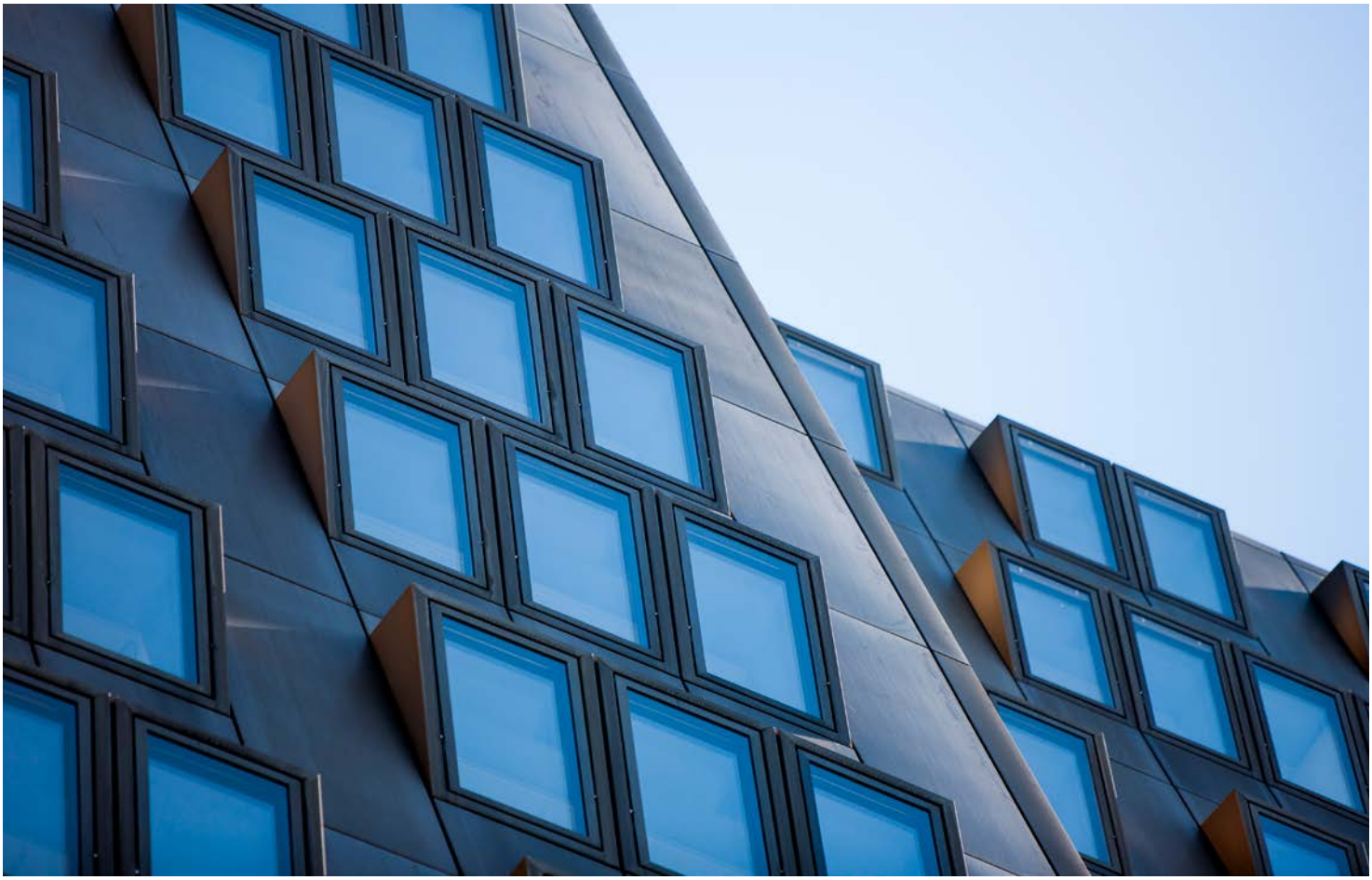
Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Koordination der Cyber–Sicherheit; Follow–up–Überprüfung

Reihe BUND 2024/28

Bericht des Rechnungshofes



III–1228 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP
Rechnungshof GZ 2024–0.691.310 (005.199)

Vorbemerkungen

Vorlage

Der Rechnungshof erstattet dem Nationalrat gemäß Art. 126d Abs. 1 Bundes–Verfassungsgesetz nachstehenden Bericht über Wahrnehmungen, die er bei einer Gebarungsüberprüfung getroffen hat.

Berichtsaufbau

In der Regel werden bei der Berichterstattung punkteweise zusammenfassend die Sachverhaltsdarstellung (Kennzeichnung mit 1 an der zweiten Stelle der Textzahl), deren Beurteilung durch den Rechnungshof (Kennzeichnung mit 2), die Stellungnahme der überprüften Stelle (Kennzeichnung mit 3) sowie die allfällige Gegenäußerung des Rechnungshofes (Kennzeichnung mit 4) aneinandergereiht.

Das in diesem Bericht enthaltene Zahlenwerk beinhaltet allenfalls kaufmännische Auf– und Abrundungen.

Der vorliegende Bericht des Rechnungshofes ist nach der Vorlage über die Website des Rechnungshofes www.rechnungshof.gv.at verfügbar.

IMPRESSUM
Herausgeber:
Rechnungshof Österreich
1030 Wien, Dampfschiffstraße 2
www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im Oktober 2024

AUSKÜNFTE
Rechnungshof
Telefon (+43 1) 711 71 – 8946
E–Mail info@rechnungshof.gv.at
facebook/RechnungshofAT
Twitter: @RHSprecher

FOTOS
Cover, S. 5: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
Art.	Artikel
BGBl.	Bundesgesetzblatt
BKA	Bundeskanzleramt
BMI	Bundesministerium für Inneres
bzw.	beziehungsweise
CERT	Computer Emergency Response Team (Computer–Notfallteam)
CSS	Cyber Sicherheit Steuerungsgruppe
EU	Europäische Union
(f)f.	folgend(e)
GovCERT	Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung)
i.d.(g.)F.	in der (geltenden) Fassung
IKDOK	Innerer Kreis der Operativen Koordinierungsstruktur
IKT	Informations– und Kommunikationstechnologie
IT	Informationstechnologie
NIS	Netz– und Informationssystemsicherheit
NISG	Netz– und Informationssystemsicherheitsgesetz
OpKoord	Operative Koordinierungsstruktur
RH	Rechnungshof
RIVIT	Richtverwendungen für den IT–Bereich
S.	Seite
TZ	Textzahl
u.a.	unter anderem
Z	Ziffer
z.B.	zum Beispiel

Um die Cyber–Sicherheit als Grundlage einer sicheren Informationstechnologie in allen staatlichen und privatwirtschaftlichen Sektoren zu gewährleisten, ist ihre Koordination von entscheidender Bedeutung. Seit dem Vorbericht des RH zur Koordination der Cyber–Sicherheit (Reihe Bund 2022/13) ist die neue EU–Cyber–Sicherheits–Richtlinie NIS–2 in Kraft getreten, die ab Oktober 2024 umzusetzen ist. Sie erweitert den Kreis der Unternehmen und öffentlichen Einrichtungen, die zu Sicherheitsmaßnahmen und Meldungen bei Sicherheitsvorfällen verpflichtet sind. Es ist daher mit einer Zunahme der koordinativen Aufgaben zu rechnen.

Das Bundeskanzleramt und das Innenministerium evaluierten die Aufgaben der Operativen Koordinierungsstruktur (OpKoord), eines zentralen Gremiums im Bereich Cyber–Sicherheit. Sie banden das für Digitalisierung zuständige Finanzministerium sowie die Länder in die Aufgaben der OpKoord ein. Ein permanentes Cyber–Lagezentrum, welches das Cyber–Lagebild erstellte und erörterte, war eingerichtet, ebenso die IT–Anwendung „IKDOK–Plattform“, die zur Bearbeitung des Cyber–Lagebildes diente.

Andere Empfehlungen waren jedoch erst teilweise oder noch nicht umgesetzt: So hatten das Bundeskanzleramt und das Innenministerium die Koordinierungsstrukturen seit dem Vorbericht nur teilweise weiterentwickelt. Es existierte nach wie vor kein Gesamtüberblick über die wichtigen Dienste der Bundeseinrichtungen. Damit konnten weder die Koordinierungsgremien noch das Cyber–Krisenmanagement auf einen solchen Gesamtüberblick zurückgreifen. Auch ein Cyber–Einsatzteam (Rapid Response Team) in Abstimmung mit dem Verteidigungsministerium und eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale gab es noch nicht. Das Frühwarnsystem zur Erkennung und Analyse von Cyber–Angriffen und das Meldeanalysesystem für Meldungen über Cyber–Risiken, –Vorfälle und –Sicherheitsvorfälle waren noch nicht fertiggestellt.

WIRKUNGSBEREICH

- Bundeskanzleramt
- Bundesministerium für Inneres

Koordination der Cyber–Sicherheit; Follow–up–Überprüfung

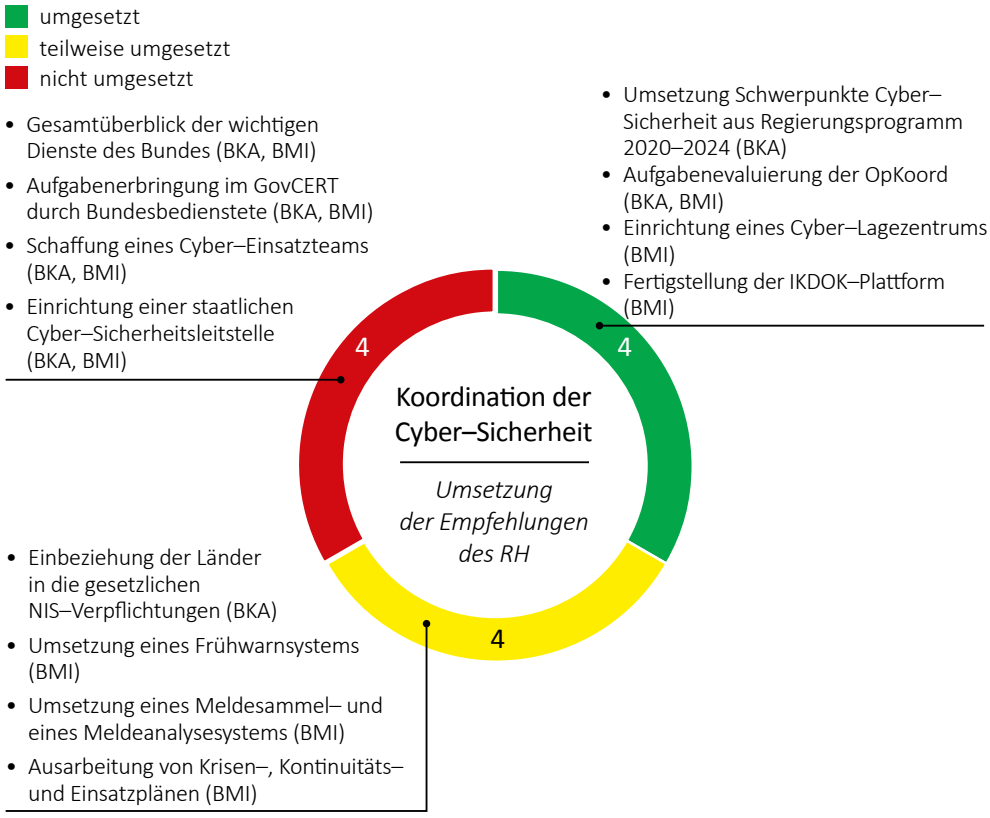
Prüfungsziel

Der RH überprüfte von September bis November 2023 das Bundeskanzleramt und das Bundesministerium für Inneres, um den Stand der Umsetzung von Empfehlungen aus seinem Vorbericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13) zu beurteilen.

Kurzfassung

Das Bundeskanzleramt setzte von acht überprüften Empfehlungen des Vorberichts zwei um, zwei teilweise um und vier nicht; das Bundesministerium für Inneres (in der Folge: **Innenministerium**) setzte von neun überprüften Empfehlungen des Vorberichts drei um, drei teilweise um und drei nicht. (TZ 15)

Abbildung 1: Umsetzungsstand ausgewählter Empfehlungen aus dem Vorbericht



Empfehlungen an mehrere Adressaten werden in dieser Abbildung nur einmal gezählt. In der Darstellung der Schlussempfehlungen (TZ 15) werden sie je Adressat nach Umsetzungsgrad dargestellt.

Quelle und Darstellung: RH

Gremien der operativen Cyber–Koordination

Die Struktur der operativen Cyber–Koordination bestand aus einem „inneren Kreis“ und einem „äußeren Kreis“:

- dem Inneren Kreis der Operativen Koordinierungsstruktur (**IKDOK**) und
- der Operativen Koordinierungsstruktur (**OpKoord**).

Gesamtüberblick über die wichtigen IT–gestützten Dienste des Bundes

Das Bundeskanzleramt setzte die Empfehlung des RH nicht um, einen Gesamtüberblick über die wichtigen Dienste des Bundes zu erstellen. Laut Bundesministeriengesetz war das Bundeskanzleramt u.a. zuständig für die Koordination der gesamten Verwaltung des Bundes und laut Netz– und Informationssystemsicherheitsgesetz (**NISG**) der Bundeskanzler für den Betrieb des Computer–Notfallteams der öffentlichen Verwaltung (**GovCERT**). Mangels Gesamtüberblick konnte die Information über die wichtigen Dienste weder im IKDOK und im GovCERT noch in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement berücksichtigt werden. (TZ 3)

Umsetzung des Regierungsprogramms 2020–2024

Das Bundeskanzleramt bereitete im überprüften Zeitraum drei von mehreren Projekten zum Schwerpunkt Cyber–Sicherheit aus dem Regierungsprogramm 2020–2024 für die Bundesregierung zur Umsetzung vor:

- staatliches Cybersicherheitszentrum,
- Aktualisierung der österreichischen Cybersicherheitsstrategie,
- zentrales, beratendes und zertifizierendes Organ in Informationssicherheitsfragen entsprechend dem Cyber Security Act der EU–Kommission und
- Einführung verbindlicher, überprüfbarer und durchsetzbarer Sicherheitsstandards im Rahmen der geltenden NIS–Richtlinie im öffentlichen Sektor.

Damit setzte das Bundeskanzleramt die Empfehlung zur Vorbereitung von weiteren Beschlüssen und Projekten zur Cyber–Sicherheit um. (TZ 4)

Aufgaben der Operativen Koordinierungsstruktur (OpKoord)

Das Bundeskanzleramt und das Innenministerium evaluierten im Jahr 2022 die Aufgaben der OpKoord. Als Ergebnis arbeiteten sie u.a. eine Geschäftsordnung für IKDOK und OpKoord aus. Sitzungen der OpKoord fanden nach wie vor zeitgleich mit jenen des IKDOK statt, weil derselbe Personenkreis die Agenden der in IKDOK bzw. OpKoord vertretenen Computer–Notfallteams wahrnahm. Darüber hinaus gab es auch anlassbezogene erweiterte OpKoord–Sitzungen.

Das Bundesministerium für Finanzen und die Länder waren nicht ständig und unmittelbar in die OpKoord eingebunden. Der operative IT–Dienstleister des Bundesministeriums für Finanzen wurde jedoch zu erweiterten OpKoord–Sitzungen eingeladen,

und der IKDOK informierte die Länder in einem monatlichen Briefing über das aktuelle OpKoord–Lagebild. Damit setzten das Bundeskanzleramt und das Innenministerium die entsprechende Empfehlung um. (TZ 5)

Cyber–Lagezentrum

Das Innenministerium richtete entsprechend der Empfehlung des RH ein aus mehreren Besprechungs– und Büroräumen bestehendes Cyber–Lagezentrum in einem seiner Amtsgebäude ein, um es dem IKDOK (und der OpKoord) zur Verfügung zu stellen. Kosten–Nutzen–Aspekte berücksichtigte es insofern, als die Räume den Dienststellen des Innenministeriums auch im Regelbetrieb als Besprechungsräume und Büros zur Verfügung standen und laufend genutzt wurden. (TZ 6)

IT–Anwendung IKDOK–Plattform

Ebenfalls umgesetzt war die Empfehlung, die im Aufbau befindliche IT–Anwendung „IKDOK–Plattform“ fertigzustellen, zur Lagebilderstellung einzusetzen und für eine gesicherte Kommunikation technisch auszugestalten. Das Innenministerium stellte die – von einem Dienstleistungsunternehmen errichtete und betriebene – IT–Anwendung „IKDOK–Plattform“ dem IKDOK und der OpKoord zur Zusammenarbeit zur Verfügung. Die IKDOK–Plattform war ein Paket aus mehreren IT–Applikationen: Diese umfassten die Funktionen Benachrichtigung, Informationsweitergabe und Diskussion, E–Mail–Verschlüsselung, Datenaustausch und –ablage sowie gemeinsame Erstellung und Bearbeitung von Dokumenten. (TZ 7)

Bundesbedienstete im Computer–Notfallteam der öffentlichen Verwaltung (GovCERT)

Entgegen der Empfehlung des RH wurden die Aufgaben des GovCERT nach wie vor nicht von Bediensteten des Bundes wahrgenommen. Laut Bundeskanzleramt seien mit den besoldungsrechtlichen Voraussetzungen im Bundesdienst Cyber–Sicherheits–Spezialistinnen und –Spezialisten schwer rekrutierbar; auf sich laufend ändernde Anforderungen im Bereich der Cyber–Sicherheit könne das Bundeskanzleramt mit zugekauften Leistungen flexibler reagieren. Dem RH war die Schwierigkeit, qualifiziertes Fachpersonal zu rekrutieren, bewusst. Er erachtete jedoch die Cyber–Sicherheit als eine staatliche Kernaufgabe, die öffentlich Bedienstete erfüllen sollten. (TZ 8)

Frühwarnsystem

Das Innenministerium hatte bis November 2023 noch kein Frühwarnsystem (Sensornetzwerk) implementiert. Nach Abschluss der Konzepterstellung Ende des dritten Quartals 2023 sollte das Umsetzungsprojekt im November 2023 gestartet werden. Damit setzte das Innenministerium die Empfehlung teilweise um, das Projekt zur Implementierung des Frühwarnsystems (Sensornetzwerk) verstärkt zu betreiben und umzusetzen. (TZ 9)

Meldeanalysesystem

Teilweise umgesetzt war die Empfehlung zum Meldesammelsystem und zum Meldeanalysesystem. Diese Systeme dienten zur Sammlung, Analyse und Bewertung von (Sicherheits–)Vorfällen. Das Meldesammelsystem wurde seit Juli 2021 verwendet. Damit war auch die Grundfunktion einer Meldeanalyse umgesetzt. Das Innenministerium plante, die Meldeanalyse durch eine – in einem EU–geförderten Projekt zu entwickelnde – Softwarelösung zu verbessern und zu ersetzen. Das Projektende für das Meldeanalysesystem war für Ende August 2024 vorgesehen. (TZ 10)

Cyber–Einsatzteam

Das Bundeskanzleramt und das Innenministerium richteten – entgegen der Empfehlung des RH – kein Cyber–Einsatzteam in Abstimmung mit dem im Bundesministerium für Landesverteidigung (in der Folge: **Verteidigungsministerium**) geplanten Cyber–Einsatzteam ein. Laut Bundeskanzleramt gab es diesbezüglich Planungen und Arbeiten im Verteidigungsministerium. Dort habe die jüngste Organisationsreform die organisatorischen Grundlagen für Cyber–Einsatzteams geschaffen. Das Innenministerium verwies auf die unterschiedlichen Ziele und die Ressourcenlage in den Ministerien bzw. in deren für Cyber–Sicherheit zuständigen Organisationseinheiten, sodass derzeit kein eigenes Cyber–Einsatzteam eingerichtet werden könne. (TZ 11)

Krisen–, Kontinuitäts– und Einsatzpläne

Das Bundeskanzleramt und das Innenministerium setzten die Empfehlung um, konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement auszuarbeiten: Eine Geschäftsordnung zur Regelung der Zusammenarbeit im Rahmen von IKDOK und OpKoord vom Juli 2023 sah Kooperationsstufen für das Ausmaß der Zusammenarbeit vor – vom Regelbetrieb bis zum Vorliegen einer Cyberkrise. Zur näheren Definition arbeitete das Innenministerium Standardhandlungsanweisungen aus; der Entwurf war noch nicht beschlossen. Für das Cyber–Krisenmanagement hiel-

ten die in IKDOK und OpKoord vertretenen Ressorts und Organisationen materielle und personelle Ressourcen bereit. (TZ 12)

Cyber–Sicherheitsleitstelle

Weiter offen war die Empfehlung des RH an das Bundeskanzleramt und das Innenministerium, eine staatliche Cyber–Sicherheitsleitstelle einzurichten. Sie verwiesen auf die im Zuge der Umsetzung der NIS–2–Richtlinie geplante Organisationsentwicklung: Diese sah vor, ein staatliches Cyber–Sicherheitszentrum einzurichten, das auch die Aufgaben einer Cyber–Sicherheitsleitstelle wahrnehmen sollte. Das Innenministerium teilte mit, dass sich die Koordinationsaufgaben einer Cyber–Sicherheitsleitstelle erst bei Einrichtung eines Cyber–Einsatzteams (TZ 11) und des Frühwarnsystems (TZ 9) ergeben würden. (TZ 13)

Einbeziehen der Länder in gesetzliche Verpflichtungen zur Netz– und Informationssystemsicherheit (NISG)

Im Zuge der bisherigen Vorarbeiten zur rechtlichen Umsetzung der NIS–2–Richtlinie führte das Bundeskanzleramt bilaterale Gespräche mit Stakeholdern wie der Wirtschaftskammer Österreich. Die Länder wurden in der Phase der Vorarbeiten vor allem im Rahmen von Vorträgen informiert; vor dem Hintergrund des seit September 2023 vorliegenden Gesetzesentwurfs fanden ab 2024 Abstimmungsgespräche und eine legistische Arbeitsgruppe unter Einbeziehung der Länder statt.

Zu den Sitzungen der Cyber Sicherheit Steuerungsgruppe (Steuerungsgruppe–CSS) waren die Länder seit 2021 nicht eingeladen, obwohl die Geschäftsordnung die Möglichkeit dazu vorsah. An der Informationsdrehscheibe des GovCERT nahmen nunmehr Vertreterinnen und Vertreter aus allen Ländern teil. Am CERT–Verbund Austria nahm Wien teil; es war das einzige Land mit einem eigenen Computer–Notfallteam (Computer Emergency Response Team – CERT). Das Bundeskanzleramt setzte damit die Empfehlung zur Einbeziehung der Länder in die gesetzlichen NIS–Verpflichtungen teilweise um. (TZ 14)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

EMPFEHLUNGEN

Bundeskanzleramt

- Die Länder wären zu den Sitzungen der Cyber Sicherheit Steuerungsgruppe einzuladen; dies insbesondere im Hinblick auf die Verpflichtungen, die sich für die Länder aus der Umsetzung der NIS–2–Richtlinie künftig ergeben. (TZ 14)

Bundesministerium für Inneres

- Der Entwurf der Standardhandlungsanweisungen, die die Kooperationsstufen für das Ausmaß der Zusammenarbeit zwischen Innerem Kreis der Operativen Koordinierungsstruktur (IKDOK) und Operativer Koordinierungsstruktur (OpKoord) konkretisieren, wäre möglichst rasch einer Beschlussfassung im IKDOK zuzuführen. (TZ 12)

Bundeskanzleramt; Bundesministerium für Inneres

- In Ergänzung zum permanenten Cyber–Lagezentrum im Bundesministerium für Inneres (TZ 6) wäre auch ein permanent verfügbares nationales Cyber–Einsatzteam in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam zu schaffen. (TZ 11)

- In Zusammenarbeit mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport – dem für Personal des Bundes und daher auch für Fragen der Besoldung zuständigen Ministerium – wären Lösungsansätze für eine Rekrutierung von Cyber–Sicherheits–Expertinnen und –Experten zu erarbeiten. (TZ 11)

- Eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale wäre einzurichten. Im Hinblick auf die laufenden Arbeiten zur Umsetzung der NIS–2–Richtlinie, in deren Rahmen auch die Einrichtung eines Cyber–Sicherheitszentrums geplant ist, sollte die Integration der Aufgaben einer Cyber–Sicherheitsleitstelle in eine derartige Einrichtung berücksichtigt werden. (TZ 13)

Zahlen und Fakten zur Prüfung

Koordination der Cyber–Sicherheit; Follow–up–Überprüfung	
wichtige Rechtsgrundlagen und Vorgaben	• Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen in der Union, ABl. L 2016/194, 1 i.d.g.F.; wird mit Wirkung vom 18. Oktober 2024 aufgehoben • Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheits-niveau in der Union (NIS–2–Richtlinie), ABl. L 2022/333, 80; anzuwenden ab 18. Oktober 2024 • Netz– und Informationssystemsicherheitsgesetz (NISG), BGBl. I 111/2018 • Netz– und Informationssystemsicherheitsverordnung (NISV), BGBl. II 215/2019 • Österreichische Strategie für Cyber Sicherheit 2021, Ministerratsbeschluss vom 22. Dezember 2021
wichtige Organisations-einheiten für Cyber–Sicherheit	• Cyber Sicherheit Steuerungsgruppe (Steuerungsgruppe–CSS) • Koordinationsausschuss im Cyberkrisenmanagement (CKM–KA) • Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK) • Operative Koordinierungsstruktur (OpKoord) • Computer–Notfallteams (CERT)
Abstufungen der Cyber–Sicherheits–Gefährdungen (Definitionen laut NISG)	
Risiko	alle Umstände oder Ereignisse, die **potenziell** nachteilige Auswirkungen auf die Sicherheit von Netz– und Informationssystemen haben
Vorfall	alle Ereignisse, die **tatsächlich** nachteilige Auswirkungen auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen haben und kein Sicherheitsvorfall sind
Sicherheitsvorfall	eine **Störung** der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat
Krise	ein oder mehrere Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwer-wiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können

Quellen: BKA; BMI

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von September bis November 2023 im Bundeskanzleramt sowie im Bundesministerium für Inneres (in der Folge: **Innenministerium**) die Umsetzung ausgewählter Empfehlungen, die er bei der vorangegangenen Gebarungsüberprüfung „Koordination der Cyber–Sicherheit“ abgegeben hatte. Der in der Reihe Bund 2022/13 veröffentlichte Bericht wird in der Folge als Vorbericht bezeichnet. Der überprüfte Zeitraum der Follow–up–Überprüfung umfasste im Wesentlichen die Jahre 2021 bis 2023 sowie – sofern für die Beurteilung relevant – auch aktuellere Entwicklungen.

(2) Zur Verstärkung der Wirkung seiner Empfehlungen hatte der RH deren Umsetzungsstand bei den überprüften Stellen nachgefragt. Das Ergebnis dieses Nachfrageverfahrens findet sich auf der Website des RH (www.rechnungshof.gv.at).

Der RH weist in diesem Zusammenhang auf seine geübte Vorgehensweise und standardisierte Berichtsstruktur für Follow–up–Überprüfungen hin. Diese haben das Ziel, den Umsetzungsstand von ausgewählten Empfehlungen des Vorberichts unter Berücksichtigung der Angaben aus der Nachfrage zum Umsetzungsstand der Empfehlungen zu beurteilen und die Einstufung in „umgesetzt“, „teilweise umgesetzt“, „zugesagt“ und „nicht umgesetzt“ zu begründen.

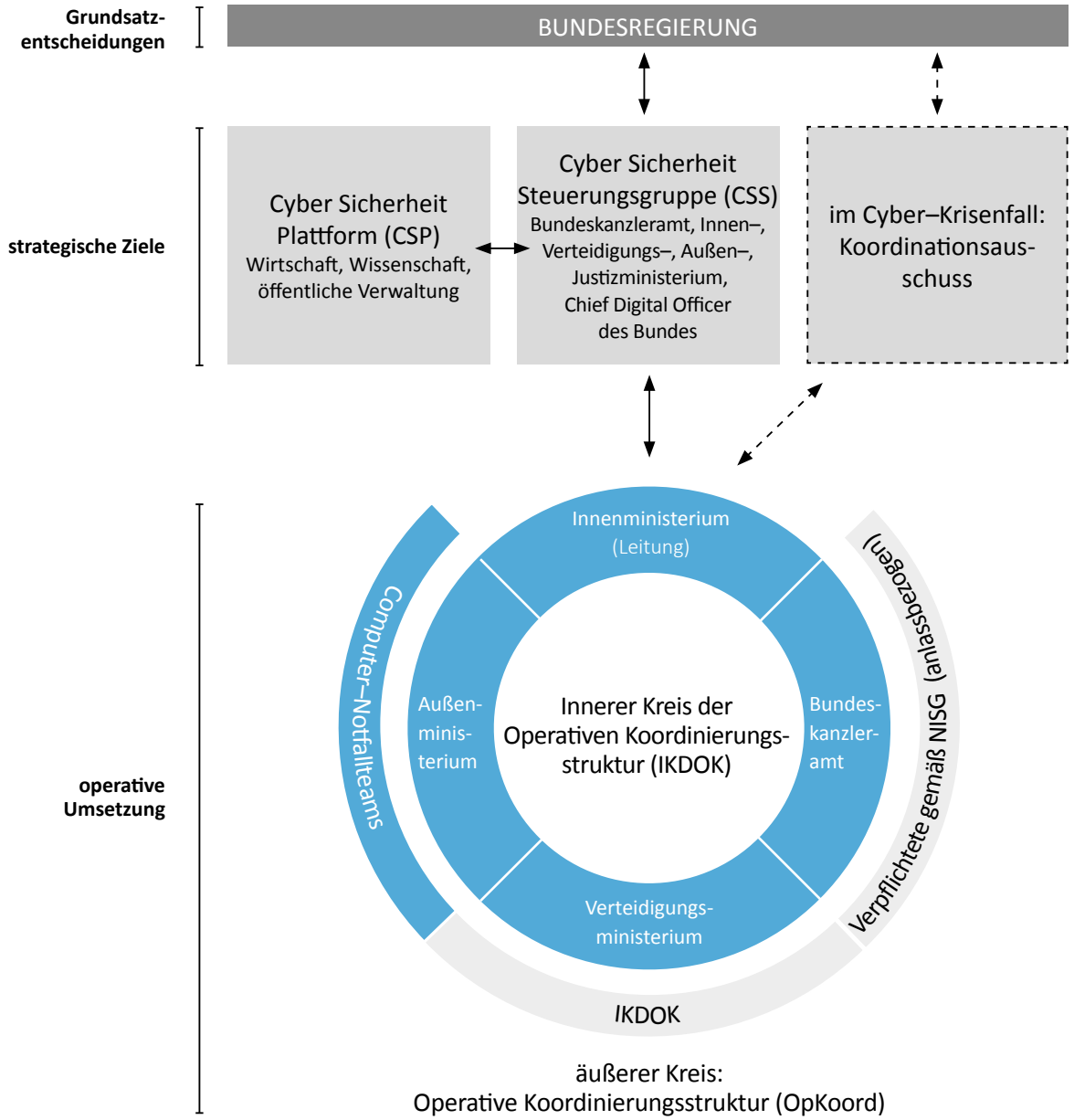
Bei den ausgewählten Empfehlungen handelte es sich insbesondere um die zentralen Empfehlungen des Vorberichts; weitere Schwerpunkte lagen darauf, die Umsetzung von Empfehlungen zur operativen Cyber–Koordination sowie zum Vorfalls– und Krisenmanagement zu überprüfen.

(3) Zu dem im April 2024 übermittelten Prüfungsergebnis nahmen das Bundeskanzleramt und das Innenministerium im Juli 2024 Stellung. Der RH erstattete seine Gegenäußerung im Oktober 2024.

Gremien zur Koordination der Cyber–Sicherheit

2 Die grundsätzliche Struktur der Gremien zur Koordination der Cyber–Sicherheit in Österreich stellte sich wie folgt dar:

Abbildung 2: Organisation der Cyber–Sicherheit gemäß Netz– und Informationssystemsicherheitsgesetz (NISG)



Quellen: BKA; BMI; Darstellung: RH

Gesamtüberblick über die wichtigen Dienste des Bundes

3.1 (1) Das Netz– und Informationssystemsicherheitsgesetz[1] (**NISG**) verpflichtete – über den Anwendungsbereich der NIS–Richtlinie[2] hinaus – auch Einrichtungen der öffentlichen Verwaltung des Bundes (insbesondere Bundesministerien) zu Sicherheitsvorkehrungen bei ihren mittels Netz– und Informationssystemen erbrachten wichtigen Diensten und zur Meldung von Sicherheitsvorfällen. Welche Dienste wichtig waren, identifizierten die Einrichtungen gemäß NISG selbst. Laut den Feststellungen des Vorberichts (TZ 4) hatte das Bundeskanzleramt einen (unverbindlichen) Umsetzungsleitfaden zur Beurteilung der wichtigen Dienste erstellt und den Einrichtungen des Bundes zur Verfügung gestellt; im Jahr 2019 hatte es eine Initiative gestartet, um die wichtigen Dienste zu erheben.

Wesentliche Aufgaben im Rahmen der Cyber–Sicherheit erbrachten im Bund u.a. der Innere Kreis der Operativen Koordinierungsstruktur (**IKDOK**) und das Computer–Notfallteam der öffentlichen Verwaltung (**GovCERT**). Der RH hatte dem Bundeskanzleramt in seinem Vorbericht (TZ 4) empfohlen, in Zusammenarbeit mit dem Innenministerium den operativen Gremien IKDOK und GovCERT einen Gesamtüberblick über die wichtigen Dienste des Bundes zur Kenntnis zu bringen und diesen in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement zu berücksichtigen.

(2) Laut Mitteilung des Bundeskanzleramts im Nachfrageverfahren sei für die Koordination der operativen Cyber–Sicherheit das Innenministerium zuständig; auch Krisen–, Kontinuitäts– und Einsatzpläne würden in die Zuständigkeit des Innenministeriums fallen.

Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, es habe dem Bundeskanzleramt als dem zuständigen obersten Organ Unterstützung zugesagt. Allfällige Einmeldungen von Ressorts würden in den „Standard Operating Procedures“ berücksichtigt.

(3) Der RH stellte nunmehr fest, dass das Bundeskanzleramt keinen Gesamtüberblick über die wichtigen Dienste des Bundes erstellt hatte. Es begründete dies damit, dass es weder die Kompetenz habe, die Aufgabenerfüllung durch die anderen Ressorts durchzusetzen, noch die operativen Kräfte, die zur Erstellung des Gesamtüberblicks erforderlich wären: Gemäß der im NISG festgelegten gesetzlichen

[1] BGBl. I 111/2018

[2] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen in der Union, ABl. L 2016/194, 1

Verpflichtung hätten die Einrichtungen des Bundes ihre wesentlichen Dienste in Eigenverantwortung zu erheben und zu verwalten. Die Einrichtungen des Bundes wären aber durch das vom Bundeskanzleramt betriebene GovCERT angehalten, eine aktuelle Liste ihrer wichtigen Dienste bereitzuhalten und im Rahmen der Krisenvorbereitungen diese Informationen den operativen Einsatzkräften zur Verfügung zu stellen (zusammen mit Asset–Listen, Configuration–Listen, Netzwerkplänen und Business–Continuity–Plänen sowie Alarmierungsplänen).

Das Innenministerium teilte mit, dass ihm bislang keine Auflistung von wichtigen Diensten des Bundes zur Kenntnis gebracht worden sei. Sofern und sobald eine derartige Auflistung verfügbar sei, werde diese in etablierte Prozesse zur Überwachung von Risiken (Risk Monitoring) aufgenommen, um frühzeitig auf sich ändernde Bedrohungen und geänderte Risiken aufmerksam zu werden und geeignete Maßnahmen zu treffen.

3.2 Das Bundeskanzleramt erstellte keinen Gesamtüberblick über die wichtigen Dienste und setzte somit die Empfehlung des RH nicht um. Infolgedessen konnte ein solcher Gesamtüberblick weder dem IKDOK und dem GovCERT zur Kenntnis gebracht werden, noch konnten ihn die Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement berücksichtigen. Der RH hielt fest, dass das Bundeskanzleramt für diese koordinative Aufgabe zuständig war: Die Zuständigkeit ergab sich

- einerseits aus dem Wirkungsbereich des Bundeskanzleramts gemäß Bundesministeriengesetz 1986[3], der u.a. die Koordination der gesamten Verwaltung des Bundes umfasste, insbesondere auch Angelegenheiten der strategischen Netz– und Informationssicherheit, und
- andererseits aus der Aufgabe des Bundeskanzlers laut NISG, das GovCERT[4] zu betreiben.

Der RH empfahl daher dem Bundeskanzleramt, einen Gesamtüberblick über die wichtigen Dienste der Einrichtungen des Bundes zu erstellen. Er wiederholte seine Empfehlung aus dem Vorbericht, in Zusammenarbeit mit dem Innenministerium diesen Gesamtüberblick den operativen Gremien IKDOK und GovCERT zur Kenntnis zu bringen und in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement zu berücksichtigen.

3.3 Laut Stellungnahme des Bundeskanzleramts sei es ihm – in Ermangelung einer gesetzlichen Verpflichtung im NISG zur Auflistung aller wichtigen IT–gestützten Dienste durch die jeweiligen Einrichtungen des Bundes – nicht möglich gewesen, auf

[3] BGBl. 76/1986 i.d.g.F., Teil 2 A.1. der Anlage zu § 2

[4] § 4 Abs. 1 Z 4 in Verbindung mit § 14 Abs. 4 NISG

Basis der freiwilligen Mitwirkung der Einrichtungen des Bundes einen abschließenden Gesamtüberblick zu erstellen.

3.4 Der RH entgegnete dem Bundeskanzleramt, dass es zwar keine gesetzliche Verpflichtung der Einrichtungen des Bundes gab, ihre wichtigen Dienste dem Bundeskanzleramt mitzuteilen. Aus ihrer gesetzlichen Verpflichtung, für ihre wichtigen Dienste Sicherheitsvorkehrungen zu treffen, mussten jedoch jeweils Übersichten für die Erstellung eines Gesamtüberblicks vorhanden sein. Der RH blieb daher bei seiner Empfehlung.

Beschlüsse und Projekte zur Umsetzung des Regierungsprogramms 2020–2024

4.1 (1) Der RH hatte dem Bundeskanzleramt als dem für die zentrale Koordination in Angelegenheiten der Cyber–Sicherheit zuständigen Bundesministerium in seinem Vorbericht (TZ 8) empfohlen, der Bundesregierung weitere Beschlüsse bzw. Projekte zur Umsetzung der im Regierungsprogramm 2020–2024[5] angeführten Schwerpunkte zur Cyber–Sicherheit vorzubereiten. Dabei wären insbesondere die regelmäßigen Berichte der Cyber Sicherheit Steuerungsgruppe (in der Folge: **Steuerungsgruppe–CSS**) zu beachten.

(2) Im Nachfrageverfahren hatte das Bundeskanzleramt mitgeteilt, dass die Steuerungsgruppe–CSS – auch aufgrund der Empfehlung des RH in TZ 9 seines Vorberichts – nunmehr wieder zweimal im Jahr einberufen werde, gegebenenfalls auch anlassbezogen. Sowohl im Rahmen der CDO[6] Taskforce als auch im Rahmen der IT–Konsolidierung des Bundes seien Cyber–Sicherheitsprojekte gestartet worden.

(3) Der RH stellte nunmehr fest, dass das Bundeskanzleramt seit 2021 folgende Themen aus dem Regierungsprogramm 2020–2024[7] vorbereitet hatte:

- Ein staatliches Cybersicherheitszentrum sollte im Zuge der Umsetzung der NIS–2–Richtlinie[8] eingerichtet werden; die rechtliche Grundlage dafür bildete ein Gesetzesentwurf zur Umsetzung der NIS–2–Richtlinie, der zur Zeit der Follow–up–Überprüfung in Ausarbeitung war.

[5] Regierungsprogramm 2020–2024 „Aus Verantwortung für Österreich“ (2020)

[6] CDO = Chief Digital Officer

[7] S. 154 ff.

[8] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS–2–Richtlinie), ABl. L 2022/333, 80

- Die – durch die Bundesregierung angenommene – Österreichische Strategie für Cybersicherheit 2021[9] aktualisierte die Österreichische Strategie für Cybersicherheit aus dem Jahr 2013 und entwickelte diese weiter.
- Ein zentrales, beratendes und zertifizierendes Organ in Informationssicherheitsfragen (entsprechend dem Cyber Security Act der EU–Kommission[10]) sollte – unter Berücksichtigung bestehender Einrichtungen – mit dem Cyberzertifizierungsgesetz geschaffen werden. Dieses war zur Zeit der Follow–up–Überprüfung in politischer Koordination.
- Hinsichtlich der Einführung von Sicherheitsstandards im Rahmen der geltenden NIS–Richtlinie im öffentlichen Sektor hatte das Bundeskanzleramt ein Projekt zur Definition gemeinsamer Cyber–Sicherheitsstandards („Security Framework Bund") – im Rahmen der IT–Konsolidierung des Bundes – gestartet. Im Zuge dessen wurde anhand definierter, an der geltenden NIS–Richtlinie orientierter Cyber–Sicherheitsstandards eine Statuserhebung über deren Umsetzung in einzelnen Ressorts durchgeführt. Noch vorhandene Mängel bei der Erreichung dieser Standards sollten vor allem durch ministerienübergreifende Projekte behoben werden.

  Damit hatte das Bundeskanzleramt wesentliche Projekte, die im Kapitel „Cybersicherheit und Digitalisierung" des Regierungsprogramms 2020–2024 festgelegt wurden, umgesetzt.

4.2 Das Bundeskanzleramt setzte die Empfehlung um, indem es im überprüften Zeitraum vier wesentliche Projekte aus dem Regierungsprogramm 2020–2024 für die Regierung vorbereitet hatte.

[9] Die Österreichische Strategie für Cybersicherheit 2021 bestand aus einem strategischen Rahmenwerk und einem regelmäßig angepassten, dynamischen Maßnahmenkatalog.

[10] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations– und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) 526/2013 (Rechtsakt zur Cybersicherheit)

Aufgaben der Operativen Koordinierungsstruktur (OpKoord)

5.1 (1) Der RH hatte in seinem Vorbericht (TZ 13) dem Bundeskanzleramt und Innenministerium empfohlen, die Aufgaben der Operativen Koordinierungsstruktur (**OpKoord**) zu evaluieren und das damalige 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.

Die Zuständigkeit für die Agenden der Digitalisierung ging im Juli 2022 mit einer Novelle des Bundesministeriengesetzes 1986 vom Bundesministerium für Digitalisierung und Wirtschaftsstandort auf das Bundesministerium für Finanzen (in der Folge: **Finanzministerium**) über.[11] Die Umsetzung der Empfehlung war daher im Hinblick auf die Integration des Finanzministeriums zu überprüfen.

(2) Im Nachfrageverfahren hatten das Bundeskanzleramt und das Innenministerium mitgeteilt, dass die Empfehlung vom Innenministerium bereits aufgegriffen und umgesetzt worden sei. Die Bundesländervertreter würden nun regelmäßig eingeladen und informiert; darüber hinaus wäre eine dem Lagebild nachfolgende, regelmäßige Austauschveranstaltung etabliert. Mehrere anlassbezogene OpKoord–Sitzungen hätten stattgefunden, der Bedarf für regelmäßige OpKoord–Sitzungen werde jährlich evaluiert.

(3) Der RH stellte nunmehr fest, dass der IKDOK im Jahr 2022 das OpKoord–Format und dessen Aufgaben diskutierte; als Ergebnis arbeiteten das Bundeskanzleramt und das Innenministerium u.a. eine Geschäftsordnung für IKDOK und OpKoord gemäß NISG[12] aus.

Zur Gewährleistung der Sicherheit von Netz– und Informationssystemen waren gemäß NISG Computer–Notfallteams eingerichtet, die teilweise im IKDOK, teilweise in der OpKoord vertreten waren. Sitzungen der OpKoord fanden nach wie vor zeitgleich mit jenen des IKDOK statt, weil derselbe technische Dienstleister und damit derselbe Personenkreis die Agenden aller dieser Computer–Notfallteams wahrnahm. Sollten weitere Computer–Notfallteams gemäß NISG eingerichtet werden und deren Agenden durch einen anderen technischen Dienstleister wahrgenommen werden, würden laut Innenministerium eigene Sitzungen mit diesen Computer–

[11] Seit Mai 2024 war das Bundeskanzleramt für Agenden der Digitalisierung zuständig.

[12] § 7 Abs. 3 NISG

Notfallteams stattfinden. Darüber hinaus konnten auch anlassbezogene Sitzungen – insbesondere im Rahmen von erweiterten OpKoord–Sitzungen – abgehalten werden. Dies war bis zum Ende der Follow–up–Überprüfung einmal, im Jahr 2022, der Fall.

Das Finanzministerium – von Juli 2022 bis Ende April 2024 für Angelegenheiten der Digitalisierung zuständig – war nicht unmittelbar in die OpKoord integriert, da ihre Zusammensetzung gesetzlich[13] festgelegt war und demnach nur aus dem IKDOK und den in § 14 NISG vorgesehenen Computer–Notfallteams bestand. Dem Finanzministerium wurden jedoch – wie jedem Bundesministerium – Lagebilder, Warnungen und sonstige Informationen zur Verfügung gestellt. An anlassbezogenen Sitzungen der erweiterten OpKoord nahm die Bundesrechenzentrum Gesellschaft mit beschränkter Haftung als operativer IT–Dienstleister des Finanzministeriums (und des Bundes im Allgemeinen) teil. Die Einbindung in strategische Fragen war gewährleistet, indem das Finanzministerium als das für Digitalisierung zuständige Ressort an der Steuerungsgruppe–CSS teilnahm.

Der IKDOK informierte die Länder seit April 2023 monatlich durch ein Briefing in Form von Videokonferenzen. Eine ständige und unmittelbare Einbindung der Länder in die OpKoord war nicht gegeben. Dies lag einerseits an den gesetzlichen Vorgaben für ihre Zusammensetzung, andererseits daran, dass noch kein Land in seinem Wirkungsbereich die Verpflichtungen des NISG – zu Sicherheitsvorkehrungen und Meldungen – für anwendbar erklärt hatte.[14]

5.2 Das Bundeskanzleramt und das Innenministerium setzten die Empfehlung um, indem sie im Jahr 2022 die Aufgaben der OpKoord evaluierten. Der operative IT–Dienstleister des Finanzministeriums wurde zu erweiterten OpKoord–Sitzungen eingeladen. Der IKDOK informierte die Länder in einem monatlichen Briefing über das aktuelle OpKoord–Lagebild.

[13] § 3 Z 5 NISG

[14] Die Verpflichtungen des NISG erfassten die Einrichtungen der Länder nicht unmittelbar. Die Länder konnten diese für ihren Wirkungsbereich (inklusive Gemeinden) allerdings auf freiwilliger Basis mittels Landesgesetz für anwendbar erklären.

Cyber–Lagezentrum

6.1 (1) Der RH hatte dem Innenministerium in seinem Vorbericht (TZ 14) empfohlen, 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 Leitungsaufgaben im IKDOK (und in der OpKoord), die dem Bundesminister für Inneres zukommen, beim Innenministerium eingerichtet werden.

(2) Laut Mitteilung des Innenministeriums im Nachfrageverfahren habe es die Empfehlung umgesetzt, indem es unter Beachtung von Kosten–Nutzen–Aspekten Räume festgelegt und eingerichtet habe, in denen IKDOK und OpKoord tagen und in denen im Anlassfall auch technische und organisatorische Fachkräfte zusammengezogen werden könnten.

(3) Der RH stellte nunmehr fest, dass das Innenministerium ein aus mehreren Besprechungs– und Büroräumen bestehendes Lagezentrum in einem Amtsgebäude des Innenministeriums eingerichtet hatte. Kosten–Nutzen–Aspekte berücksichtigte das Ministerium insofern, als die Räume den Dienststellen auch im Regelbetrieb als Besprechungsräume und Büros im Rahmen des Desk Sharing zur Verfügung standen und laufend – neben den regelmäßigen und anlassbezogenen IKDOK– und OpKoord–Sitzungen – auch für sonstige Besprechungen, Projektsitzungen und Seminare genutzt wurden.

6.2 Das Innenministerium setzte die Empfehlung um, indem es in einem seiner Amtsgebäude ein Cyber–Lagezentrum einrichtete. Kosten–Nutzen–Aspekte berücksichtigte das Ministerium dabei, indem es die Räume auch für andere Zwecke als die Lagebesprechungen von IKDOK und OpKoord zur Verfügung stellte.

IT–Anwendung IKDOK–Plattform

7.1 (1) Der RH hatte dem Innenministerium in seinem Vorbericht (TZ 15) empfohlen, die im Aufbau befindliche IT–Anwendung „IKDOK–Plattform“ fertigzustellen, zur Lagebilderstellung einzusetzen und für eine gesicherte Kommunikation technisch auszugestalten.

(2) Laut Mitteilung des Innenministeriums im Nachfrageverfahren habe es die Empfehlung umgesetzt, indem die Plattform fertiggestellt worden und im Einsatz sei.

(3) Der RH stellte nunmehr fest, dass die IKDOK–Plattform vom Dienstleistungsunternehmen A, das auch das GovCERT betrieb, errichtet und betrieben wurde und dem IKDOK und der OpKoord zur Zusammenarbeit zur Verfügung stand. Die Administration lag beim Innenministerium. Die IKDOK–Plattform war ein Paket aus mehreren IT–Applikationen: Diese umfassten die Funktionen Benachrichtigung, Informationsweitergabe und Diskussion, E–Mail–Verschlüsselung, Datenaustausch und –ablage sowie gemeinsame Erstellung und Bearbeitung von Dokumenten. Die IKDOK–Plattform ermöglichte den IKDOK–Teilnehmerinnen und –Teilnehmern, Beiträge unmittelbar und selbstständig (ohne E–Mail–Verkehr) zu ändern, was den Komfort erhöhte und die Effizienz steigerte.

7.2 Das Innenministerium setzte die Empfehlung um, indem es dem IKDOK und der OpKoord zur Lagebilderstellung die – von einem Dienstleistungsunternehmen errichtete – IT–Anwendung „IKDOK–Plattform“ zur Verfügung stellte. Die IKDOK–Plattform war zum gesicherten Austausch von Informationen und Daten geeignet.

Aufgabenerbringung durch Bundesbedienstete im Computer–Notfallteam der öffentlichen Verwaltung (GovCERT)

8.1 (1) Der RH hatte dem Bundeskanzleramt in seinem Vorbericht (TZ 19) empfohlen, in Erwägung zu ziehen, die Aufgaben des GovCERT langfristig durch eigene Bedienstete des Bundes zu erbringen.

(2) Im Nachfrageverfahren hatte das Bundeskanzleramt auf die beschränkten Ressourcen und Planstellen hingewiesen. Auch das Gehaltsschema im öffentlichen Bereich sei nicht annähernd attraktiv genug, um geeignetes Personal mit den erforderlichen Fähigkeiten anzustellen.

(3) Der RH stellte nunmehr fest, dass nach Auskunft des Bundeskanzleramts das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS) noch keine entsprechenden Planstellen im Bundeskanzleramt genehmigt hatte. Darüber hinaus sei mit den besoldungsrechtlichen Voraussetzungen im Bundesdienst – einschließlich RIVIT–Schema (Gehaltsschema für Richtverwendungen für IT–Sonderverträge des Bundes) – entsprechendes Fachpersonal schwer rekrutierbar, da für Fachkräfte auf dem Gebiet der Cyber–Sicherheit im privatwirtschaftlichen Sektor ein höheres Gehaltsniveau üblich sei. Da sich die Anforderungen im Bereich der Cyber–Sicherheit laufend änderten, könne mit zugekauften Leistungen von extern Beschäftigten flexibler reagiert werden.

8.2 Das Bundeskanzleramt setzte die Empfehlung nicht um. Der RH verkannte nicht die Schwierigkeit, Fachpersonal mit den für das GovCERT erforderlichen Qualifikationen zu rekrutieren. Er erachtete jedoch die Cyber–Sicherheit (als Teil der öffentlichen Sicherheit) als eine staatliche Kernaufgabe, die durch öffentlich Bedienstete erfüllt werden sollte.

Der RH wiederholte daher seine Empfehlung an das Bundeskanzleramt aus dem Vorbericht, in Erwägung zu ziehen, die Aufgaben des GovCERT langfristig durch Bedienstete des Bundes zu erbringen.

Aus Sicht des RH war es aber auch erforderlich, die für die Personalbewirtschaftung des Bundes zuständigen Stellen in die spezielle Problematik, Cyber–Sicherheits–Expertinnen und –Experten zu rekrutieren, einzubinden.

Der RH empfahl daher dem Bundeskanzleramt, in Zusammenarbeit mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport – dem für Personal des Bundes und daher auch für Fragen der Besoldung zuständigen Ministerium – Lösungsansätze für eine Rekrutierung von Cyber–Sicherheits–Expertinnen und –Experten zu erarbeiten.

8.3 Das Bundeskanzleramt führte in seiner Stellungnahme aus, dass die Planstellensituation für das GovCERT unverändert sei. Im Entwurf zum NISG 2024 seien die Aufgaben des GovCERT dem Bundesminister für Inneres zugeschrieben und entsprechende Planstellen mit RIVIT–Bewertung vorgesehen gewesen; der Entwurf habe jedoch in der Plenarsitzung des Nationalrats vom 4. Juli 2024 die erforderliche Mehrheit nicht erreicht. Das Bundeskanzleramt erarbeite nunmehr gemeinsam mit dem Innenministerium die weitere Vorgehensweise; an der Aufteilung zwischen strategischen (Bundeskanzleramt) und operativen Aufgaben (Innenministerium) ändere sich vorläufig nichts. Das Ziel, im Rahmen des Umsetzungsrechtsakts zur NIS–2–Richtlinie Planstellen mit RIVIT–Bewertungen vorzusehen, werde weiterverfolgt.

Frühwarnsystem

9.1 (1) Der RH hatte dem Innenministerium in seinem Vorbericht (TZ 20) empfohlen, das Projekt zur Implementierung des Frühwarnsystems (Sensornetzwerk) verstärkt zu betreiben und umzusetzen. Im Sinne des gesamtstaatlichen und sektorübergreifenden Ziels, Cyber–Angriffe zu erkennen bzw. deren Auswirkungen so gering wie möglich zu halten sowie Muster und Vorgehensweisen bei Cyber–Angriffen zu analysieren, sollten möglichst viele Organisationen an diesem Frühwarnsystem (Sensornetzwerk) teilnehmen, um dadurch eine großflächige Abdeckung der Risiken zu erreichen.

(2) Im Nachfrageverfahren hatte das Innenministerium mitgeteilt, dass die Maßnahme in Umsetzung sei. Aufgrund der Komplexität des Unterfangens sei ein – in der Endphase befindliches – Vorprojekt notwendig gewesen, um die Unterlagen für das Vergabeverfahren zu erarbeiten. Mit dem Start des Vergabeverfahrens für das Umsetzungsprojekt sei im Laufe des Jahres 2023 zu rechnen.

(3) Der RH stellte nunmehr fest, dass das Innenministerium bis November 2023 noch kein Frühwarnsystem (Sensornetzwerk) implementiert und in Betrieb genommen hatte. Im Oktober 2022 erteilte das Innenministerium nach einem Vergabeverfahren den Auftrag für das Konzept eines Frühwarnsystems. Nach Abschluss der Konzeption Ende des dritten Quartals 2023 wurde das Umsetzungsprojekt im November 2023 mit einem Kick–off gestartet und ein Projektplan erstellt. Gemäß dem Projektauftrag sollte das Frühwarnsystem im Oktober 2026 in den Regelbetrieb übergehen.

9.2 Das Innenministerium setzte die Empfehlung teilweise um, weil es die Konzeption mit Ende des dritten Quartals 2023 abgeschlossen hatte, das eigentliche Umsetzungsprojekt im November 2023 jedoch erst in der Vorbereitungsphase war.

Der RH empfahl daher dem Innenministerium, das Projekt zur Implementierung des Frühwarnsystems (Sensornetzwerk) verstärkt zu betreiben und abzuschließen.

9.3 Das Innenministerium teilte in seiner Stellungnahme mit, dass das Projekt zur Implementierung des Frühwarnsystems im Zeitplan sei und verstärkt betrieben werde. Zusätzliche Ressourcen (erfahrene Fachkräfte im einschlägigen Bereich) stünden ab dem dritten Quartal 2024 zur Verfügung. Ein Pilotbetrieb sei ab dem dritten Quartal 2025 vorgesehen.

Meldesammel– und Meldeanalysesystem

10.1 (1) Der RH hatte dem Innenministerium in seinem Vorbericht (TZ 21) empfohlen, das Meldesammelsystem rasch umzusetzen; die Erfahrungen aus dem Betrieb sollten dafür genutzt werden, die im NISG vorgesehene IKT[15]–Lösung für ein NIS[16]–Meldeanalysesystem umzusetzen. Die beiden Systeme dienten zur Sammlung, Analyse und Bewertung von (Sicherheits–)Vorfällen.

(2) Laut Mitteilung des Innenministeriums im Nachfrageverfahren sei die Empfehlung umgesetzt: Das Meldesammelsystem sei in Betrieb; das Meldeanalysesystem werde im Rahmen des EU–geförderten Projekts AWAKE umgesetzt und solle im Jahr 2023 den Pilotbetrieb aufnehmen.

(3) Der RH stellte nunmehr fest, dass das Meldesammelsystem seit Juli 2021 im Einsatz war. Die NIS–Meldesammelstelle betrieb dieses System unter Verwendung eines Ticketingsystems und eines Workflow– und Dokumentenverwaltungssystems. Durch die NIS–Meldesammelstelle war auch die Grundfunktion einer Meldeanalyse umgesetzt. Eine Softwarelösung, die in einem EU–geförderten Projekt mit dem Bundeskanzleramt und weiteren Partnern in Entwicklung war, sollte die Meldeanalyse verbessern und ergänzen. Geplantes Projektende für das Meldeanalysesystem war Ende August 2024.

10.2 Das Innenministerium setzte die Empfehlung teilweise um, indem es im Juli 2021 ein Meldesammelsystem in Betrieb nahm. Dieses enthielt bereits die Grundfunktion einer Meldeanalyse. Es bildete somit die Grundlage für ein Meldeanalysesystem, das in einem weiterführenden Projekt in Entwicklung war.

Der RH empfahl dem Innenministerium, das im NISG vorgesehene Meldeanalysesystem umzusetzen, indem es das gestartete Projekt zur Weiterentwicklung des Meldesammelsystems konsequent weiterverfolgt und abschließt. Durch die Weiterentwicklung soll auch die zu erwartende steigende Anzahl von Meldungen über Sicherheitsvorfälle effizient bearbeitet werden, die sich aus dem erweiterten Kreis der von der NIS–2–Richtlinie erfassten Einrichtungen ergibt.

10.3 Laut Stellungnahme des Innenministeriums sei das Meldesammelsystem umgesetzt; das Projekt zur Implementierung des Meldeanalysesystems werde weiterhin verfolgt und sei im Zeitplan.

[15] IKT = Informations– und Kommunikationstechnologie

[16] NIS = Netz– und Informationssystemsicherheit

Cyber–Einsatzteam

11.1 (1) Der RH hatte in seinem Vorbericht (TZ 25) dem Bundeskanzleramt und dem Innenministerium empfohlen, in Ergänzung zur Schaffung des permanenten Cyber–Lagezentrums im Innenministerium auch ein permanent verfügbares Cyber–Einsatzteam (Rapid Response Team) in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam zu schaffen.

(2) Laut Mitteilung des Bundeskanzleramts im Nachfrageverfahren habe das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport die vorgesehenen Planstellen für das Cyber–Einsatzteam im Bundesministerium für Landesverteidigung (in der Folge: **Verteidigungsministerium**) abgelehnt. Ein Cyber–Einsatzteam in der geforderten und benötigten Ausprägung werde es daher nicht geben.

Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass die Umsetzung dieser Empfehlung gesamtstaatlich in Arbeit und mit dem Schwerpunkt im Verteidigungsministerium eingeleitet worden sei. Im Innenministerium gebe es Vorgaben dafür, im konkreten Anlassfall umgehend Sonderkommissionen oder Task Forces zu bilden, die als Cyber–Einsatzteam dienen.

(3) Der RH stellte nunmehr fest, dass das Bundeskanzleramt und das Innenministerium kein Cyber–Einsatzteam eingerichtet hatten.

Laut Bundeskanzleramt gab es diesbezüglich Planungen und Arbeiten im Verteidigungsministerium. Dort habe die jüngste Organisationsreform die organisatorischen Grundlagen für Cyber–Einsatzteams geschaffen. Auf die konkrete Umsetzung und insbesondere auf die für das Verteidigungsministerium erforderliche Genehmigung von Planstellen bzw. die Personalrekrutierung habe das Bundeskanzleramt aber keinen Einfluss.

Das Innenministerium verwies auf die unterschiedlichen Ziele und die Ressourcenlage in den Ministerien bzw. in deren für Cyber–Sicherheit zuständigen Organisationseinheiten, sodass derzeit kein eigenes Cyber–Einsatzteam eingerichtet werden könne. Im Rahmen seiner Kompetenz zur Kriminalitätsbekämpfung bilde das Innenministerium im Anlassfall – neben der Strafverfolgung durch die Sicherheitsbehörden – organisationsübergreifende Sonderkommissionen und (zum Teil interministerielle) Task Forces zur Bündelung von fachlichen und personellen Ressourcen.

11.2 Das Bundeskanzleramt und das Innenministerium setzten die Empfehlung zum Cyber–Einsatzteam nicht um. Der RH räumte ein, dass das Verteidigungsministerium organisatorische Grundlagen für die Einrichtung von Cyber–Einsatzteams in seinem Wirkungsbereich geschaffen hatte und dass das Innenministerium bei Cyber–Sicherheitsvorfällen anlassbezogen Einheiten bildete, die u.a. Aufgaben eines Cyber–

Einsatzteams wahrnehmen konnten. Er erachtete jedoch ein permanent eingerichtetes Cyber–Einsatzteam als erforderlich, um Cyber–Sicherheitsvorfälle effizient zu bewältigen.

Er hielt daher seine Empfehlung an das Bundeskanzleramt und an das Innenministerium aufrecht, in Ergänzung zum permanenten Cyber–Lagezentrum im Innenministerium (TZ 6) auch ein permanent verfügbares nationales Cyber–Einsatzteam in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam zu schaffen.

Aus Sicht des RH war es aber auch erforderlich, in die spezielle Problematik der Rekrutierung von Cyber–Sicherheits–Expertinnen und –Experten für das Cyber–Einsatzteam die für die Personalbewirtschaftung des Bundes zuständigen Stellen einzubinden.

Der RH wiederholte daher gegenüber dem Bundeskanzleramt und dem Innenministerium seine Empfehlung in TZ 8, in Zusammenarbeit mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport – dem für Personal des Bundes und daher auch für Fragen der Besoldung zuständigen Ministerium – Lösungsansätze für eine Rekrutierung von Cyber–Sicherheits–Expertinnen und –Experten zu erarbeiten.

11.3 (1) Das Bundeskanzleramt verwies in seiner Stellungnahme auf seine Ausführungen zu TZ 8 und auf die Stellungnahme des Innenministeriums.

(2) Laut Stellungnahme des Innenministeriums zur Einrichtung eines Cyber–Einsatzteams sei – wie schon in der Stellungnahme zum Vorbericht ausgeführt – ein weiterer Aufbau der personellen Kapazitäten im Bereich Cyber–Sicherheit im Innenministerium geplant und teilweise bereits in Umsetzung. Dieser personelle Aufbau sei die Voraussetzung zur Sicherstellung einer erweiterten Einsatzfähigkeit im Rahmen von Rapid Response Teams.

Für die Umsetzung der Empfehlung zur Rekrutierung von Fachkräften sei das Bundeskanzleramt zuständig.

11.4 Der RH entgegnete dem Innenministerium, dass die Einrichtung eines Cyber–Einsatzteams wie auch die Mitwirkung an der Schaffung geeigneter Grundlagen für die Rekrutierung des dafür erforderlichen Personals eine gemeinsame Aufgabe von Bundeskanzleramt und Innenministerium war. Er hielt daher seine Empfehlung aufrecht.

Krisen–, Kontinuitäts– und Einsatzpläne

12.1 (1) Der RH hatte dem Bundeskanzleramt und dem Innenministerium in seinem Vorbericht (TZ 26) empfohlen, konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement auszuarbeiten.

(2) Laut Mitteilung des Bundeskanzleramts im Nachfrageverfahren würden diese Pläne im Rahmen des internen Projekts „Stärkung der Cyber–Abwehrfähigkeiten im Bundeskanzleramt“ entwickelt, jedoch nur bezogen auf den Wirkungsbereich des Bundeskanzleramts; für das gesamtstaatliche Cyber–Krisenmanagement sei das Innenministerium zuständig.

Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass die Empfehlung laufend in Umsetzung sei. Pläne in Form von Standard Operating Procedures würden laufend aktualisiert; diese beinhalteten auch die Vernetzung und Schnittstellen mit europäischen Partnern (Cyber Crisis Liaison Network, CSIRT[17] Netzwerk).

(3) Der RH stellte nunmehr fest, dass der Bundesminister für Inneres im Juli 2023 eine Geschäftsordnung zur Regelung der Zusammenarbeit in IKDOK und OpKoord erlassen hatte. Die – an alle am IKDOK teilnehmenden Ressorts versandte – Geschäftsordnung sah Kooperationsstufen für das Ausmaß der Zusammenarbeit vor – vom Regelbetrieb bis zum Vorliegen einer Cyberkrise. Standardhandlungsanweisungen (Standard Operating Procedures) sollten diese Stufen näher definieren; dazu wurden zur Zeit der Follow–up–Überprüfung neue Standardhandlungsanweisungen erstellt und bestehende angepasst und ergänzt. Ein Entwurf lag dem RH vor, ein geschäftsordnungsmäßiger Beschluss war noch nicht gefasst.

Das Innenministerium hatte außerdem interne Pläne zur Einberufung des IKDOK im Falle einer Cyberkrise und zur Unterstützung des Cyber–Krisenmanagements erstellt. Für das Cyber–Krisenmanagement hielten das Innenministerium und die anderen in IKDOK und OpKoord vertretenen Ressorts und Organisationen materielle und personelle Ressourcen bereit.

Seit Mitte September 2023 war im Bundeskanzleramt ein ressortinternes, nur den eigenen Wirkungsbereich betreffendes Managementsystem für Informationssicherheit (ISMS[18]) im Einsatz. Das Bundeskanzleramt hatte den anderen Bundesministerien Informationen über die Umsetzung im eigenen Haus und Vorlagen, Richtlinien und Prozesse zur Übernahme in den eigenen Wirkungsbereich angeboten. Zum interministeriellen Informations– und Erfahrungsaustausch diente auch eine vom Bundeskanzleramt geschaffene Plattform.

[17] CSIRT = Computer Security Incident Response Team

[18] ISMS = Information Security Management System

12.2 Das Bundeskanzleramt und das Innenministerium setzten die Empfehlung zu den Krisen–, Kontinuitäts– und Einsatzplänen teilweise um: Der Bundesminister für Inneres erließ eine Geschäftsordnung für die Zusammenarbeit in IKDOK und OpKoord, die Kooperationsstufen für das Ausmaß der Zusammenarbeit festlegte – vom Regelbetrieb bis zum Vorliegen einer Cyberkrise. Die bereits angepassten bzw. ergänzten Standardhandlungsanweisungen, die die Kooperationsstufen konkretisieren sollten, lagen jedoch erst als Entwurf vor.

Der RH empfahl daher dem Innenministerium, den Entwurf der Standardhandlungsanweisungen, die die Kooperationsstufen für das Ausmaß der Zusammenarbeit zwischen IKDOK und OpKoord konkretisieren, möglichst rasch einer Beschlussfassung im IKDOK zuzuführen.

12.3 Das Innenministerium teilte in seiner Stellungnahme mit, dass die Standardhandlungsanweisungen mittlerweile im IKDOK beschlossen worden seien. Somit sei die Empfehlung des RH umgesetzt.

Cyber–Sicherheitsleitstelle

13.1 (1) Der RH hatte dem Bundeskanzleramt und dem Innenministerium in seinem Vorbericht (TZ 26) empfohlen, eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale einzurichten und das Cyber–Einsatzteam (Rapid Response Team) dort zu integrieren.

(2) Laut Mitteilung des Bundeskanzleramts im Nachfrageverfahren liege dies in der Zuständigkeit des Innenministeriums. Das Bundeskanzleramt habe im Zentralen Ausweichsystem in St. Johann im Pongau ein Ausweichlagezentrum für Cyberkrisen eingerichtet. Dieses verfüge auch über die benötigten Anbindungen zu den Bundesministerien.

Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass diese Empfehlung nicht umgesetzt sei.

(3) Der RH stellte nunmehr fest, dass eine staatliche Cyber–Sicherheitsleitstelle nicht eingerichtet war.

Das Bundeskanzleramt verwies auf die Zuständigkeit des Innenministeriums. Es sei geplant, ein staatliches Cyber–Sicherheitszentrum im Zuge der Umsetzung der NIS–2–Richtlinie einzurichten; die rechtliche Grundlage dafür war in Ausarbeitung. Das Cyber–Sicherheitszentrum sollte auch die Aufgaben einer Cyber–Sicherheitsleitstelle wahrnehmen.

Nach Ansicht des Innenministeriums könnten sich die Aufgaben einer Cyber–Sicherheitsleitstelle nur aus der Koordinierung der Tätigkeit von Cyber–Einsatzteams (Koordination der Teams) und des Frühwarnsystems (laufendes Monitoring der Sensoren, Koordination im Anlassfall) ergeben. Da aber zur Zeit der Follow–up–Überprüfung kein Cyber–Einsatzteam installiert war (TZ 11) und sich das Frühwarnsystem erst in der Konzeptionsphase befand (TZ 9), wäre eine Cyber–Sicherheitsleitstelle noch nicht erforderlich. Das Innenministerium wies jedoch darauf hin, dass im Zuge der Umsetzung der NIS–2–Richtlinie und der damit verbundenen Ausweitung der Normunterworfenen ohnedies eine Organisationsentwicklung notwendig werde. Die Empfehlung des RH werde daher bei den Plänen zu dieser neuen Aufbau– und Ablauforganisation berücksichtigt.

13.2 Das Bundeskanzleramt und das Innenministerium setzten die Empfehlung nicht um.

Der RH hielt daher seine Empfehlung an das Bundeskanzleramt und an das Innenministerium aufrecht, eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale einzurichten. Im Hinblick auf die laufenden Arbeiten zur Umsetzung der NIS–2–Richtlinie, in deren Rahmen auch die Einrichtung eines Cyber–Sicherheitszentrums geplant ist, sollte die Integration der Aufgaben einer Cyber–Sicherheitsleitstelle in eine derartige Einrichtung berücksichtigt werden.

Gleichzeitig verwies der RH auf seine noch offenen Empfehlungen, ein Frühwarnsystem (TZ 9) und ein Cyber–Einsatzteam (Rapid Response Team, TZ 11) einzurichten.

13.3 Das Bundeskanzleramt und das Innenministerium verwiesen in ihren Stellungnahmen auf die vom Innenministerium zum Vorbericht abgegebene Stellungnahme. Demnach solle die Einrichtung einer staatlichen Cyber–Sicherheitsleitstelle im Rahmen des geplanten Cyber–Lagezentrums betrachtet werden und in die diesbezüglichen Planungen miteinfließen.

13.4 Der RH erwiderte dem Bundeskanzleramt und dem Innenministerium, dass das Cyber–Lagezentrum ohne Cyber–Sicherheitsleitstelle eingerichtet wurde. Er bekräftigte daher seine Empfehlung, die Integration der Aufgaben einer Cyber–Sicherheitsleitstelle in das im Zuge der Umsetzung der NIS–2–Richtlinie geplante Cyber–Sicherheitszentrum zu berücksichtigen.

Einbeziehen der Länder in die gesetzlichen Verpflichtungen zur Netz– und Informationssystemsicherheit

14.1 (1) Die Verpflichtungen des NISG erfassten die Einrichtungen der Länder nicht unmittelbar. Die Länder konnten diese für ihren Wirkungsbereich (inklusive Gemeinden) allerdings auf freiwilliger Basis mittels Landesgesetz für anwendbar erklären. Ein derartiges Landesgesetz hatte bis zur Vorprüfung kein Land erlassen (siehe dazu Vorbericht TZ 2, TZ 4 und TZ 29). Dadurch war nicht sichergestellt, dass das Schutzniveau von Einrichtungen der Länder jenem der Einrichtungen des Bundes entsprach; weiters waren die Länder weder in die strategische (z.B. Steuerungsgruppe–CSS) noch in die operative Koordination (OpKoord) der Cyber–Sicherheit regelmäßig eingebunden. Daher hatte der RH dem Bundeskanzleramt in seinem Vorbericht (TZ 29) empfohlen, 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.

Im Jänner 2023 trat eine neue Richtlinie zur Netz– und Informationssicherheit in Kraft, die NIS–2–Richtlinie. Sie ersetzt ab Oktober 2024 die geltende NIS–Richtlinie[19] und ist bis dahin in nationales Recht umzusetzen. Die neue NIS–2–Richtlinie enthielt wesentliche Änderungen u.a. in Bezug auf die Einbeziehung der öffentlichen Verwaltung. Einrichtungen der öffentlichen Verwaltung auf Ebene der Zentralregierungen waren jedenfalls zu Sicherheitsmaßnahmen und Meldungen bei Sicherheitsvorfällen verpflichtet, Einrichtungen auf Ebene der Regionen – in Österreich der Länder – abhängig von einer risikobasierten Bewertung. Die Umsetzung der Empfehlung war daher auch im Hinblick auf die Einbindung der Länder in die bisherigen Vorarbeiten zur rechtlichen Umsetzung der NIS–2–Richtlinie zu überprüfen.

(2) Im Nachfrageverfahren hatte das Bundeskanzleramt mitgeteilt, dass die Vorbereitungen auf die Umsetzung der NIS–2–Richtlinie laufen würden. Die Länder seien an einer gemeinsamen Umsetzung interessiert und das Bundeskanzleramt arbeite im Entwurf auf eine gemeinsame Umsetzung hin. Das Bundeskanzleramt wies ergänzend darauf hin, dass auch eine Zustimmung der Länder die notwendige Verfassungsbestimmung zur flächendeckenden Umsetzung ersetzen könne.

(3) Zur Einbindung der Länder in die bisherigen Vorarbeiten zur rechtlichen Umsetzung der NIS–2–Richtlinie stellte der RH nunmehr fest, dass das Bundeskanzleramt im September 2023 einen ersten Gesetzesentwurf – abgestimmt mit dem Innenministerium – fertiggestellt hatte; die zugehörige Wirkungsorientierte Folgenabschätzung sowie die Erläuternden Bemerkungen waren zur Zeit der Follow–up–Überprüfung in

[19] Die Richtlinie (EU) 2016/1148 wird mit Wirkung vom 18. Oktober 2024 aufgehoben (Art. 44 NIS–2–Richtlinie).

Fertigstellung. Im Zuge der Erarbeitung des Gesetzesentwurfs hatte das Bundeskanzleramt bilaterale Gespräche mit dem Magistrat der Stadt Wien sowie mit der Wirtschaftskammer Österreich und weiteren Stakeholdern geführt. Die Einbindung der Länder erfolgte in der Phase der Vorarbeiten durch Informationsvorträge; vor dem Hintergrund des nunmehr vorliegenden Gesetzesentwurfs organisierten das Bundeskanzleramt und das Innenministerium im ersten Quartal 2024 Abstimmungsgespräche, eine legistische Arbeitsgruppe unter Einbeziehung der Länder, die bis zum März 2024 zwei Sitzungen abhielt, sowie eine Bund–Länder–Besprechung mit Vertretern der Kabinette der beiden Bundesministerien. Mehrere Länder nutzten die Möglichkeit, zum Gesetzesentwurf inhaltlich Stellung zu nehmen.

In die Koordinierungsgremien der Cyber–Sicherheit waren die Länder unterschiedlich eingebunden:

- Im überprüften Zeitraum wurden die Länder nicht zu den Sitzungen der Steuerungsgruppe–CSS eingeladen, obwohl die Geschäftsordnung dieses Gremiums die Möglichkeit dazu vorsah.
- An der Informationsdrehscheibe des GovCERT nahmen nunmehr nach Aufforderung des Bundeskanzleramts auch Kärnten und die Steiermark und somit Vertreterinnen und Vertreter aus allen Ländern teil.
- Am CERT–Verbund Austria nahm Wien teil; es war das einzige Land mit einem eigenen Computer–Notfallteam.
- Zur Einbindung in die OpKoord siehe TZ 5.

14.2 Das Bundeskanzleramt setzte die Empfehlung zur Einbeziehung der Länder teilweise um: Es informierte die Länder über die Vorarbeiten zur rechtlichen Umsetzung der NIS–2–Richtlinie durch Vorträge und durch bilaterale Gespräche (mit Wien) und band sie über Abstimmungsgespräche und eine legistische Arbeitsgruppe in die weitere Bearbeitung des Gesetzesentwurfs ein. Alle Länder nahmen an der Informationsdrehscheibe des GovCERT teil.

Das Bundeskanzleramt lud die Länder aber nicht zu den Sitzungen der Steuerungsgruppe–CSS ein.

Der RH empfahl daher dem Bundeskanzleramt, die Länder zu den Sitzungen der Steuerungsgruppe–CSS einzuladen; dies insbesondere im Hinblick auf die Verpflichtungen, die sich für die Länder aus der Umsetzung der NIS–2–Richtlinie künftig ergeben.

14.3 Das Bundeskanzleramt merkte in seiner Stellungnahme an, dass es – wie auch das Innenministerium – im regelmäßigen Austausch mit den Ländern stehe. Da die

Länder von den Verpflichtungen des NISG nicht umfasst seien, fehle eine entsprechende gesetzliche Grundlage, diese in das Sitzungsformat einzuladen.

14.4 Der RH entgegnete dem Bundeskanzleramt, dass eine Einbeziehung der Länder in die Verpflichtungen des NISG keine Voraussetzung für ihre Einladung zu den Sitzungen der Steuerungsgruppe–CSS war und wies nochmals auf die künftigen Verpflichtungen der Länder aus der NIS–2–Richtlinie hin. Er hielt daher seine Empfehlung aufrecht.

Schlussempfehlungen

15 Der RH stellte fest, dass

- das Bundeskanzleramt von acht überprüften Empfehlungen des Vorberichts zwei umsetzte, zwei teilweise und vier nicht umsetzte.
- das Innenministerium von neun überprüften Empfehlungen des Vorberichts drei umsetzte, drei teilweise und drei nicht umsetzte.

Umsetzungsgrad der Empfehlungen des Vorberichts						Reihe Bund 2022/13
Vorbericht			Nachfrage-verfahren	Follow–up–Überprüfung		
TZ	Empfehlungsinhalt		Status	TZ		Umsetzungsgrad
Bundeskanzleramt						
4	In Zusammenarbeit mit dem Bundesministerium für Inneres wäre den operativen Gremien Innerer Kreis der Operativen Koordinierungsstruktur (**IKDOK**) und Computer–Notfallteam der öffentlichen Verwaltung (**GovCERT**) ein Gesamtüberblick der wichtigen Dienste des Bundes zur Kenntnis zu bringen; dieser wäre in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement zu berücksichtigen.		keine Angabe	3		nicht umgesetzt
8	Das Bundeskanzleramt als das für die zentrale Koordination in Angelegenheiten der Cyber–Sicherheit zuständige Bundes-ministerium sollte der Bundesregierung weitere Beschlüsse bzw. Projekte zur Umsetzung der im Regierungsprogramm 2020–2024 angeführten Schwerpunkte zur Cyber–Sicherheit vorbereiten. Dabei wären insbesondere die regelmäßigen Berichte der Cyber Sicherheit Steuerungsgruppe zu beachten.		umgesetzt	4		umgesetzt
13	Die Aufgaben der Operativen Koordinierungsstruktur (**OpKoord**) wären zu evaluieren und das für Digitalisierung zuständige Bundesministerium sowie die Länder auf geeignete Weise zu integrieren. Hierbei wäre auch festzulegen, ob die OpKoord regelmäßig oder nur im Bedarfsfall einzuberufen wäre.		umgesetzt	5		umgesetzt
19	Es wäre in Erwägung zu ziehen, die Aufgaben des GovCERT langfristig durch eigene Bedienstete des Bundes zu erbringen.		nicht umgesetzt	8		nicht umgesetzt
25	Ein permanent verfügbares Cyber–Einsatzteam (Rapid Response Team) wäre zu schaffen; dies in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatz-team.		zugesagt	11		nicht umgesetzt
26	Es wären konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement auszuarbeiten.		teilweise umgesetzt	12		teilweise umgesetzt
26	Eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale wäre einzurichten und das Cyber–Einsatzteam (Rapid Response Team) dort zu integrieren.		nicht umgesetzt	13		nicht umgesetzt
29	Im Rahmen der Aufgaben der strategischen Koordination der Cyber–Sicherheit wäre auf eine wirksame Einbeziehung der Länder in die gesetzlichen Verpflichtungen zur Netz– und Informationssystemsicherheit hinzuwirken.		zugesagt	14		teilweise umgesetzt

Umsetzungsgrad der Empfehlungen des Vorberichts					Reihe Bund 2022/13
Vorbericht		Nachfrage-verfahren	Follow–up–Überprüfung		
TZ	Empfehlungsinhalt	Status	TZ	Umsetzungsgrad	
Bundesministerium für Inneres					
4	Das Bundeskanzleramt sollte in Zusammenarbeit mit dem Bundesministerium für Inneres den operativen Gremien Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK) und Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) einen Gesamtüberblick der wichtigen Dienste des Bundes zur Kenntnis bringen; dieser wäre in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement zu berücksichtigen.	umgesetzt	3	nicht umgesetzt	
13	Die Aufgaben der Operativen Koordinierungsstruktur (OpKoord) wären zu evaluieren und das für Digitalisierung zuständige Bundesministerium sowie die Länder auf geeignete Weise zu integrieren. Hierbei wäre auch festzulegen, ob die OpKoord regelmäßig oder nur im Bedarfsfall einzuberufen wäre.	umgesetzt	5	umgesetzt	
14	Ein Cyber–Lagezentrum wäre 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.	umgesetzt	6	umgesetzt	
15	Die im Aufbau befindliche „IKDOK–Plattform“ wäre fertigzustellen, zur Lagebilderstellung einzusetzen und auch für eine gesicherte Kommunikation technisch auszugestalten.	umgesetzt	7	umgesetzt	
20	Das Projekt zur Implementierung des Frühwarnsystems (Sensornetzwerk) wäre verstärkt zu betreiben und umzusetzen. Im Sinne des gesamtstaatlichen und sektorübergreifenden Ziels, Cyber–Angriffe zu erkennen bzw. deren Auswirkungen so gering wie möglich zu halten sowie Muster und Vorgehensweisen bei Cyber–Angriffen zu analysieren, sollten möglichst viele Organisationen an diesem Frühwarnsystem (Sensornetzwerk) teilnehmen, um dadurch eine großflächige Abdeckung der Risiken zu erreichen.	zugesagt	9	teilweise umgesetzt	
21	Das Meldesammelsystem wäre rasch umzusetzen; die Erfahrungen aus dem Betrieb sollen dafür genutzt werden, die im Netz– und Informationssystemsicherheitsgesetz vorgesehene IKT–Lösung für ein NIS–Meldeanalysesystem umzusetzen.	umgesetzt	10	teilweise umgesetzt	
25	Ein permanent verfügbares Cyber–Einsatzteam (Rapid Response Team) wäre zu schaffen; dies in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam.	zugesagt	11	nicht umgesetzt	
26	Es wären konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement auszuarbeiten.	teilweise umgesetzt	12	teilweise umgesetzt	
26	Eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale wäre einzurichten und das Cyber–Einsatzteam (Rapid Response Team) dort zu integrieren.	nicht umgesetzt	13	nicht umgesetzt	

Anknüpfend an den Vorbericht hob der RH folgende Empfehlungen hervor:

Bundeskanzleramt

(1) Es wäre in Erwägung zu ziehen, die Aufgaben des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) langfristig durch Bedienstete des Bundes zu erbringen. (TZ 8)

(2) Die Länder wären zu den Sitzungen der Cyber Sicherheit Steuerungsgruppe einzuladen; dies insbesondere im Hinblick auf die Verpflichtungen, die sich für die Länder aus der Umsetzung der NIS–2–Richtlinie künftig ergeben. (TZ 14)

Bundesministerium für Inneres

(3) Das Projekt zur Implementierung des Frühwarnsystems (Sensornetzwerk) wäre verstärkt zu betreiben und abzuschließen. (TZ 9)

(4) Das im Netz– und Informationssystemsicherheitsgesetz (NISG) vorgesehene Meldeanalysesystem wäre umzusetzen, indem das gestartete Projekt zur Weiterentwicklung des Meldesammelsystems konsequent weiterverfolgt und abgeschlossen wird. Durch die Weiterentwicklung soll auch die zu erwartende steigende Anzahl von Meldungen über Sicherheitsvorfälle effizient bearbeitet werden, die sich aus dem erweiterten Kreis der von der NIS–2–Richtlinie erfassten Einrichtungen ergibt. (TZ 10)

(5) Der Entwurf der Standardhandlungsanweisungen, die die Kooperationsstufen für das Ausmaß der Zusammenarbeit zwischen den Gremien Innerer Kreis der Operativen Koordinierungsstruktur (**IKDOK**) und Operative Koordinierungsstruktur (**OpKoord**) konkretisieren, wäre möglichst rasch einer Beschlussfassung im IKDOK zuzuführen. (TZ 12)

Bundeskanzleramt; Bundesministerium für Inneres

(6) Das Bundeskanzleramt sollte einen Gesamtüberblick über die wichtigen Dienste der Einrichtungen des Bundes erstellen. In Zusammenarbeit mit dem Bundesministerium für Inneres wäre dieser Gesamtüberblick den operativen Gremien IKDOK und GovCERT zur Kenntnis zu bringen und in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement zu berücksichtigen. (TZ 3)

(7) In Ergänzung zum permanenten Cyber–Lagezentrum im Bundesministerium für Inneres (TZ 6) wäre auch ein permanent verfügbares nationales Cyber–Einsatzteam in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam zu schaffen. (TZ 11)

(8) In Zusammenarbeit mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport – dem für Personal des Bundes und daher auch für Fragen der Besoldung zuständigen Ministerium – wären Lösungsansätze für eine Rekrutierung von Cyber–Sicherheits–Expertinnen und –Experten zu erarbeiten. (TZ 8, TZ 11)

(9) Eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale wäre einzurichten. Im Hinblick auf die laufenden Arbeiten zur Umsetzung der NIS–2–Richtlinie, in deren Rahmen auch die Einrichtung eines Cyber–Sicherheitszentrums geplant ist, sollte die Integration der Aufgaben einer Cyber–Sicherheitsleitstelle in eine derartige Einrichtung berücksichtigt werden. (TZ 13)

Rechnungshof Österreich

Wien, im Oktober 2024
Die Präsidentin:

Dr. Margit Kraker

Anhang

Ressortbezeichnung und –verantwortliche

Tabelle A: Bundeskanzleramt

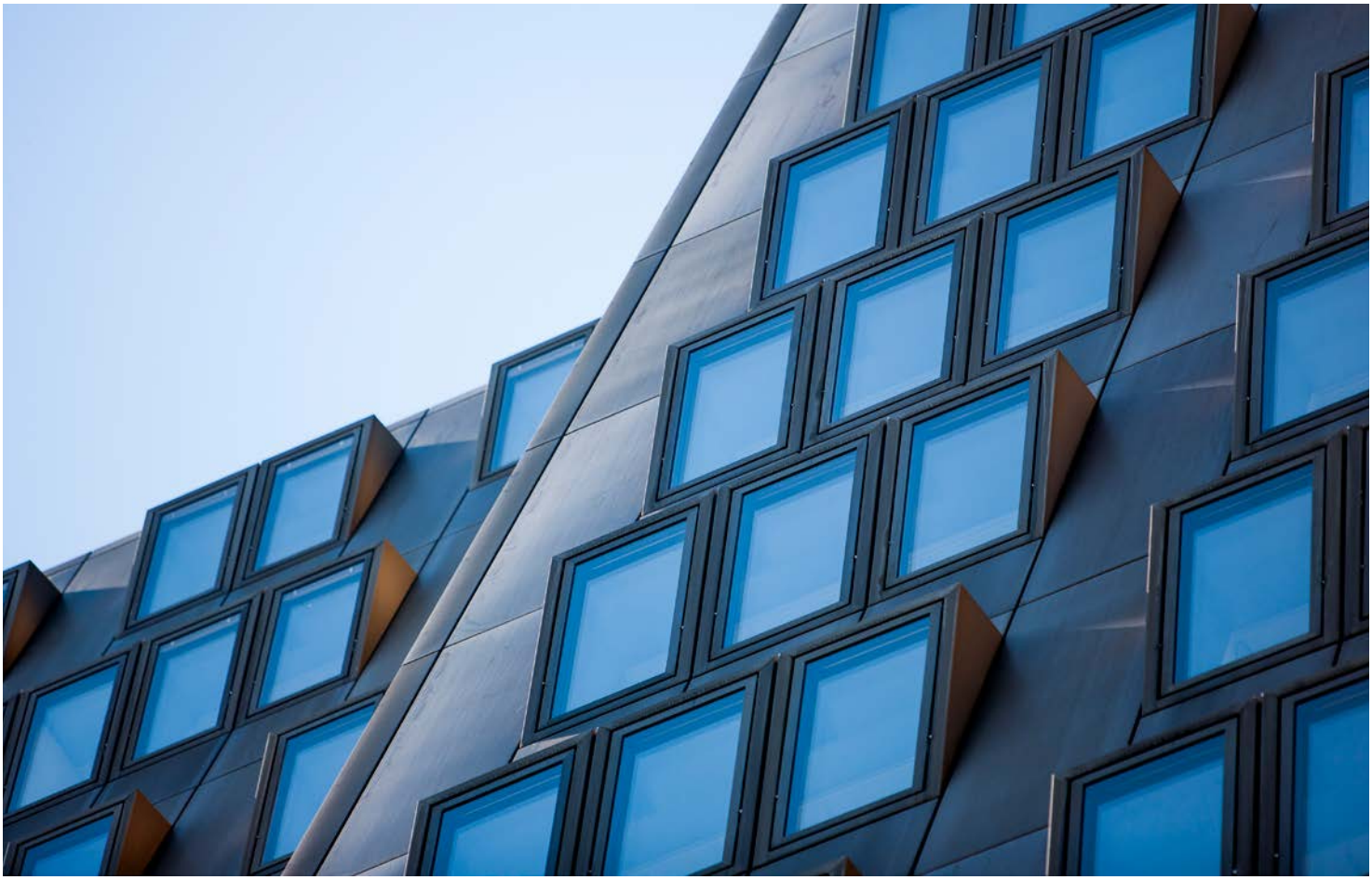
Zeitraum	Bundesministerien-gesetz–Novelle	Ressortbezeichnung	Bundeskanzler
überprüfter Zeitraum	–	Bundeskanzleramt	bis 11. Oktober 2021: Sebastian Kurz
			11. Oktober 2021 bis 6. Dezember 2021: Mag. Alexander Schallenberg, LL.M.
			seit 6. Dezember 2021: Karl Nehammer, MSc

Quelle: Parlament; Zusammenstellung: RH

Tabelle B: Innenministerium

Zeitraum	Bundesministerien-gesetz–Novelle	Ressortbezeichnung	Bundesminister
überprüfter Zeitraum	–	Bundesministerium für Inneres	bis 6. Dezember 2021: Karl Nehammer, MSc
			seit 6. Dezember 2021: Mag. Gerhard Karner

Quelle: Parlament; Zusammenstellung: RH



	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-10-23T18:01:26+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	