Die Empfehlung wird durch die vorgeschlagene Regelung insofern teilweise berücksichtigt, da zwar eine Rechtsgrundlage für eine unabhängige Überprüfung zumindest für wesentliche Einrichtungen grundsätzlich geschaffen wurde, eine solche Überprüfung jedoch nicht automatisch, sondern erst nach entsprechender Aufforderung der Cybersicherheitsbehörde an die Bundesministerien erfolgen soll.

2.3 Gesetzliche Verankerung der Cyber Sicherheit Steuerungsgruppe

In SE 9 des genannten Berichts empfahl der RH, dass

- die Cyber Sicherheit Steuerungsgruppe – wie in ihrer Geschäftsordnung vorgesehen – mindestens zweimal im Jahr einzuberufen wäre,
- das Bundesministerium für Digitalisierung und Wirtschaftsstandort und die Länder zu diesen Sitzungen einzuladen wären und
- sicherzustellen wäre, dass regelmäßige Berichte zur Cyber–Sicherheit an die Bundesregierung, insbesondere zur Umsetzung und Weiterentwicklung ihrer strategischen Vorgaben sowie der rechtlichen Grundlagen zu Cyber–Sicherheit, erfolgen.

In § 12 des Entwurfs wird die bisher lediglich in der Österreichischen Strategie für Cybersicherheit vorgesehene Cyber Sicherheit Steuerungsgruppe gesetzlich verankert. Die für Digitalisierungs–

und Telekommunikationsangelegenheiten zuständigen Bundesministerinnen bzw. Bundesminister sind gemäß Abs. 3 ebenso als Teilnehmer vorgesehen wie Vertreter der Bundesländer, wenn der Teilnehmerkreis themenorientiert erweitert wird. In Abs. 2 Z 3 der vorgeschlagenen Regelung wird als eine der Aufgaben die Mitwirkung an der Erstellung eines jährlichen Berichts zur Cybersicherheit genannt.

Die vorgeschlagene Regelung trägt der angesprochenen Empfehlung des RH Rechnung und wird daher insofern positiv bewertet.

2.4 Evaluierung und regelmäßige Einberufung der OpKoord

In SE 12 des genannten Berichts empfahl der RH, die Aufgaben der OpKoord zu evaluieren und das Bundesministerium für Digitalisierung und Wirtschaftsstandort sowie die Länder auf geeignete Weise zu integrieren. Hierbei wäre auch festzulegen, ob die OpKoord regelmäßig oder nur im Bedarfsfall einzuberufen wäre.

§ 3 Z 33 und § 14 des Entwurfs halten die bisherige Struktur und Funktion der OpKoord aufrecht. Nach § 14 Abs. 4 des Entwurfs können Regelungen über Einberufung und Aufgaben in einer Geschäftsordnung getroffen werden.

Die vorgeschlagenen Regelungen sehen daher eine gesetzliche Grundlage für eine Berücksichtigung der o.a. Empfehlungen des RH vor.

2.5 Umsetzung weiterer Empfehlungen aus dem Bericht Reihe Bund 2022/13

Im genannten Bericht des RH wurde weiters empfohlen

- die im Aufbau befindliche „IKDOK–Plattform“ fertigzustellen, zur Lagebilderstellung einzusetzen und auch für eine gesicherte Kommunikation technisch auszugestalten (SE 16),
- zu prüfen, ob das jeweils aktuelle Cyber–Lagebild (in Form des OpKoord–Lagebildes) auch den verfassungsmäßigen Einrichtungen der Länder zur Kenntnis gebracht werden kann (SE 17) und
- dass der Bundesminister für Inneres als Vertreter Österreichs beim Aufbau des neuen EU–weiten Netzwerks CyCLONe mitwirken sollte (SE 18).

Die Berücksichtigung dieser Empfehlungen durch folgende Regelungen des vorliegenden Entwurfs

- Erlassung einer gesetzlichen Grundlage für die IKDOK–Plattform (§ 19 des Entwurfs),
- Möglichkeit zur Datenübermittlung an weitere „wesentliche und wichtige Einrichtungen“ aufgrund einer ausdrücklichen gesetzlichen Grundlage (§ 43 Abs. 3 des Entwurfs) sowie
- der in § 4 Abs. 1 Z 7 des Entwurfs verankerten Aufgabe der Cybersicherheitsbehörde, die Vertretung Österreichs im Netzwerk EU–CyCLONe wahrzunehmen; der zu erstellende nationale Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes ist auch dem EU–CyCLONe zu übermitteln (§ 16 Abs. 4 i.V.m. § 43 Abs. 3 des Entwurfs)

wird daher zusammengefasst positiv bewertet.

3. Nicht berücksichtigte Empfehlungen des Rechnungshofes

Insbesondere zu auch organisatorischen Regelungen bei der Bewältigung von Cyberkrisen weist der RH auf folgende Empfehlungen des Berichts „Koordination der Cybersicherheit“ hin, die mit dem vorliegenden Entwurf weiterhin nicht berücksichtigt werden.

3.1 SE 19, TZ 19 des Berichts – Computer–Notfallteams

Der RH empfahl in Erwägung zu ziehen, die Aufgaben des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) langfristig durch eigene Bedienstete des Bundes zu erbringen.

§ 8 Abs. 3 des Entwurfs sieht jedoch vor, sektorspezifische CSIRTS (Computer Security Incident Response Team) wie auch das GovCERT – wie bisher – zu ermächtigen. Ebenso sind in der wirkungsorientierten Folgenabschätzung (WFA) (insb. S. 41) finanzielle Aufwendungen für einen Betrieb mit der vollen Personenanzahl von 20 VBÄ (ab dem Jahr 2026) angegeben. Die dafür angegebenen Personalkosten ergeben sich nach der WFA *„daraus, wie die Personen besoldet wären, wenn sie im Bund arbeiten würden“*.

3.2 SE 29, TZ 24 des Berichts – Cyberkrisenmanagement–Koordinationsausschuss

Die SE 29 dieses Berichts lautete: *„Im Falle einer Cyber–Krise, die Systeme des Bundes bzw. von Bundesministerien betrifft, wäre der Cyberkrisenmanagement–Koordinationsausschuss auch um entscheidungsbefugte Vertreterinnen und Vertreter des Bundesministeriums für Finanzen, des Bundesministeriums für Digitalisierung und Wirtschaftsstandort und der Bundesrechenzentrum Gesellschaft mit beschränkter Haftung zu erweitern, um eine abgestimmte Vorgangsweise hinsichtlich der wichtigen bundesweiten IT–Systeme zu gewährleisten*.“

Der Entwurf sieht den Cyberkrisenmanagement–Koordinationsausschuss nicht mehr vor. Stattdessen regelt § 16 in Umsetzung von Art. 9 der RL (EU) 2022/2555 das Management von Cybersicherheitsvorfällen großen Ausmaßes. Dieses ist von der Cybersicherheitsbehörde (lt. WFA einer Abteilung innerhalb der Behörde) durchzuführen. Für die Reaktion ist ein nationaler Plan zu erstellen. Dieser Plan soll die Aufgaben, Zuständigkeiten und Verfahren der Behörden enthalten und die Integration in das allgemeine Krisenmanagement beschreiben.

Damit wird die konkrete Ausgestaltung des Cyberkrisenmanagements nicht gesetzlich geregelt, sondern einem „Plan“ vorbehalten. Dieser soll nach § 15 Abs. 3 Z 11 des Entwurfs Bestandteil der ÖSCS werden.

Die Empfehlung wurde somit nicht umgesetzt. Im Gegenteil soll die bisherige gesetzliche Regelung (siehe insb. § 14 NISG zum CSIRTs–Netzwerk) aufgegeben und im Gesetz lediglich auf den von der EU geforderten nationalen Plan und die nationale Strategie (ÖSCS) verwiesen werden.

3.3 SE 30, TZ 25 des Berichts – Cyber–Einsatzteam

Die Empfehlung des RH lautete: „*Ein permanent verfügbares Cyber–Einsatzteam (Rapid Response Team) wäre zu schaffen; dies in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam*."

Der Entwurf sieht kein solches Einsatzteam vor. Das nationale CSIRT sowie das GovCERT sind nur „gegebenenfalls" (vgl. § 8 Abs. 1 Z 3 i.V.m. Abs. 2 und 4 des Entwurfs) zur Unterstützung bei der Bewältigung von Cybersicherheitsvorfällen zuständig. Auch die Erläuterungen zu dieser Bestimmung führen auf S. 15 aus, dass CSIRTs nur in Ausnahmefällen „*nach Möglichkeit und Ermessen auch vor Ort eine technische Unterstützung leisten*" können.

Der RH betont auch aus Anlass der vorliegenden Begutachtung, dass er ein permanent eingerichtetes Cyber–Einsatzteam zur effizienten Bewältigung von Cyber–Sicherheitsvorfällen für erforderlich erachtet.

3.4 SE 33, TZ 26 des Berichts – Cyber–Sicherheitsleitstelle

Die Empfehlung des RH lautete: „*Eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale wäre einzurichten und das Cyber–Einsatzteam (Rapid Response Team) dort zu integrieren*."

Der RH weist darauf hin, dass der Entwurf weder die Einrichtung eines Cyber–Sicherheitszentrums noch eines Cyber Security Operations Centers (SOC) oder Rapid Response Teams ausdrücklich vorsieht.

Dem gemäß § 6 des Entwurfs geplanten nationalen Koordinierungszentrum sind vorwiegend generelle, langfristige, präventive und strategische Aufgaben nach der EU–Verordnung 2021/887 (etwa die Förderung von Forschung und Innovation, Information der Öffentlichkeit und Beratungsaufgaben) nicht aber die Aufgaben einer Cyber–Sicherheitsleitstelle (inklusive Einsatzzentrale und Einsatzteam für akute Vorfälle) zugewiesen.

Demgegenüber bezeichnet die WFA jedoch die Cybersicherheitsbehörde im BMI als „Nationales Cybersicherheitszentrum", das in der Sektion IV installiert werden soll. Teil davon soll auch ein Referat mit der Bezeichnung „SOC–Plattform" sein. Dieses soll die IKT–Lösungen, z.B. Frühwarnsystem betreiben. Nach den Erläuterungen sind jedoch die SOCs der Teilnehmer jeweils für die Analyse zuständig.

Nach Ansicht des RH sind die Aufgaben der SOC–Plattform daher so ausgestaltet, dass diese zwar zur Bereitstellung von Informationen, aber nicht zur Koordination und zum Einsatz im Sinne einer Leitstelle herangezogen werden soll.

4. Berührungspunkte zum Bundes–Krisensicherheitsgesetz

Hinsichtlich der wesentlichen Änderungen zum Cyberkrisen–Management (Abschaffung des Koordinationsausschusses, Aufhebung gesetzlicher Regelungen dazu, nationaler Plan im Sinne der Richtlinie als Grundlage) weist der RH darauf hin, dass gerade für Cyberkrisen eine klare gesetzliche Regelung unabdingbar ist. Wie bereits in der (beiliegenden) Stellungnahme des RH zum Entwurf eines Bundes–Krisensicherheitsgesetzes (17237/SN–245/ME) ausgeführt, müssen Abgrenzungsfragen zum Bundes–Krisensicherheitsgesetz geklärt werden. Diese Abgrenzung sollte auch in eindeutigen Gesetzesbestimmungen zum Ausdruck kommen.

Der Begriff „Cyberkrise“ wird offenbar durch den Begriff des „Cybersicherheitsvorfalls großen Ausmaßes“ ersetzt. Dieser ist aber – entsprechend der Richtlinie – so definiert (§ 3 Z 31), dass er die Reaktionsfähigkeit eines Mitgliedstaates der Europäischen Union übersteigt oder beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat. Damit würden rein österreichische Cyberkrisen nicht darunterfallen. Es besteht daher das Risiko, dass solche auf Österreich beschränkte Krisen vom Gesetzesentwurf nicht als „Cybersicherheitsvorfälle großen Ausmaßes“ erfasst wären. Zumindest in den Erläuterungen sollte eine Klarstellung erfolgen, ob diese Cyberkrisen nunmehr nach den Verfahren des Bundes–Krisensicherheitsgesetzes zu bewältigen wären.

5. Zusammenfassende Bemerkung

Vor dem Hintergrund seiner Begutachtung fasst der RH zusammen, das der Entwurf einerseits eine Reihe seiner Empfehlungen aus dem Bericht „Koordination der Cybersicherheit“ (Reihe Bund 2022/13) berücksichtigt, andererseits aber auch eine Reihe von Empfehlungen aus dem angesprochenen Bericht unberücksichtigt lässt.

Insbesondere angesichts der nicht umgesetzten Empfehlungen weist der RH auf Folgendes hin:

Die Empfehlungen zum Aufbau eines Rapid Response Teams, Security Operations Centers und einer Cyber–Sicherheitsleitstelle (TZ 25 und TZ 26) werden durch den Entwurfstext nicht ausdrücklich aufgegriffen; in den Erläuterungen (inkl. WFA) werden nur die ersten Schritte erwähnt (Entwicklung von IKT–Lösungen, SOC–Plattform, Frühwarnsystem). Ein wie vom RH als erforderlich erachtetes Rapid Response Team für die Verwaltung wird durch den vorliegenden Entwurf jedenfalls nicht eingerichtet. Wie weit die Umsetzung der IKT–Lösungen in der Praxis reichen wird (insbesondere wie viele Einrichtungen sich an diesen IKT–Lösungen beteiligen werden), kann im Rahmen des Begutachtungsverfahrens noch nicht beurteilt werden.

Der RH weist ausdrücklich darauf hin, dass die möglichst rasche Umsetzung insbesondere dieser Empfehlungen eine wichtige infrastrukturelle Maßnahme darstellen würde; dies angesichts der Tatsache, dass jederzeit mit Cyber–Vorfällen zu rechnen ist, die mit größtmöglicher Effizienz zu bekämpfen sind.

6. Finanzielle Auswirkungen der Risikomanagementmaßnahmen – § 32 des Entwurfs

Der RH weist einleitend darauf hin, dass die „Anlage 3: Risikomanagementmaßnahmen Bereiche“ deutlich mehr Aspekte umfasst, als in der NIS–2–Richtlinie vorgesehen. Nach Ansicht des RH kann infolge der Umsetzung dieser Maßnahmen durch die wesentlichen und wichtigen Einrichtungen ein Mehraufwand entstehen.

Bei der Bewertung der verhältnismäßigen Umsetzung von Risikomanagementmaßnahmen nach § 32 Abs. 3 des Entwurfs sind Faktoren wie das Ausmaß der Risikoexposition der Einrichtung sowie ihrer Dienste, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Cybersicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen gebührend zu berücksichtigen. Da somit für die Bewertung der Verhältnismäßigkeit hinsichtlich der Umsetzung von Risikomanagementmaßnahmen keine klaren Vorgaben vorliegen, können die für die

Umsetzung dieser Risikomanagementmaßnahmen erforderlichen Ressourcen derzeit nicht abgeschätzt werden. Eine diesbezügliche Präzisierung wird daher angeregt.

Nach § 32 Abs.ç4 des Entwurfs hat der Bundesminister für Inneres mit Verordnung die Risikomanagementmaßnahmen in den Bereichen der Anlage 3 hinsichtlich technischer, operativer und organisatorischer Anforderungen präzisierend festzulegen. Der RH weist daher aus Anlass der vorliegenden Begutachtung darauf hin, eine entsprechende Abschätzung hinsichtlich der für die Umsetzung erforderlichen Ressourcen– sowohl personell, finanziell als auch zeitlich – bei der Erlassung der entsprechenden Verordnung vorzunehmen.

Von dieser Stellungnahme wird jeweils eine Ausfertigung dem Präsidium des Nationalrates und dem Bundesministerium für Finanzen übermittelt.

Mit freundlichen Grüßen

Die Präsidentin:
Dr. Margit Kraker

F.d.R.d.A.:
Daniela Pristusek

1 Beilage

Republik Österreich Rechnungshof Österreich @AMTSSIGNATUR	**Unterzeichner/ Siegelersteller**	Rechnungshof
	Datum/Zeit-UTC	2024-04-29T14:54:12+02:00
	Aussteller-Zertifikat	a-sign-corporate-light-02
	Serien-Nr.	28250739
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.rechnungshof.gv.at/ueber-den-rh/amtssignatur.html
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	