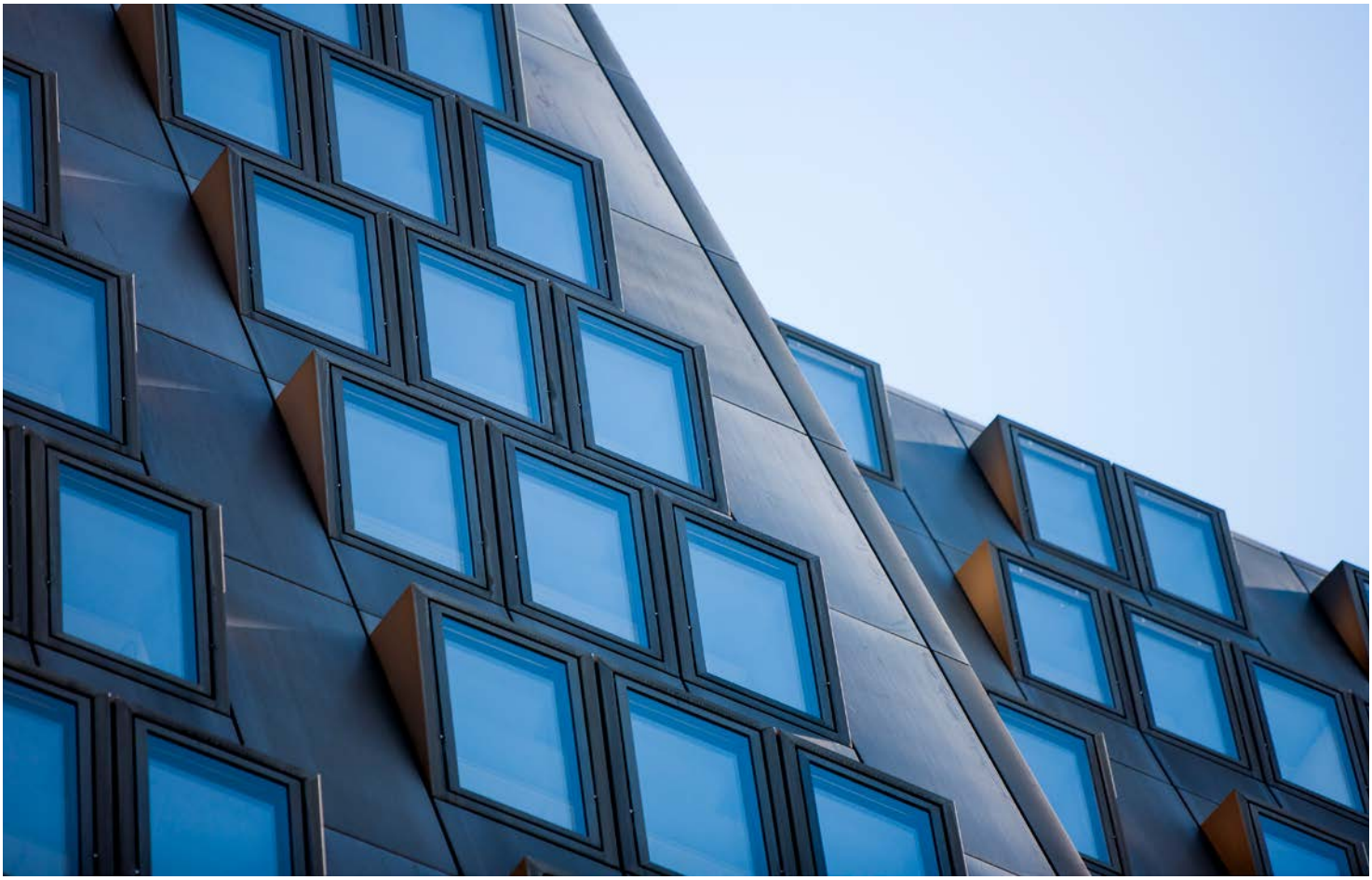
Rechnungshof Österreich

Unabhängig und objektiv für Sie.

Management der IT–Sicherheit im Finanzministerium, Klimaschutz-ministerium und Landwirtschaftsministerium

Reihe BUND 2024/16

Bericht des Rechnungshofes



III–1164 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP
Rechnungshof GZ 2024–0.348.624 (005.097)

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 Mai 2024

AUSKÜNFTE

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

FOTOS

Cover, S. 8: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
Art.	Artikel
BGBl.	Bundesgesetzblatt
BMAW	Bundesministerium für Arbeit und Wirtschaft
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BMF	Bundesministerium für Finanzen
BMG	Bundesministeriengesetz 1986
BMI	Bundesministerium für Inneres
BMK	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
BML	Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft
BMLRT	Bundesministerium für Landwirtschaft, Regionen und Tourismus
BMNT	Bundesministerium für Nachhaltigkeit und Tourismus
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BRZ GmbH	Bundesrechenzentrum Gesellschaft mit beschränkter Haftung
bzw.	beziehungsweise
COVID	corona virus disease (Coronaviruskrankheit)
ELAK	elektronischer Akt, elektronisches Aktenverwaltungssystem
etc.	et cetera
EU	Europäische Union
EUR	Euro
(f)f.	folgend(e)
G(es)mbH	Gesellschaft mit beschränkter Haftung
Hrsg.	Herausgeber
i.d.(g.)F.	in der (geltenden) Fassung
IKT	Informations– und Kommunikationstechnologie
InfoSiG	Informationssicherheitsgesetz
IP	Internetprotokoll
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IT	Informationstechnologie

lit.	litera (Buchstabe)
Mio.	Million
NIS	Netz– und Informationssystemsicherheit
NISG	Netz– und Informationssystemsicherheitsgesetz
PC	Personalcomputer
PIN	Personal Identification Number
rd.	rund
RH	Rechnungshof
S.	Seite
TZ	Textzahl
u.a.	unter anderem
USB	Universal Serial Bus
VPN	Virtual Private Network
Z	Ziffer
z.B.	zum Beispiel

Ein hohes Maß an IT–Sicherheit zu gewährleisten stellt für die öffentliche Verwaltung eine zentrale Aufgabe dar. Dies insbesondere, um die öffentliche Leistungserbringung aufrechterhalten zu können. Das Finanzministerium, das Klimaschutzministerium und das Landwirtschaftsministerium hatten in unterschiedlichem Ausmaß wichtige technische Maßnahmen im Bereich der IT–Sicherheit am IT–Arbeitsplatz sowie im Bereich der zentralen IT–Systeme umgesetzt. Als kritische Phase für die durchgängige Gewährleistung der IT–Sicherheit zeigte sich der Zeitraum der Verschiebung von IT–Arbeitsplätzen nach ressortübergreifenden Zuständigkeitsänderungen und der Überleitung auf die IT–Sicherheitsstrategie des aufnehmenden Bundesministeriums.

Im August 2020 beauftragten die Generalsekretäre auf Grundlage eines Ministerratsbeschlusses das Programm IT–Konsolidierung. Das Programm–Management nahm im überprüften Zeitraum das Digitalisierungsministerium – bzw. ab Juli 2022 das Finanzministerium – mit dem Bundeskanzleramt wahr. Zum Stand Juni 2023 war keines der IT–Projekte, die aus dem Programm hervorgegangen waren, umgesetzt.

Die Österreichische Cybersicherheitsstrategie (2021) und das Österreichische Informationssicherheitshandbuch (2023) waren aktuell; zum Stand Juni 2023 gab es jedoch keine einheitlichen Sicherheitsstandards für die IT der Bundesverwaltung, obwohl das Regierungsprogramm 2020–2024 und die Empfehlung des Nationalen Sicherheitsrates bereits im Jahr 2020 die Notwendigkeit solcher Standards dokumentiert hatten. Auch das im Rahmen des Programms IT–Konsolidierung beauftragte Projekt Security Framework Bund befand sich erst im Anfangsstadium.

Handlungsbedarf für die Zukunft sieht der RH insbesondere durch die neue NIS–2–Richtlinie der EU über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau. Diese Richtlinie ist bis Oktober 2024 in nationales Recht umzusetzen. Sie erfordert eine Erhöhung der IT–Sicherheitsmaßnahmen in öffentlichen Einrichtungen, insbesondere im Bereich Risiko– und Notfallmanagement.

WIRKUNGSBEREICH

- Bundesministerium für Finanzen
- Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
- Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft

Management der IT–Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium

Prüfungsziel

Der RH überprüfte von Februar bis Mai 2023 ausgewählte Aspekte des Managements der IT–Sicherheit im Finanzministerium, im Klimaschutzministerium und im Landwirtschaftsministerium. Der überprüfte Zeitraum umfasste insbesondere die Jahre 2018 bis 2022.

Mit der Verschiebung von Kompetenzen zwischen diesen Ressorts wurden im überprüften Zeitraum auch IT–Arbeitsplätze verschoben. Die Gebarungsüberprüfung befasste sich daher auch mit der Integration der betreffenden IT–Arbeitsplätze in den jeweiligen neuen Ressorts. (TZ 1)

Kurzfassung

Laut der Studie „Cybersecurity in Österreich 2023“ nahmen Cyber–Angriffe 2023 gegenüber 2022 um rd. 200 % zu. Ein hohes Maß an IT–Sicherheit zu gewährleisten, stellt für die öffentliche Verwaltung eine zentrale Aufgabe dar. Dies insbesondere, um die öffentliche Leistungserbringung aufrechterhalten zu können. (TZ 2)

IT–Betreuung und Zuständigkeit

Gemäß Bundesministeriengesetz war das Bundeskanzleramt u.a. für Angelegenheiten der strategischen Netz– und Informationssicherheit (gemäß Netz– und Informationssystemsicherheitsgesetz – **NISG**) zuständig. Die Koordination und zusammenfassende Behandlung in Angelegenheiten der Informationstechnologie waren dem für Digitalisierungsangelegenheiten zuständigen Bundesministerium zugewiesen (das war bis zur Bundesministeriengesetz–Novelle 2022 das Digitalisierungs-

ministerium, von Juli 2022 bis April 2024 das Finanzministerium und ab Mai 2024 das Bundeskanzleramt). Für die ressorteigene IT und die IT–Sicherheit war hingegen jedes Bundesministerium selbst verantwortlich; eine Kompetenz zur Koordination der IT–Sicherheit war im Bundesministeriengesetz nicht ausdrücklich erwähnt. (TZ 3)

Bundesministeriengesetz–Novellen führten 2018 bis 2022 mehrmals zu umfassenden Verschiebungen von Zuständigkeiten zwischen den Bundesministerien; das beinhaltete die Organisationseinheiten, ihre Bediensteten, die IT–Arbeitsplätze und IT–Fachanwendungen. Die daraus folgende Verschiebung von IT–Arbeitsplätzen und die Überleitung auf die IT–Sicherheitsstrategie des aufnehmenden Bundesministeriums war eine kritische Phase für die durchgängige Gewährleistung der IT–Sicherheit. (TZ 3)

Im Jänner 2020 und Juli 2022 waren die drei überprüften Bundesministerien – Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium – von solchen Kompetenzänderungen betroffen. Die Integration der neu einzugliedernden bzw. das Herauslösen der abzugebenden Organisationseinheiten waren mit hohem Arbeitsaufwand verbunden und dauerten jeweils bis zu rund einem Jahr bzw. bei einigen Fachapplikationen noch länger. (TZ 4)

IT–Konsolidierung

Mit dem IKT–Konsolidierungsgesetz bestand seit 2012 die Grundlage für die Zusammenführung und Vereinheitlichung der Informations– und Kommunikationstechnologie (**IKT**) des Bundes. Dennoch fehlte zum Stand Juni 2023 die zur näheren Ausführung des IKT–Konsolidierungsgesetzes vorgesehene Verordnung; zuständig dafür war das Bundesministerium, in dessen Kompetenz die Digitalisierung fiel (bis Juli 2022 das Bundesministerium für Digitalisierung und Wirtschaftsstandort, von Juli 2022 bis April 2024 das Finanzministerium, ab Mai 2024 das Bundeskanzleramt). (TZ 5)

Im August 2020 beauftragten die Generalsekretäre auf Grundlage eines Ministerratsbeschlusses aus 2019 das Programm IT–Konsolidierung. Das Programm–Management sollte das Digitalisierungsministerium und von Juli 2022 bis April 2024 das die Digitalisierungsagenden übernehmende Finanzministerium gemeinsam mit dem Bundeskanzleramt stellen; die entsprechende Position im Finanzministerium war von Jänner 2023 bis Mitte Juni 2023 unbesetzt. Im Juni 2023, drei Jahre nach dem Auftrag vom August 2020, war keines der Projekte zur IT–Konsolidierung umgesetzt:

- Bei den Projekten „Standardarbeitsplatz und sichere Basisdienste“ sowie „Hotline/Service Desk“ waren die Analyse und Konzeption abgeschlossen. Der Lenkungsausschuss hatte aber die bundesweite Umsetzung eines derartig umfassenden Projekts

als nicht erfolgversprechend eingeschätzt; die Erkenntnisse der Analyse und Konzeption sollen in nachfolgenden Projekten berücksichtigt werden.

- Fünf Projekte des Programms IT–Konsolidierung befanden sich im Juni 2023 in der Analyse– und Konzeptionsphase: Für zwei dieser Projekte war keine Umsetzungsphase mehr vorgesehen; bei drei Projekten hatte der Lenkungsausschuss noch nicht über ihre Umsetzung entschieden. (TZ 6)

Grundlagen der IT–Sicherheit

Technische Vorgaben

Die Österreichische Cybersicherheitsstrategie (2021) und das Österreichische Informationssicherheitshandbuch (2023) waren aktuell. Zum Stand Juni 2023 lagen jedoch keine einheitlichen Sicherheitsstandards für die IT der Bundesverwaltung vor, obwohl das Regierungsprogramm 2020–2024 und die Empfehlung des Nationalen Sicherheitsrates bereits im Jahr 2020 die Notwendigkeit solcher Standards dokumentiert hatten. (TZ 7)

Rechtliche Vorgaben und Entwicklung

Die unterschiedlichen rechtlichen Grundlagen für klassifizierte Informationen – Informationssicherheitsgesetz sowie Geheimschutzordnung des Bundes – waren nicht harmonisiert. (TZ 8)

Bis Oktober 2024 ist die NIS–2–Richtlinie der EU – über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau – in nationales Recht umzusetzen. Diese Richtlinie erfordert eine Erhöhung der IT–Sicherheitsmaßnahmen in öffentlichen Einrichtungen, insbesondere im Bereich Risiko– und Notfallmanagement. (TZ 9)

IT–Sicherheitsstrategien der Ministerien

Die ressortweit kundgemachte IT–Sicherheitsstrategie des Finanzministeriums befand sich auf dem aktuellen Stand. Sie verfolgte die wesentlichen Ziele, die für eine umfassende IT–Sicherheit ausschlaggebend sind, und berücksichtigte organisatorische und personelle Aspekte. Die IT–Sicherheitsstrategie des Klimaschutzministeriums stammte aus 2002: Damit entsprachen die IT–Sicherheitspolitik und die Grundsätze der IT–Sicherheit nicht mehr zur Gänze den aktuellen Gegebenheiten. Im Landwirtschaftsministerium war nur die IT–Strategie mit Rundschreiben kundgemacht, nicht jedoch die interne IT–Sicherheitsstrategie mit Zielen, Verantwortlichkeiten und Organisation des IT–Sicherheitsmanagements. Das Klimaschutz– und das Landwirtschaftsministerium erfassten in ihren IT–Sicherheitsstrategien nur teilweise die nachgeordneten Bereiche, das Finanzministerium zur Gänze. (TZ 10)

Risikomanagement

Das Finanzministerium hatte ein umfassendes IT–Risikomanagementsystem eingerichtet. Das Klimaschutz– und das Landwirtschaftsministerium überprüften die vorhandenen Schutzbedarfs– und Risikoanalysen im Anlassfall, aber nicht regelmäßig. Beide Ministerien hatten nach eigener Einschätzung keine wichtigen Dienste im Sinne des NISG identifiziert, obwohl dem Klimaschutzministerium z.B. das Führerscheinregister und das elektronische Datenmanagement nach dem Abfallwirtschaftsgesetz zugeordnet waren und das Landwirtschaftsministerium das Wasserinformationssystem führte. (TZ 11)

Internes Berichtswesen

Ein regelmäßiges und ein anlassbezogenes Berichtswesen zur IT–Sicherheit waren im Finanzministerium standardisiert eingerichtet. Im Klimaschutz– und im Landwirtschaftsministerium erfolgte keine regelmäßige, standardisierte Berichterstattung mit Kennzahlen zur IT–Sicherheit an die obere Führungsebene. (TZ 12)

IT–Sicherheitsorganisation

Die IKT–Abteilungen der drei überprüften Bundesministerien nahmen die IT–Angelegenheiten und das Management der IT–Sicherheit jeweils innerhalb ressortspezifischer organisatorischer Rahmenbedingungen wahr. (TZ 13)

Das Klimaschutzministerium hatte keinen für die Informations– und IT–Sicherheit gesamtverantwortlichen Chief Information Security Officer (CISO) eingerichtet. Im Landwirtschaftsministerium war die Rolle des Chief Information Security Officers mit der Rolle des IT–Abteilungsleiters (Chief Information Officer – CIO) ident und damit nicht unabhängig. (TZ 14)

Das Informationssicherheitsmanagement–Team im Klimaschutzministerium entsprach in der eingerichteten Form nicht den Vorgaben der eigenen IT–Sicherheitspolitik. (TZ 15)

IT–Sicherheit und Telearbeit

Aufbauend auf der Standard–Softwarebüroausstattung der Bundesverwaltung („Bundesclient–Architektur“) installierten die überprüften Bundesministerien jeweils auch ressortspezifische IT–Anwendungen. Auf den mobilen Arbeitsplatzrechnern war ein gesicherter Zugriff auf das ressorteigene Netzwerk installiert. Ende Dezember 2022 besaßen die drei Ministerien eine für Telearbeit geeignete Ausstattung mit mobilen dienstlichen IT–Arbeitsplätzen (Laptops) für alle Bediensteten, teilweise auch mit dienstlichen Mobiltelefonen. (TZ 16)

Zusätzlich zu den IT–Sicherheitsrisiken eines IT–Arbeitsplatzes an der Dienststelle ergaben sich bei der Telearbeit weitere spezifische Risiken. Zu diesen zählten etwa der Verlust der mobilen IT–Ausstattung, ein unbemerkter Zugang nicht berechtigter Personen zu den mobilen Arbeitsplatzrechnern, das Ausspähen von Zugangsdaten oder eine allfällige, infrastrukturbedingt geringere IT–Sicherheit als beim IT–Arbeitsplatz an der Dienststelle. Das Finanzministerium, das Klimaschutzministerium und das Landwirtschaftsministerium hatten in unterschiedlichem Ausmaß wichtige technische Maßnahmen im Bereich IT–Sicherheit am IT–Arbeitsplatz umgesetzt. (TZ 17)

Die Bediensteten authentifizierten sich in den drei Bundesministerien am IT–Arbeitsplatz mit Benutzername und Passwort. Zusätzlich war im Finanzministerium im Sinne der Zwei–Faktor–Authentifizierung die chipbasierte Dienstkarte erforderlich; in den beiden anderen Bundesministerien war jeweils nur ein gerätespezifisches Kennwort einzugeben. (TZ 18)

In den drei überprüften Bundesministerien waren mit Stand 2023 insgesamt fünf unterschiedliche Videokonferenzsysteme im Einsatz. Das 2021 gestartete Projekt „Videokonferenzsystem Bund“, das ursprünglich bis Ende 2021 abgeschlossen sein sollte, hatte eine einheitliche Videokonferenzlösung zum Ziel. Es sollte gemäß aktualisierter Planung im Sommer 2023 in Betrieb gehen; an der Behebung eines technischen Problems wurde zum Ende der Gebarungsüberprüfung noch gearbeitet. (TZ 19)

Die drei überprüften Bundesministerien regelten die Informations– und Datensicherheit in allgemeinen Richtlinien zur Informations– und Datensicherheit und in Telearbeitsrichtlinien. Diese brachten sie den Bediensteten mit Schreiben und zusätzlich auf ressortinternen Informationsplattformen zur Kenntnis. (TZ 20)

IT–Sicherheit Personal

Das Finanzministerium, das Klimaschutzministerium und das Landwirtschaftsministerium legten die wesentlichen Regelungen zum Management der personellen IT–Sicherheit fest. Das Landwirtschaftsministerium machte jedoch keine Vorgaben zum Umgang mit klassifizierten Informationen. (TZ 21)

Die Awareness–Schulungen für IT–Sicherheit im Finanzministerium waren verpflichtend; nach der Integration der im Juli 2022 neu übernommenen Bereiche hatten in der Zentralstelle – also ohne nachgeordnete Stellen – mit Stand 1. April 2023 erst 60 % der Bediensteten die Schulungen absolviert; das Klimaschutzministerium hatte das Thema „IT–Sicherheit im Arbeitsalltag“ noch nicht in seine Schulungen integriert; die Schulungen des Landwirtschaftsministeriums waren lediglich freiwillig. (TZ 22)

Das Finanzministerium, das Klimaschutzministerium und das Landwirtschaftsministerium bezogen IT–Dienstleistungen von externen Unternehmen in unterschiedlichem Ausmaß. Das Klimaschutzministerium setzte zur Server–Betreuung externes Personal mit permanenten Fernwartungszugriffen und privilegierten Rechten ein. Dies barg IT–Sicherheitsrisiken, die durch einen zeitlich begrenzten und anlassbezogenen Zugriff minimiert werden könnten. (TZ 23)

IT–Sicherheit der Infrastruktur

Ziel von technischen und organisatorischen Maßnahmen im Bereich IT–Sicherheit ist es, die Sicherheit der zentralen IT–Komponenten bzw. der IT–Anwendungen zu erhöhen. Dabei sollten Maßnahmen eingesetzt werden, die unter Berücksichtigung von Kosten–Nutzen–Erwägungen erwarten lassen, dass ein hohes Sicherheitsniveau erreicht wird. Das Finanzministerium, das Klimaschutzministerium und das Landwirtschaftsministerium hatten in unterschiedlichem Ausmaß wichtige technische Maßnahmen für die IT–Sicherheit der zentralen IT–Systeme umgesetzt. (TZ 24)

Das Finanzministerium konnte IT–Sicherheitsrisiken durch die zahlreich durchgeführten IT–Sicherheitsüberprüfungen in hohem Ausmaß detektieren, analysieren und durch geeignete Maßnahmen reduzieren. Die IT–Sicherheitsüberprüfungen des Klimaschutz– und des Landwirtschaftsministeriums deckten nicht alle Bereiche ab; es waren dabei größtenteils keine externen Expertinnen und Experten eingebunden. (TZ 25)

Das Finanzministerium richtete ein umfangreiches Notfallmanagement für die eingesetzten IT–Verfahren ein. Das Notfallhandbuch bzw. die Notfallkonzepte des Klimaschutzministeriums stammten aus 2005 und entsprachen somit nicht mehr den aktuellen IT–Systemen. Das Landwirtschaftsministerium hatte noch kein umfassendes Notfallhandbuch oder ein ähnliches Konzept in Kraft gesetzt. (TZ 26)

Die Datensicherungs– und Wiederherstellungskonzepte des Klimaschutzministeriums bzw. des Landwirtschaftsministeriums stammten aus den Jahren 2013 bzw. 2015 und wurden seitdem nicht mehr aktualisiert. (TZ 27)

Das Finanzministerium ließ das Notfallmanagement neben den regelmäßigen Testungen auch mithilfe von externen Audits überprüfen. Auch das Klimaschutz– und das Landwirtschaftsministerium testeten ihre Notfallszenarien, externe Audits wurden dazu jedoch nicht durchgeführt. (TZ 28)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

ZENTRALE EMPFEHLUNGEN

- Das für die Koordination der IT zuständige Bundeskanzleramt sollte die nötige Teilnahme der Bundesministerien an der Umsetzung der im Projekt Security Framework Bund zu erarbeitenden Sicherheitsstandards fördern. Dies wäre über eine Einbeziehung in die Themen der Konferenz der Generalsekretäre bzw. eines gleichwertigen Gremiums (aus den internen administrativen Spitzen der Bundesministerien) zu begleiten. (TZ 7)

- Das Bundesministerium für Finanzen, das Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie und das Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft sollten sich auf die Anforderungen durch die Umsetzung der 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) vorbereiten und den nationalen Umsetzungsprozess begleiten, um die wesentlichen Themen – wie Risikomanagement, Notfallvorsorge, Krisenmanagement, Verantwortung der Ressortleitung – ressortintern zeitgerecht zu berücksichtigen. (TZ 9)

- Das Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie und das Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft sollten ihre jeweiligen Authentifizierungsmethoden für die IT–Arbeitsplätze einer Risikoanalyse unterziehen, den Bedarf nach einer Zwei–Faktor–Authentifizierung prüfen und diese allenfalls einsetzen. (TZ 18)

- Das Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie und das Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft sollten zunächst den Bedarf an IT–Sicherheitsüberprüfungen basierend auf einer umfassenden Risikoanalyse erheben, sodann die notwendigen IT–Sicherheitsüberprüfungen priorisieren und diese Überprüfungen schließlich zeitnah unter Berücksichtigung der verfügbaren Ressourcen sowie bedarfsgerecht unter Einbindung von externem Fachwissen durchführen. (TZ 25)

- Das Bundesministerium für Finanzen, das Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie und das Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft sollten in Bezug auf Telearbeit konkret festlegen, ob bestimmte dienstliche Aufgaben jedenfalls aus Sicherheitsgründen an der Dienststelle zu verrichten sind. (TZ 20)

Zahlen und Fakten zur Prüfung

Management der IT–Sicherheit im Finanz–, Klimaschutz– und Landwirtschaftsministerium						
Rechtsgrundlagen	Netz– und Informationssystemsicherheitsgesetz (NISG), BGBl. I 111/2018 Datenschutz–Grundverordnung (DSGVO), Verordnung (EU) 2016/679, ABl. L 2016/119, 1 Informationssicherheitsgesetz (InfoSiG), BGBl. I 23/2002 i.d.g.F. Informationssicherheitsverordnung (InfoSiV), BGBl. II 548/2003 i.d.g.F.					
	Finanzministerium		**Klimaschutzministerium**		**Landwirtschaftsministerium**	
	Anzahl Vollbeschäftigungsäquivalente in den IKT–Abteilungen (zum 31. Dezember)					
	intern[1]	extern[1]	intern	extern[2]	intern	extern
2018	128,48	51	23	8 (3)	30,58	5
2019	137,25	39	23	8 (3)	27,73	5
2020	137,43	37	26	11 (6)	28,73	5
2021	133,78	39	28	13 (7)	28,78	5
2022	204,00	137	28	12 (6)	31,83	6
	Anzahl 2018 bis 2022					
durchgeführte IT–Sicherheitsüberprüfungen	255 davon 3 intern[3]		65 davon 57 intern		7 davon 5 intern	
	Anteil in %					
Anteil der Arbeitsplätze mit dienstlicher, für Telearbeit geeigneter IT–Ausstattung zum 31. Dezember 2022	100		100		100	
Anteil der Bediensteten mit Anordnung/Vereinbarung zur regelmäßigen Telearbeit zum 31. Dezember 2022	48		70		31	
Anteil jener Bediensteten, die regelmäßige oder anlassbezogene Telearbeit in Anspruch nahmen (im Dezember 2022)	69		62		72	

IKT = Informations– und Kommunikationstechnologie

Quellen: BMF; BMK; BML

[1] Alle IT–Abteilungen des Finanzministeriums; das waren von 2018 bis 2021 die Abteilungen GS/PM, I/10, I/11, II/11, II/12 und im Jahr 2022 die Abteilungen Präs. 6, I/10, I/11, II/11, II/12, V/1, V/2, V/3, V/4, V/5, V/6 und V/8.

[2] in Klammer davon Arbeitsleihen eines privaten Personalserviceunternehmens

[3] zusätzlich 27.045 Schwachstellen–Scans

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von Februar 2023 bis Mai 2023 ausgewählte Aspekte des Managements der IT–Sicherheit im Bundesministerium für Finanzen (in der Folge: **Finanzministerium**), im Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (in der Folge: **Klimaschutzministerium**) und im Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft (in der Folge: **Landwirtschaftsministerium**). Die nachgeordneten Dienststellen dieser Ressorts[1] wurden nur in Einzelfällen behandelt.

Aufgrund der Bundesministeriengesetz–Novelle 2024[2] übernahm das Bundeskanzleramt ab 1. Mai 2024 – und damit nach Abgabe der Stellungnahme durch das Finanzministerium – die Digitalisierungsangelegenheiten inklusive der Verantwortung für die IT–Konsolidierung vom Finanzministerium. Jene Empfehlungen, die Digitalisierungsangelegenheiten betreffen (TZ 3, TZ 5, TZ 6, TZ 7, TZ 19) und aus Feststellungen zum Finanzministerium resultieren, richtet der RH daher nunmehr an das Bundeskanzleramt.

Die Gebarungsüberprüfung orientierte sich an Aspekten, die der RH bereits im Zuge seiner Prüfungen „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“[3] (Reihe Bund 2021/31) sowie „Dienstrechtliche und technische Umsetzung von Telearbeit in ausgewählten Bundesministerien“ (Reihe Bund 2022/27) in anderen Ressorts überprüft hatte.

Der überprüfte Zeitraum umfasste insbesondere die Jahre 2018 bis 2022. Soweit erforderlich nahm der RH auch auf frühere Entwicklungen Bezug.

[1] Der RH verwendet in diesem Bericht den Begriff (Bundes–)Ministerium für die Zentralstelle ohne nachgeordnete Dienststellen, den Begriff Ressort für Zentralstelle und nachgeordnete Dienststellen.

[2] BGBl. I 44/2024

[3] Bundeskanzleramt, Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport, Bundesministerium für Digitalisierung und Wirtschaftsstandort, Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz

Im überprüften Zeitraum änderten sich durch mehrere Novellen des Bundesministeriengesetzes 1986 (**BMG**)[4] die Zuordnung von Angelegenheiten zu den überprüften Bundesministerien (siehe dazu Tabelle 2 in TZ 3) und – wie in folgender Tabelle abgebildet – teilweise die Bezeichnung dieser Ministerien:

Tabelle 1: Bezeichnung der überprüften Bundesministerien im Zeitraum 2018 bis 2022

Bezeichnung laut Bundesministeriengesetz 1986			Bezeichnung im RH–Bericht
bis 28. Jänner 2020	von 29. Jänner 2020 bis 17. Juli 2022	ab 18. Juli 2022	
Bundesministerium für Finanzen (BMF)	Bundesministerium für Finanzen (BMF)	Bundesministerium für Finanzen (BMF)	Finanzministerium
Bundesministerium für Verkehr, Innovation und Technologie (BMVIT)	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK)	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK)	Klimaschutzministerium
Bundesministerium für Nachhaltigkeit und Tourismus (BMNT)	Bundesministerium für Landwirtschaft, Regionen und Tourismus (BMLRT)	Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft (BML)	Landwirtschaftsministerium

Quelle: Bundesministeriengesetz 1986

Ziel der Gebarungsüberprüfung war es, die Konzeption und Umsetzung ausgewählter Aspekte des Managements der IT–Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium darzustellen und zu beurteilen. Dies betraf insbesondere die Themen IT–Sicherheitsstrategie, IT–Sicherheitsorganisation, IT–Sicherheit beim Personal sowie IT–Sicherheit der Infrastruktur.

Mit der Verschiebung von Kompetenzen zwischen den Ressorts wurden im überprüften Zeitraum auch IT–Arbeitsplätze verschoben. Die Gebarungsüberprüfung befasste sich daher auch mit der Integration der betreffenden IT–Arbeitsplätze in die jeweiligen neuen Ressorts. Hier stellte insbesondere die Phase des Übergangs der IT–Betreuung eine Herausforderung bei der Gewährleistung der IT–Sicherheit dar.

Nicht Thema der Gebarungsüberprüfung war das Management der IT–Sicherheit bei den Dienstleistern (z.B. Bundesrechenzentrum Gesellschaft mit beschränkter Haftung (**BRZ GmbH**)) und bei den nachgeordneten Dienststellen der überprüften Bundesministerien.

[4] BGBl. 76/1986 i.d.g.F.; hier angesprochene Novellen: BGBl. I 8/2020, in Kraft getreten am 29. Jänner 2020; BGBl. I 98/2022, in Kraft getreten am 18. Juli 2022

(2) Im Jahr 2015 beschlossen die 193 Mitgliedstaaten der Vereinten Nationen die sogenannte Agenda 2030 („Transformation unserer Welt: die Agenda 2030 für nachhaltige Entwicklung“). Österreich verpflichtete sich, bis zum Jahr 2030 auf die Umsetzung der 17 nachhaltigen Entwicklungsziele („Sustainable Development Goals“ (**SDG**)), die durch 169 Unterziele konkretisiert waren, hinzuarbeiten. Wesentlich für die in der Gebarungsüberprüfung behandelten Themen ist das SDG 9, mit welchem eine widerstandsfähige Infrastruktur aufgebaut, breitenwirksame und nachhaltige Industrialisierung gefördert und Innovationen unterstützt werden sollen.

(3) Zu dem im November 2023 übermittelten Prüfungsergebnis nahmen das Klimaschutzministerium im Jänner 2024, das Finanz– und das Landwirtschaftsministerium im Februar 2024 Stellung. Der RH erstattete seine Gegenäußerungen im Mai 2024.

(4) Das Klimaschutzministerium gab in seiner Stellungnahme an, dass allgemein die Feststellungen des RH nachvollziehbar seien. Einige Empfehlungen würden neben einer Erhöhung der IKT–Sicherheit auch eine Einschränkung der Bedienbarkeit der IKT–Systeme darstellen; bei diesen Empfehlungen sei zu evaluieren, wie der Zielkonflikt Sicherheit versus Bedienbarkeit am besten zu lösen wäre. Die Empfehlungen des RH würden jedenfalls in die Planungen für die kommenden Jahre einfließen, mit der Umsetzung einiger Empfehlungen sei bereits begonnen worden. Darüber hinaus gab das Klimaschutzministerium keine Stellungnahme ab.

IT–Sicherheit im öffentlichen Bereich (Sicherheitsvorfälle)

2 (1) Im Jahr 2023 veröffentlichte ein Beratungsunternehmen gemeinsam mit dem Sicherheitsforum Digitale Wirtschaft Österreich des Kompetenzzentrums Sicheres Österreich[5] die Studie „Cybersecurity in Österreich“[6]. Gemäß dieser Studie hatten 2023 gegenüber 2022 Cyber–Angriffe um rd. 200 % zugenommen. 12 % der betroffenen Unternehmen erlitten einen finanziellen Schaden von jeweils mehr als 1 Mio. EUR. 33 % mussten ihren Betrieb aufgrund von Cyber–Angriffen mehrere Tage bis Wochen unterbrechen. Zugenommen hatten in den letzten Jahren insbe-

[5] Nach Angaben des Sicherheitsforums Digitale Wirtschaft Österreich betreibt es eine kooperative Zusammenarbeit zwischen Behörden, Wirtschaft und Wissenschaft und bildet durch die Einbindung von Expertinnen und Experten aus dem strategischen sowie technischen Bereich die Basis für eine nachhaltige sichere Digitalisierung der österreichischen Wirtschaft.

[6] KPMG Security Services GmbH (Hrsg.), Cybersecurity in Österreich (2023)

sondere Cyber–Attacken aus dem Bereich Identitätsdiebstahl[7], Datendiebstahl im Zusammenhang mit Ransomware–Aktivitäten[8] und Social Engineering[9].

(2) Auch die öffentliche Verwaltung war in der Vergangenheit von Cyber–Angriffen betroffen. In den vergangenen Jahren war ein stetiger Anstieg schwerwiegender Vorfälle zu verzeichnen (2020: neun, 2021: 13, 2022: 16). Ein Sicherheitsvorfall betraf z.B. das Land Kärnten, einer das Außenministerium.

Auch das Computer Emergency Response Team für die öffentliche Verwaltung (GovCERT)[10] verzeichnete 2023 einen weiteren Anstieg der entsprechenden Meldungen; so wurden bereits in den ersten drei Monaten 2023 mehr als 50 Sicherheitsvorfälle bzw. –probleme gemeldet. Davon waren fünf als schwerwiegender Vorfall einzustufen.

(3) Die drei überprüften Bundesministerien waren im überprüften Zeitraum 2018 bis 2022 ebenfalls von Sicherheitsvorfällen betroffen:

- Zwei der Bundesministerien erstatteten Meldung über Sicherheitsvorfälle nach dem Netz– und Informationssystemsicherheitsgesetz[11] (**NISG**) (TZ 8).
- Es traten auch Sicherheitsvorfälle in Form von Attacken auf IT–Services, von Verbindungsproblemen aufgrund von Leitungsausfällen, von Sicherheits–Zertifikatproblemen (für die Nutzung beim Telearbeits–Zugang sowie bei Videokonferenz–Zugängen), Fehlkonfigurationen von Netzwerkkomponenten, Datenverschlüsselung oder auch Datenschutzverletzungen auf.

Ein hohes Maß an IT–Sicherheit zu gewährleisten stellt für die öffentliche Verwaltung eine zentrale Aufgabe dar. Dies insbesondere, um die öffentliche Leistungserbringung aufrechterhalten zu können.

7 Identitätsdiebstahl ist laut Definition der Studie der rechtswidrige Zugriff auf persönliche Identifikationsinformationen einer Person, z.B. auf die Sozialversicherungsnummer oder auf das Geburtsdatum, um dann in betrügerischer Absicht illegale Handlungen auszuführen.

8 Ransomware zielt laut Definition der Studie darauf ab, den Zugriff auf wichtige Dateien oder Systeme zu sperren oder zu verschlüsseln und Lösegeld zu fordern.

9 Beim Social Engineering setzen laut Definition der Studie Angreiferinnen und Angreifer psychologische Techniken ein, um Personen dazu zu bringen, vertrauliche Informationen preiszugeben, unerlaubten Zugang zu Systemen zu gewähren oder bestimmte Handlungen auszuführen.

10 Die Kernfunktion des GovCERT ist die Koordination zwischen den einzelnen Stellen der öffentlichen Verwaltung. Dies beinhaltet u.a. die Sammlung und Bewertung von Vorfällen aus dem operativen IKT–Betrieb der Bundes–, Landes–, Stadt– und Gemeindeverwaltungen.

11 BGBl. I 111/2018

IT–Betreuung

Änderung der Ressortkompetenzen

3.1 (1) BMG–Novellen[12] führten im überprüften Zeitraum mehrmals zur Verschiebung von Kompetenzen zwischen den Bundesministerien. Die BMG–Novelle 2020 war auf eine Regierungsneubildung infolge der Nationalratswahl im Jahr 2019 zurückzuführen; Grund für die darauffolgenden Kompetenzverschiebungen waren Regierungsumbildungen und daraus resultierende Wechsel von Bundesministerinnen und –ministern. Die folgende Tabelle 2 fasst jene Kompetenzänderungen zusammen, die die überprüften Bundesministerien im überprüften Zeitraum 2018 bis 2022 betrafen:

Tabelle 2: Kompetenzänderungen betreffend das Finanz–, das Klimaschutz– und das Landwirtschaftsministerium durch Novellen des Bundesministeriengesetzes 1986 im Zeitraum 2018 bis 2022

Kompetenz nach Bundesministeriengesetz	Bundesministerium (für)			
	ab 8. Jänner 2018	ab 29. Jänner 2020	ab 1. Februar 2021[1]	ab 18. Juli 2022
Digitalisierung[2]	Digitalisierung und Wirtschaftsstandort	Digitalisierung und Wirtschaftsstandort	Digitalisierung und Wirtschaftsstandort	Finanzen
Klima– und Umweltschutz	Nachhaltigkeit und Tourismus	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Energiewesen	Nachhaltigkeit und Tourismus	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bergwesen	Nachhaltigkeit und Tourismus	Landwirtschaft, Regionen und Tourismus	Landwirtschaft, Regionen und Tourismus	Finanzen
Tourismus	Nachhaltigkeit und Tourismus	Landwirtschaft, Regionen und Tourismus	Landwirtschaft, Regionen und Tourismus	Arbeit und Wirtschaft
Zivildienst	Inneres	Landwirtschaft, Regionen und Tourismus	Landwirtschaft, Regionen und Tourismus	Bundeskanzleramt[3]
Post– und Telekommunikationswesen	Verkehr, Innovation und Technologie	Landwirtschaft, Regionen und Tourismus	Landwirtschaft, Regionen und Tourismus	Finanzen

[1] keine Kompetenzverschiebungen mit zweiter BMG–Novelle 2021 (BGBl. I 148/2021)
[2] Ab Mai 2024 übernahm das Bundeskanzleramt diese Angelegenheiten aufgrund der BMG–Novelle 2024 (BGBl. I 44/2024).
[3] Zuständigkeitsbereich der Staatssekretärin

Quelle: Bundesministeriengesetz 1986

(2) Die Verschiebung von Kompetenzen zwischen den Ressorts machte es auch erforderlich, die zuständigen Organisationseinheiten und ihre Bediensteten sowie die zugehörigen IT–Arbeitsplätze zu übertragen.

[12] Jänner 2018: BGBl. I 164/2017; Jänner 2020: BGBl. I 8/2020; Juli 2022: BGBl. I 98/2022

Diese Migration der IT–Arbeitsplätze verlangte jeweils,

1. die IT–Ausstattung der Arbeitsplätze der übernommenen Bediensteten mit jener des aufnehmenden Bundesministeriums zu vereinheitlichen,

2. die mit den übertragenen Zuständigkeiten verbundenen IT–Fachanwendungen im aufnehmenden Bundesministerium zu integrieren und dafür eine eigene IT–Betreuung sicherzustellen oder externe Dienstleister einzusetzen und

3. die eigene IT–Sicherheitsstrategie und die darauf aufbauenden technischen Methoden und Produkte auf die neue IT–Ausstattung der Arbeitsplätze, IT–Fachanwendungen und deren IT–Infrastruktur anzuwenden.

Der Migrationsprozess dauerte in den drei überprüften Bundesministerien bis zu einem Jahr (TZ 4). Während dieses Zeitraums übernahmen die IT–Abteilungen der abgebenden Bundesministerien weiterhin die Betreuung der IT–Arbeitsplätze und waren für die IT–Sicherheit verantwortlich. Das aufnehmende Ministerium hatte in dieser Phase der Migration für die neuen IT–Arbeitsplätze und Fachanwendungen die Risikoanalysen durchzuführen und die spezifischen technischen und organisatorischen Sicherheitsmaßnahmen umzusetzen.

(3) Angelegenheiten der ressorteigenen IT und IT–Sicherheit oblagen im überprüften Zeitraum gemäß BMG[13] jedem Bundesministerium selbst. Die Kompetenz für Angelegenheiten der strategischen Netz– und Informationssystemsicherheit lag beim Bundeskanzleramt. Die Kompetenz zur Koordination der IT war bis zur BMG–Novelle 2022[14] im Bundesministerium für Digitalisierung und Wirtschaftsstandort (in der Folge: **Digitalisierungsministerium**) angesiedelt. Das Finanzministerium war danach ab Juli 2022 bis April 2024 für die Koordination und zusammenfassende Behandlung in Angelegenheiten der Informationstechnologien sowie für allgemeine Angelegenheiten der Koordination, der Planung und des Einsatzes der automationsunterstützten Datenverarbeitung zuständig.[15] Die Kompetenz zur Koordination der IT–Sicherheit war hingegen im BMG nicht erwähnt. Damit fehlten eine Koordination der IT–Sicherheit und generelle Identifikation von IT–Sicherheitsrisiken.

[13] Anlage 1 Z 5 BMG

[14] BGBl. I 98/2022

[15] Ab Mai 2024 übernahm das Bundeskanzleramt diese Agenden.

(4) Der RH verwies in diesem Zusammenhang auch auf seinen Bundesrechnungsabschluss 2022[16], in dem er sich bereits kritisch zu den Kompetenzverschiebungen geäußert hatte, insbesondere, dass

- die vielschichtigen Änderungen zwischen Rubriken und Untergliederungen Zeitreihenbrüche verursachten und in den betroffenen Bereichen Vorjahresvergleiche erschwerten bzw. verunmöglichten.
- er mit der mehrmaligen Änderung der Budgetstruktur innerhalb eines sehr kurzen Zeitraums die im Bundeshaushaltsgesetz 2013[17] festgelegten Grundsätze der Budgetklarheit, Transparenz und Sparsamkeit als nicht erfüllt sah, insbesondere weil die Vergleichbarkeit der Gebarung im Zeitverlauf nicht oder nur mit erheblichem Erhebungsaufwand möglich war.

3.2 Der RH hielt fest, dass die Verschiebung von Kompetenzen und der zugehörigen IT–Arbeitsplätze zwischen den Bundesministerien die Migration der IT–Ausstattung der Arbeitsplätze, der IT–Fachanwendungen und der IT–Infrastruktur vom abgebenden Bundesministerium in das aufnehmende Bundesministerium notwendig machte. Da das Management der IT–Sicherheit ebenfalls in hohem Maße ressortspezifisch geprägt war, erforderte die Verschiebung der IT–Arbeitsplätze und Fachanwendungen auch, diese auf die IT–Sicherheitsstrategie des aufnehmenden Bundesministeriums und die darauf aufbauenden technischen Methoden und Produkte überzuleiten. Der Zeitraum der Migration der IT–Arbeitsplätze stellte daher eine kritische Phase für die durchgängige Gewährleistung der IT–Sicherheit dar.

Der RH stellte fest, dass das BMG zwar die Kompetenz für die Koordination der IT festlegte, aber die Aspekte der Koordination der IT–Sicherheit nicht ausdrücklich erwähnte. Er hatte bereits in seinem Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 2) dem Bundeskanzleramt und dem damals zuständigen Digitalisierungsministerium empfohlen, eine Regierungsvorlage zu erarbeiten, mit der im BMG eine Kompetenz zur Koordination der IT–Sicherheit klar und ausdrücklich festgelegt wird. Diese Empfehlung war bis zum Ende der Gebarungsüberprüfung im Juni 2023 noch nicht umgesetzt.

Der RH empfahl dem für das BMG sowie seit Mai 2024 auch für die Digitalisierungsangelegenheiten zuständigen Bundeskanzleramt, eine Regierungsvorlage zu erarbeiten, mit der im BMG eine Kompetenz zur Koordination der IT–Sicherheit klar und ausdrücklich festgelegt wird.

[16] Bundesrechnungsabschluss für das Jahr 2022, Textteil: Band 1, S. 73

[17] BGBl. I 139/2009 i.d.g.F.

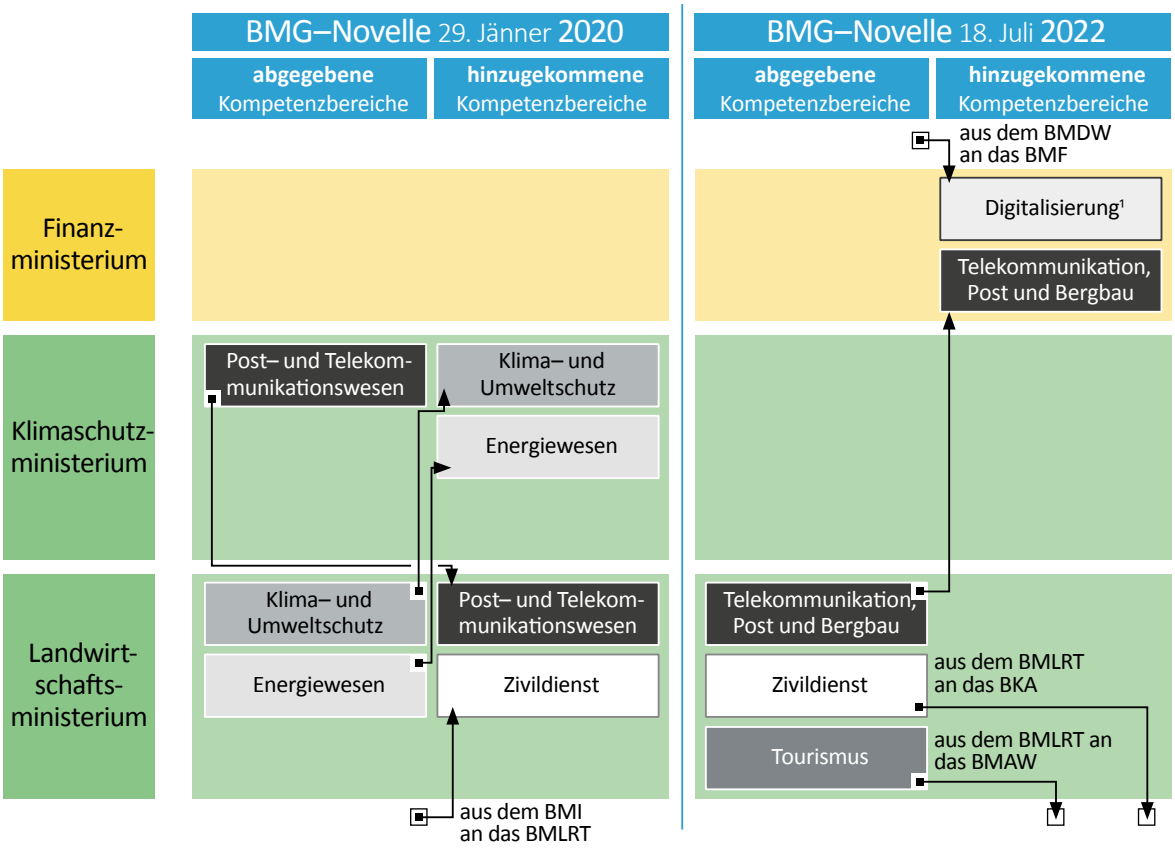
3.3 Laut Stellungnahme des zum Stellungnahmezeitpunkt (Februar 2024) zuständigen Finanzministeriums werde in dem im Rahmen des Programms IT–Konsolidierung durchgeführten Analyse– und Konzeptionsprojekt Security Framework Bund ein Zielbild zu einem „IT Security Framework Bund“ erarbeitet, das sowohl die organisatorischen (Personal, Prozesse, Strukturen) als auch technischen Bestandteile eines solchen Frameworks für die Bundesministerien beschreibe.

3.4 Der RH stellte klar, dass die Empfehlung darauf abzielte, die Kompetenz zur Koordination der IT–Sicherheit im BMG festzulegen. Er betonte erneut die Notwendigkeit einer gesetzlichen Grundlage zur kontinuierlichen Sicherstellung der IT–Sicherheit.

Übernahme von IT–Agenden

4.1 (1) Die von dieser Gebarungsüberprüfung umfassten Bundesministerien waren im überprüften Zeitraum von folgenden Kompetenzänderungen betroffen:

Abbildung 1: Kompetenzverschiebungen aufgrund von Novellen des Bundesministeriengesetzes 1986 (BMG) im Zeitraum 2018 bis 2022



[1] Mit 1. Mai 2024 wechselten die Agenden der Digitalisierung vom Finanzministerium in das Bundeskanzleramt.

BKA = Bundeskanzleramt
BMAW = Bundesministerium für Arbeit und Wirtschaft
BMDW = Bundesministerium für Digitalisierung und Wirtschaftsstandort (jetzt BMAW)
BMF = Bundesministerium für Finanzen
BMI = Bundesministerium für Inneres
BMLRT = Bundesministerium für Landwirtschaft, Regionen und Tourismus (jetzt Landwirtschaftsministerium)

Quelle: Bundesministeriengesetz 1986; Darstellung: RH

- Im Jänner 2020 wechselten die Agenden
  - Klima und Umweltschutz sowie Energiewesen vom BMNT (jetzt Landwirtschaftsministerium) ins BMVIT (jetzt Klimaschutzministerium),
  - Zivildienst vom BMI ins BMLRT (jetzt Landwirtschaftsministerium),
  - Post– und Telekommunikationswesen vom BMVIT (jetzt Klimaschutzministerium) ins BMLRT (jetzt Landwirtschaftsministerium).

- Im Juli 2022 wechselten die Agenden
  - Digitalisierung vom BMDW (jetzt BMAW) ins Finanzministerium[18],
  - Post– und Telekommunikationswesen inklusive Bergbau vom BMLRT (jetzt Landwirtschaftsministerium) ins Finanzministerium,
  - Tourismus und Zivildienst vom BMLRT (jetzt Landwirtschaftsministerium) in ein jeweils anderes Bundesministerium.

Dadurch ergaben sich auch ressortübergreifende Verschiebungen der entsprechenden Abteilungen oder Sektionen.

(2) Die Eingliederung der im Juli 2022 übertragenen zwei Sektionen Digitalisierung und E–Government sowie Telekommunikation, Post und Bergbau setzte das Finanzministerium gemeinsam mit der BRZ GmbH in einem Projekt von Juli bis Dezember 2022 um. Die Übernahme der zwei neuen Sektionen erfolgte sukzessive und umfasste die IT–Infrastruktur, die IT–Betreuung und laufende IT–Projekte. Zudem mussten diverse Verträge[19] übernommen bzw. geändert und Arbeitsprozesse angepasst werden.

Das Finanzministerium erstellte für die IT–Sicherheit der neuen Sektionen eine Onboarding Roadmap zur Informationssicherheit sowie zu den Datenschutzregelungen und –prozessen, stimmte diese mit den neuen Sektionen ab und organisierte dazu Informationsveranstaltungen. Für die IT–Verfahren der zwei neuen Sektionen führte das Finanzministerium bis Juni 2023 39 Risikoanalysen betreffend Informationssicherheit bzw. Datenschutz durch.

Das Finanzministerium teilte mit, dass es durch die umfangreichen Maßnahmen zur Integration der IT der zwei neuen Sektionen zu einer massiven Mehrbelastung der IT–Abteilung sowie des Informationssicherheitsmanagement–Teams gekommen sei.

(3) Aufgrund der Kompetenzänderungen im Jänner 2020 hatte das Klimaschutzministerium drei Sektionen und sechs Abteilungen aus den Bereichen Klimaschutz, Umweltschutz sowie Energiewesen einzugliedern. Die Abteilungen des Post– und Telekommunikationswesens wurden hingegen an das damalige BMLRT (jetzt Landwirtschaftsministerium) abgegeben.

Für die Integration der neuen Organisationseinheiten führte das Klimaschutzministerium von Jänner bis Dezember 2020 ein Migrationsprojekt durch. In diesem Zeitraum, also bis Dezember 2020, verblieben die vom Klimaschutzministerium aufgenommenen Organisationseinheiten (z.B. Klima– und Umweltschutz, Energiewesen) mit den dazugehörigen Services weiterhin in der IT–Betreuung des Land-

[18] ab Mai 2024 ins Bundeskanzleramt

[19] z.B. für Datenleitungen, Druckerverträge; Verwaltungsübereinkommen mit dem Landwirtschaftsministerium für Weiterbetreuung einer Abteilung

wirtschaftsministeriums. Die IT–Betreuung der vom Klimaschutzministerium im Jänner 2020 abgegebenen Organisationseinheiten des Post– und Telekommunikationswesens wurden bis Mai 2021 sukzessive vom aufnehmenden Ministerium (BMLRT, jetzt Landwirtschaftsministerium) übernommen. Die Übergabe einzelner Fachanwendungen[20] war erst im Oktober 2021 endgültig abgeschlossen.

Laut Klimaschutzministerium seien sowohl die Integration der neuen als auch die Übertragung der abgegebenen Organisationseinheiten mit hohem internem Zeitaufwand verbunden gewesen.

(4) Das Landwirtschaftsministerium konnte die Betreuung des laut BMG im Jänner 2020 übertragenen neuen Bereichs Post– und Telekommunikationswesen erst sukzessive bis Mai 2021 übernehmen; gleichzeitig betreute es die an das Klimaschutzministerium abgegebenen Sektionen Klima– und Umweltschutz sowie Energiewesen noch bis Dezember 2020. Laut Landwirtschaftsministerium seien sowohl die Integration der neuen als auch die Übertragung der abgegebenen Organisationseinheiten mit hohem internem Zeitaufwand verbunden gewesen.

Mit der BMG–Novelle 2022 wurden die Sektion Telekommunikation, Post und Bergbau vom damaligen BMLRT (jetzt Landwirtschaftsministerium) an das Finanzministerium sowie der Bereich Tourismus an das BMAW und die Zivildienstagentur an das Bundeskanzleramt abgegeben. Da jedoch der Ausbau der entsprechenden technischen Infrastruktur samt Migration einer Fachanwendung für die Abteilung Telekompolitik und IKT[21]–Infrastruktur im Finanzministerium kurzfristig nicht realisierbar war, wurde diese Fachanwendung[22] bis Ende Juli 2023 nach wie vor vom Landwirtschaftsministerium betreut. Das Finanzministerium plante, mit diesen Leistungen ab August 2023 die BRZ GmbH zu beauftragen; zwischenzeitlich schlossen das Finanz– und das Landwirtschaftsministerium im März 2023 ein Verwaltungsübereinkommen für eine befristete Weiterbetreuung ab.

(5) Die drei überprüften Bundesministerien teilten zu den Verschiebungen aufgrund der Kompetenzänderungen mit, dass neben den umfangreichen Arbeiten zur Integration der neuen bzw. Segregation der abgegebenen IT–Arbeitsplätze noch spezielle Maßnahmen für hinzugekommene Fachanwendungen bzw. deren Betreuung erforderlich waren: Um deren sicheren Betrieb zu gewährleisten, mussten in intensiven Abstimmungs–, Dokumentations– und Lernphasen umfangreiche Detailkenntnisse erlangt werden. Diese komplexen Maßnahmen waren umfangreich und zeitaufwändig.

[20] November 2020: GIS–Server für Breitbandoffensive; Jänner 2021: Applikationen der Fernmeldebehörde; Oktober 2021: Funk3

[21] Informations– und Kommunikationstechnologie (**IKT**)

[22] Clientbetrieb für zehn mobile IT–Arbeitsplätze; Serverbetrieb für GIS; Netzwerkbetrieb

4.2 Der RH wies kritisch darauf hin, dass die Integration der neu einzugliedernden und das Herauslösen der abzugebenden Organisationseinheiten mit hohem Arbeits– und Zeitaufwand verbunden waren. Er stellte fest, dass die IT–mäßige Integration der eingegliederten Organisationseinheiten einen Zeitraum von bis zu rund einem Jahr beanspruchte bzw. bei einigen Fachapplikationen noch länger dauerte. Der RH verwies auf die Sicherheitsrisiken, die in dieser Phase der Überleitung der IT–Betreuung und der Überleitung auf die neuen Sicherheitsstandards gegeben waren. Er verwies dazu auf seine Empfehlungen zur IT–Konsolidierung in TZ 3 und TZ 6.

IKT–Konsolidierungsgesetz

5.1 (1) Das IKT–Konsolidierungsgesetz[23] diente seit 2012 als Grundlage für die Vereinheitlichung bestehender und neuer IKT–Lösungen des Bundes. Die einheitlichen Systeme sollten auf Basis vorgegebener IKT–Standards verwendet werden, um einen effizienten Betrieb und ein hohes Maß an Datensicherheit zu erzielen. Die nähere Festlegung der IKT–Standards sollte durch Verordnung erfolgen. Zuständig hierfür war im überprüften Zeitraum bis 17. Juli 2022 das Digitalisierungsministerium, infolge der BMG–Novelle 2022 ab 18. Juli 2022 das Finanzministerium. Zusätzlich war das Einvernehmen mit dem Bundeskanzleramt herzustellen. Infolge der BMG–Novelle 2024 war ab dem 1. Mai 2024 das Bundeskanzleramt zuständig.

(2) § 2 Abs. 1 IKT–Konsolidierungsgesetz führte jene IKT–Lösungen und IT–Verfahren an, die 2012 für eine Vereinheitlichung und für die Festlegung von IKT–Standards in Aussicht genommen worden waren. Dies waren insbesondere der standardisierte IT–Büroarbeitsplatz in der Bundesverwaltung („Bundesclient–Architektur“), eine gemeinsame Lösung zur Entwicklung und Wartung der Internetauftritte der Bundesdienststellen (Content–Management–System), das IT–Lizenzmanagement des Bundes und die duale Zustellung.[24]

Bis zum Juni 2023 fehlten spezielle Verordnungen mit IKT–Standards. Das Digitalisierungsministerium bzw. in der Folge das Finanzministerium hatte einen Entwurf für eine Verordnung zum Content–Management–System erarbeitet; dieser wurde aber nicht weiterverfolgt, nachdem die Bundesministerien (mit Ausnahme des Innenministeriums, des Verteidigungsministeriums und des Außenministeriums) das Content–Management–System faktisch umgesetzt hatten. Lediglich für die duale (elektronische) Zustellung gab es eigene gesetzliche Regelungen[25]. Zudem startete

[23] BGBl. I 35/2012 i.d.g.F.

[24] Weiters waren dies auch elektronische Signaturen, das Identity– und Accessmanagement (Rechte– und Rollenverwaltung), der Elektronische Akt (**ELAK**), Softwarebausteine bzw. Softwarebibliotheken sowie Basiskomponenten (z.B. Scanning).

[25] Zustellgesetz, BGBl. 200/1982 i.d.g.F.; Bundesabgabenordnung, BGBl. 194/1961 i.d.g.F.; FinanzOnline–Verordnung 2006, BGBl. II 97/2006 i.d.g.F.

das Finanzministerium weitere Projekte zur Vereinheitlichung von wesentlichen IKT–Lösungen und IT–Verfahren, die im IKT–Konsolidierungsgesetz von 2012 nicht enthalten waren (z.B. für IT–Sicherheit, standardisierte Rechenzentrumservices, TZ 6).

5.2 Der RH kritisierte – wie schon in seinem Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 3) –, dass nunmehr elf Jahre nach Inkrafttreten des IKT–Konsolidierungsgesetzes die IKT–Standards für einheitliche Systeme noch nicht in der dafür vorgesehenen Form festgelegt waren. Eine entsprechende Verordnung war auch im Juni 2023 noch nicht erlassen.

Der RH wiederholte daher seine Empfehlung an das seit Mai 2024 auch für Digitalisierungsagenden zuständige Bundeskanzleramt, die im IKT–Konsolidierungsgesetz vorgesehene Verordnung zu erlassen.

Weiters wies der RH darauf hin, dass die Vereinheitlichung der 2012 im IKT–Konsolidierungsgesetz genannten IKT–Lösungen und IT–Verfahren für einzelne Verfahren (Content–Management–System, duale Zustellung) abgeschlossen war und das Finanzministerium an anderen, nicht im Gesetz aufgezählten Projekten arbeitete, z.B. in den Bereichen IT–Sicherheit und standardisierte Rechenzentrumservices. Die Aufzählung von betroffenen IKT–Lösungen und IT–Verfahren im IKT–Konsolidierungsgesetz von 2012 war daher nicht mehr aktuell.

Der RH empfahl dem seit Mai 2024 für Digitalisierungsagenden zuständigen Bundeskanzleramt, im Hinblick auf die zu erlassende(n) Verordnung(en) mit IKT–Standards auch eine Regierungsvorlage zur Aktualisierung der Aufzählung von betroffenen IKT–Lösungen und IT–Verfahren in § 2 Abs. 1 IKT–Konsolidierungsgesetz vorzubereiten.

5.3 Das zum Stellungnahmezeitpunkt zuständige Finanzministerium teilte in seiner Stellungnahme mit, dass im Rahmen der IT–Konsolidierung ein Entwurf zur „Bundes Content Management System (B–CMS) Verordnung“ in den Abstimmungsprozess eingebracht worden sei. Dieser Entwurf sei bisher nicht angenommen worden. Ein Entwurf zur einheitlichen „Lizenzmanagement (LIMBO) Verordnung“ sei erstellt worden.

Die Aufzählung von betroffenen IKT–Lösungen und IT–Verfahren des Bundes im IKT–Konsolidierungsgesetz (§ 2 Abs. 1) sei nur beispielhaft und nicht als abschließend zu verstehen. Für zwei der im IKT–Konsolidierungsgesetz genannten IKT–Lösungen und IT–Verfahren (Content–Management–System und IT–Lizenzmanagement) seien – wie ausgeführt – bereits Verordnungsentwürfe erstellt worden.

5.4 Der RH verwies hinsichtlich der Verordnung zum Content–Management–System auf seine Feststellungen, wonach der Verordnungsentwurf nicht weiterverfolgt wurde, da die Bundesministerien das Content–Management–System faktisch umgesetzt hatten. Der RH anerkannte zwar die Erstellung eines weiteren Verordnungsentwurfs, hielt jedoch erneut fest, dass elf Jahre nach Inkrafttreten des IKT–Konsolidierungsgesetzes noch keine Verordnung zur Festlegung von IKT–Standards erlassen wurde. Die Aktualisierung der Aufzählung von betroffenen IKT–Lösungen und IT–Verfahren des Bundes im IKT–Konsolidierungsgesetz (§ 2 Abs. 1) erachtete der RH trotz ihres beispielhaften Charakters aus Gründen der Transparenz und Rechtssicherheit als zweckmäßig. Er hielt seine Empfehlungen daher aufrecht.

Programm IT–Konsolidierung

6.1 (1) Die Konferenz der Generalsekretäre[26] vereinbarte 2018 die Umsetzung von IT–Konsolidierungsmaßnahmen. Die im November 2019 im Ministerrat präsentierte „Machbarkeitsstudie“ stellte die Notwendigkeit einer IT–Konsolidierung hinsichtlich der IT–Arbeitsplätze, Standard– und Fachanwendungen sowie der zentralen IT–Infrastruktur fest. Im November 2019 beschloss die Bundesregierung die Umsetzung der vorgeschlagenen Konsolidierungsmaßnahmen. Auch die nachfolgende Bundesregierung setzte sich in ihrem Regierungsprogramm 2020–2024 das Ziel der IT–Konsolidierung bestehender Bundessysteme.

(2) Im August 2020 erteilten die Generalsekretäre[27] einen konkreten Auftrag für eine IT–Konsolidierung. Der Programmauftrag richtete sich an das damalige Digitalisierungsministerium und das Bundeskanzleramt unter Mitwirkung aller Ressorts. Zu den im Programmauftrag angeführten Zielen zählten Kosteneinsparungen, eine zuverlässige Sicherheitsarchitektur, eine verbesserte einheitliche Servicequalität einschließlich schnellerer Erbringung sowie gesteigerte Transparenz und zentrale Steuerung. Die Zuständigkeit für Digitalisierungsangelegenheiten verschob sich mit der BMG–Novelle 2022 in das Finanzministerium.

(3) Nach dem Programmauftrag sollte zunächst das Digitalisierungsministerium und von Juli 2022 bis April 2024 das die Digitalisierungsagenden übernehmende Finanzministerium gemeinsam mit dem Bundeskanzleramt das Programm–Management stellen. Dieses war Auftraggeber der einzelnen Projekte im Programm und trug die Verantwortung für die Erreichung der Programmziele. Die Position des Finanzministeriums im Programm–Management war von Jänner 2023 bis Juni 2023 vakant,

[26] zu diesem Gremium siehe RH–Bericht „Generalsekretariate in den Bundesministerien“ (Reihe Bund 2021/12, TZ 35)

[27] Unterzeichnung des Auftrags durch alle zwölf betrauten Generalsekretäre sowie durch den Kabinettschef des Justizministeriums, das keinen Generalsekretär eingesetzt hatte

Mitte Juni 2023 wurde sie neu besetzt. Das Bundeskanzleramt begleitete die Projekte auch in diesem Zeitraum.

Das Programm–Management leitete auch das Konsolidierungsboard, in dem sich die Ressorts über die in Projekten entwickelten Konzepte austauschten. Die überprüften Bundesministerien nahmen regelmäßig am Konsolidierungsboard teil, das von Juni 2021 bis Juni 2023 sechsmal tagte.

Der Lenkungsausschuss stellte die oberste Steuerungs– und Kontrollinstanz des Programms IT–Konsolidierung dar; er traf u.a. Entscheidungen über die Umsetzung von Projekten. Zur Zeit der Gebarungsüberprüfung war der Lenkungsausschuss mit Bediensteten des Bundeskanzleramts, des Finanzministeriums und des Bundesministeriums für Kunst, Kultur, öffentlichen Dienst und Sport besetzt.

(4) Das Programm umfasste im Mai 2023 insgesamt acht Projekte zu verschiedenen Aspekten der IT–Konsolidierung; zwei weitere Projekte waren in Vorbereitung:

Tabelle 3: Status der Projekte des Programms IT–Konsolidierung im Mai 2023

Projekt	Analyse und Konzeption	Umsetzung	Mitwirkung der überprüften Bundesministerien
Videokonferenzsystem des Bundes	abgeschlossen	in der Phase der Fertigstellung	Finanzministerium Klimaschutzministerium Landwirtschaftsministerium
Standardarbeitsplatz und sichere Basisdienste	abgeschlossen	Umsetzung durch den Lenkungsausschuss abgelehnt; bisherige Ergebnisse fließen in weiterführende Projekte ein	Finanzministerium Landwirtschaftsministerium
Hotline/Service Desk[1]	abgeschlossen	Umsetzung durch den Lenkungsausschuss abgelehnt; bisherige Ergebnisse fließen in weiterführende Projekte ein	–
Software Asset Management für Bundesauftraggeber	Analyse abgeschlossen; Detailkonzeption in Ausarbeitung	Entscheidung des Lenkungsausschusses über Umsetzung noch nicht erfolgt	Finanzministerium Klimaschutzministerium Landwirtschaftsministerium
Standardisierte Rechenzentrumservices	begonnen	nicht Bestandteil des Projekts	Finanzministerium
Standard Services	begonnen	Entscheidung des Lenkungsausschusses über Umsetzung noch nicht erfolgt	Finanzministerium
Security Framework Bund	begonnen	Entscheidung des Lenkungsausschusses über Umsetzung noch nicht erfolgt	Finanzministerium
IT Service Management–Prozesse	begonnen	nicht Bestandteil des Projekts	Finanzministerium Klimaschutzministerium

[1] gemeinsame Abwicklung mit dem Projekt „Standardarbeitsplatz und sichere Basisdienste“

Quelle: BMF

Darüber hinaus koordinierte das Programm–Management sechs Arbeitspakete, in denen u.a. ein Zielbild zur IT–Konsolidierung, ein Katalog bereits bestehender IT–Services und ein Konzept zur IT–Governance erarbeitet wurden. Nicht Bestandteil des Programms war es, Maßnahmen zur IT–Konsolidierung in den einzelnen Bundesministerien zu setzen.

In drei Projekten des Programms IT–Konsolidierung war die Analyse– und Konzeptionsphase abgeschlossen: Im Projekt Videokonferenzsystem des Bundes befand sich die Umsetzung – die Schaffung einer einheitlichen Standardlösung – in der Phase der Fertigstellung (TZ 19). Bei zwei Projekten („Standardarbeitsplatz und sichere Basisdienste“ sowie „Hotline/Service Desk“) hatte der Lenkungsausschuss allerdings die Umsetzung des Projekts als nicht erfolgversprechend eingeschätzt und entschieden, sie nicht unmittelbar umzusetzen; die bisherigen Ergebnisse der Analyse und Konzeption sollten in nachfolgenden Projekten Berücksichtigung finden.

Fünf Projekte des Programms IT–Konsolidierung befanden sich zur Zeit der Gebarungsüberprüfung noch in der Analyse– und Konzeptionsphase: Bei zwei Projekten war eine nachfolgende Umsetzung im Rahmen des Projekts nicht vorgesehen, bei drei Projekten war die Entscheidung des Lenkungsausschusses über die künftige Umsetzung noch offen.

6.2 Der RH kritisierte, dass das Finanzministerium, das mit der BMG–Novelle 2022 Digitalisierungsangelegenheiten übernahm, von Jänner 2023 bis Mitte Juni 2023 die Position des Programm–Managements nicht besetzte. Er anerkannte, dass das Bundeskanzleramt die Projekte auch in diesem Zeitraum begleitete.

Der RH kritisierte, dass drei Jahre nach dem Auftrag vom August 2020 keines der Projekte zur IT–Konsolidierung umgesetzt war:

- Bei den Projekten „Standardarbeitsplatz und sichere Basisdienste“ sowie „Hotline/Service Desk“ waren die Analyse und Konzeption abgeschlossen. Der Lenkungsausschuss hatte aber die bundesweite Umsetzung eines derartig umfassenden Projekts als nicht erfolgversprechend eingeschätzt; die Erkenntnisse der Analyse und Konzeption sollen in nachfolgenden Projekten berücksichtigt werden.
- Fünf Projekte des Programms IT–Konsolidierung befanden sich im Juni 2023 in der Analyse– und Konzeptionsphase: Für zwei dieser Projekte war keine Umsetzung vorgesehen, bei drei Projekten hatte der Lenkungsausschuss noch keine Entscheidung über eine nachfolgende Umsetzung getroffen.

Der RH empfahl dem Bundeskanzleramt, das seit Mai 2024 die Digitalisierungsagenden – und damit auch die Verantwortung für die IT–Konsolidierung – übernommen hatte, die im Programm IT–Konsolidierung erstellten Konzepte von den einzelnen Ressorts auf ihre Umsetzbarkeit prüfen und analysieren zu lassen, ob die Umsetzung schrittweise in Teilprojekten erfolgen sollte.

Der RH erachtete die aktive Teilnahme möglichst vieler Bundesministerien an den einzelnen Projekten zur IT–Konsolidierung als wesentlich, um eine Umsetzung zu fördern.

Er empfahl daher dem Bundeskanzleramt, das seit Mai 2024 die Digitalisierungsagenden – und damit auch die Verantwortung für die IT–Konsolidierung – übernommen hatte, die Bundesministerien zur Teilnahme und aktiven Mitwirkung an den Projekten der IT–Konsolidierung zu motivieren.

6.3 Laut Stellungnahme des zum Stellungnahmezeitpunkt (Februar 2024) für Digitalisierungsagenden zuständigen Finanzministeriums erarbeite es im Rahmen der Analyse– und Konzeptionsprojekte des Programms IT–Konsolidierung Grundlagen für die Umsetzung dieser Vorhaben. Die Ergebnisse würden in einer Entscheidungsgrundlage aufbereitet und dem Lenkungsausschuss zur IT–Konsolidierung zur Beschlussfassung vorgelegt. Die einzelnen Ressorts bekämen die erstellten Konzepte im Rahmen des IT–Konsolidierungsboards zur Verfügung gestellt, damit sie diese auf Umsetzbarkeit in ihrem eigenen Ressort prüfen und gegebenenfalls umsetzen können. Die konkrete Umsetzung von Maßnahmen liege in der Zuständigkeit der jeweiligen Ressorts.

Im Zuge des aktiv betriebenen Stakeholder–Managements im Programm IT–Konsolidierung seien mehrfach Gespräche mit den einzelnen Ressorts geführt worden, um diese zur Mitwirkung am Programm sowie zur Umsetzung von IKT–Services zu motivieren. Zudem würden die Beteiligung und aktive Mitwirkung an den Projekten des Programms durch das IT–Konsolidierungsboard gefördert, das sich aus Vertreterinnen und Vertretern aller Bundesministerien zusammensetze und Sitzungen in regelmäßigen Abständen abhalte.

6.4 Der RH wiederholte, dass drei Jahre nach dem Auftrag vom August 2020 noch keines der Projekte des Programms IT–Konsolidierung umgesetzt war. Aus Sicht des RH kam dem Bundeskanzleramt, das mit der BMG–Novelle 2024 die Digitalisierungsagenden – und damit auch die Verantwortung für die IT–Konsolidierung – übernommen hatte, eine wichtige Rolle bei der Erreichung der Ziele des Programms zu. Er verwies daher nochmals auf seine Empfehlungen und auf die Verantwortung, die auch die anderen Ressorts für die erfolgreiche Umsetzung der Projekte und somit der Ziele des Programms IT–Konsolidierung trugen.

Grundlagen der IT–Sicherheit

Technische Vorgaben

7.1 (1) Im Dezember 2021 beschloss die Bundesregierung die aktualisierte „Österreichische Strategie für Cybersicherheit 2021“ (in der Folge: **Cybersicherheitsstrategie**) unter Federführung des Bundeskanzleramts. Eine sichere IT im öffentlichen Sektor sollte das Vertrauen in die staatlichen Institutionen stärken und die Handlungsfähigkeit des Staates schützen. Die organisatorischen Grundstrukturen und –prozesse der staatlichen Cyber–Sicherheitsvorsorge waren im NISG (TZ 8) festgelegt.[28]

(2) Das Österreichische Informationssicherheitshandbuch (in der Folge: **Informationssicherheitshandbuch**[29]) enthielt Leitlinien und Empfehlungen zur sicheren Gestaltung der IT und zur Etablierung eines Informationsmanagementsystems in Unternehmen und in der öffentlichen Verwaltung. Es wurde im Februar 2023 aktualisiert.

(3) Das Regierungsprogramm 2020–2024 setzte im Kapitel Cyber–Sicherheit – im Rahmen der strategischen Koordinierungsfunktion des Bundeskanzleramts – das Ziel einheitlicher Sicherheitsstandards für die IKT der öffentlichen Verwaltung. Auch ein Beschluss des Nationalen Sicherheitsrates von Februar 2020 empfahl der Bundesregierung, verbindliche Sicherheitsstandards für präventive Vorkehrungen in staatlichen IT–Systemen auszuarbeiten.

Im Rahmen des Programms IT–Konsolidierung (TZ 6) wurde im Oktober 2022 das Projekt Security Framework Bund beauftragt; Teilnehmer waren vorerst sechs Bundesministerien unter Leitung des Bundeskanzleramts. Ziel des Projekts war, bis Ende 2023 den Ist–Zustand in den beteiligten sechs Bundesministerien und den Soll–Zustand der IT–Sicherheit des Bundes (Zielbild, siehe TZ 6) zu analysieren und zu vergleichen sowie Entscheidungsgrundlagen für die Umsetzung von Maßnahmen der IT–Sicherheit zu erarbeiten.

7.2 (1) Der RH bewertete die Aktualisierung der Cybersicherheitsstrategie sowie des Informationssicherheitshandbuchs positiv.

Er hielt kritisch fest, dass im Juli 2023 noch keine einheitlichen Sicherheitsstandards für die IT der Bundesverwaltung vorlagen, obwohl das Regierungsprogramm 2020–2024 und die Empfehlung des Nationalen Sicherheitsrates bereits 2020 die Notwen-

[28] siehe auch den RH–Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13)

[29] Ein Projekt des Bundeskanzleramts in Zusammenarbeit mit dem Zentrum für sichere Informationstechnologie – Austria (A–SIT); das Informationssicherheitshandbuch enthielt Beschreibungen der detaillierten Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems, https://www.sicherheitshandbuch.gv.at (abgerufen am 24. August 2023).

digkeit solcher Standards dokumentiert hatten. Das im Rahmen des Programms IT–Konsolidierung der Bundesregierung zur IT–Sicherheit beauftragte Projekt Security Framework war mit Mai 2023 beendet.

Der RH empfahl dem seit Mai 2024 in Nachfolge des Finanzministeriums für die Koordination der IT zuständigen Bundeskanzleramt, die nötige Teilnahme der Bundesministerien an der Umsetzung der im Projekt Security Framework Bund zu erarbeitenden Sicherheitsstandards zu fördern. Dies wäre über eine Einbeziehung in die Themen der Konferenz der Generalsekretäre[30] bzw. eines gleichwertiges Gremiums (aus den internen administrativen Spitzen der Bundesministerien) zu begleiten.

(2) Da noch keine einheitlichen Sicherheitsstandards für die IT der Bundesverwaltung vorlagen, zog der RH ausgewählte Aspekte des Informationssicherheitshandbuchs (für Unternehmen und die öffentliche Verwaltung, Stand Februar 2023) als Maßstab für den nachfolgenden Vergleich der in den Bundesministerien eingesetzten Maßnahmen des Managements der IT–Sicherheit heran.

7.3 Laut Stellungnahme des zum Stellungnahmezeitpunkt (Februar 2024) noch für Digitalisierungsagenden zuständigen Finanzministeriums sei eine weitere Unterstützung des Projekts Security Framework Bund, das im Rahmen des Programms IT–Konsolidierung durchgeführt werde, vorgesehen. Der IKT–Lenkungsausschuss werde über die Ergebnisse des Analyse– und Konzeptionsprojekts informiert. Ziel dieses Vorhabens sei die Schaffung eines Zielbilds zu einem „IT Security Framework Bund“, das sowohl die organisatorischen (Personal, Prozesse, Strukturen) als auch technischen Bestandteile eines solchen Frameworks für die Bundesministerien auf Basis bereits vorliegender Überlegungen (insbesondere Cybersicherheitsstrategie, Erkenntnisse aus zurückliegenden Sicherheitsvorfällen etc.), aktueller Standards und Good bzw. Best Practices beschreibe.

7.4 Der RH begrüßte die vom Finanzministerium geplante Unterstützung des Projekts. Ergänzend wiederholte er, dass über den IKT–Lenkungsausschuss hinaus auch weitere bundesweite Gremien, wie die Konferenz der Generalsekretäre, einbezogen werden sollten, um die Umsetzung des Projekts voranzutreiben.

[30] zu diesem Gremium siehe RH–Bericht „Generalsekretariate in den Bundesministerien“ (Reihe Bund 2021/12, TZ 35)

Rechtliche Vorgaben

8.1 (1) Nach dem NISG hatten die Einrichtungen des Bundes für die von ihnen auf IKT–Basis betriebenen wichtigen Dienste geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese hatten den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.[31] Ziel war ein hohes Sicherheitsniveau von Netz– und Informationssystemen. Die wichtigen Dienste wurden im Gesetz nicht näher bestimmt. Sie waren daher von jeder Einrichtung des Bundes selbst zu identifizieren (siehe TZ 11). Der RH hatte die Verpflichtungen nach dem NISG bereits in seinem Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13, TZ 4) beschrieben. Die neue NIS–2–Richtlinie[32] der EU verpflichtete die Mitgliedstaaten, sie bis Oktober 2024 in nationales Recht umzusetzen (TZ 9).

(2) Nach der unmittelbar anwendbaren Datenschutz–Grundverordnung der EU (DSGVO[33]) hatten die für eine Datenverarbeitung Verantwortlichen und ihre Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen,[34] um ein angemessenes Sicherheitsniveau zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

(3) Das Informationssicherheitsgesetz (**InfoSiG**[35]) und die ausführende Informationssicherheitsverordnung (InfoSiV[36]) regelten in Umsetzung völkerrechtlicher Verpflichtungen Sicherheitsmaßnahmen für Informationen, die einer besonderen Geheimhaltung unterliegen (klassifizierte Informationen, internationaler Geheimschutz). Die Geheimschutzordnung des Bundes (Beschluss des Ministerrates vom Jänner 2008) betraf den nationalen Geheimschutz klassifizierter Informationen abseits völkerrechtlicher Verpflichtungen. Beide Regelungskomplexe enthielten – im Detail unterschiedliche – Vorgaben für besondere Sicherungsmaßnahmen bei elektronischer Verarbeitung.

Die im Bundeskanzleramt eingerichtete Informationssicherheitskommission hatte in ihrem Bericht 2020 auf die Risiken der genannten unterschiedlichen Regelungen hingewiesen. Daher hatte der RH in seinem Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 6) unter Hinweis auf diese Unterschiede empfohlen, eine Regierungsvorlage zu erar-

31 § 22 NISG

32 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

33 Datenschutz–Grundverordnung (EU) 2016/679, ABl. L 2016/119, 1

34 Art. 5 Abs. 1 lit. f und Art. 32 Datenschutz–Grundverordnung

35 BGBl. I 23/2002 i.d.g.F.

36 BGBl. II 548/2003 i.d.g.F.

beiten, die ein einheitliches Regelungssystem zur elektronischen Verarbeitung klassifizierter Informationen für den internationalen und nationalen Geheimschutz schafft. Das Bundeskanzleramt hatte hierzu in seiner Stellungnahme mitgeteilt, dass eine neue Rechtsgrundlage („InfoSiG neu") im Rahmen der im Bundeskanzleramt eingerichteten Informationssicherheitskommission in Ausarbeitung sei. Dieser Kommission gehörten die Informationssicherheitsbeauftragten aller Bundesministerien an.

Eine entsprechende Regierungsvorlage bzw. ein Gesetzesbeschluss lagen im Juni 2023 nicht vor. Nach Auskunft des Bundeskanzleramts[37] war ein Fachentwurf bereits erarbeitet und befand sich im politischen Abstimmungsprozess.

8.2 Der RH hielt kritisch fest, dass die noch nicht abgeschlossene Harmonisierung der unterschiedlichen rechtlichen Grundlagen für klassifizierte Informationen (Informationssicherheitsgesetz und Geheimschutzordnung des Bundes) nach wie vor das von der Informationssicherheitskommission identifizierte Sicherheitsrisiko in sich barg.

Der RH verwies daher auf seine Empfehlung an das Bundeskanzleramt, eine Regierungsvorlage zu erarbeiten, die ein einheitliches Regelungssystem zur elektronischen Verarbeitung klassifizierter Informationen für den internationalen und nationalen Geheimschutz schafft (RH–Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien" (Reihe Bund 2021/31, TZ 6)).

Hierzu empfahl er dem Finanz–, dem Klimaschutz– und dem Landwirtschaftsministerium, die Vorbereitung der Regierungsvorlage für das „InfoSiG neu" in der Informationssicherheitskommission sowie im Abstimmungsprozess mit den Bundesministerien zu unterstützen, um die Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen abzuschließen.

Der RH verwies zur Identifikation wichtiger Dienste in den Bundesministerien sowie zu den Herausforderungen der Umsetzung der NIS–2–Richtlinie auf die TZ 9 und TZ 11.

8.3 (1) Das Finanzministerium sagte in seiner Stellungnahme zu, die Empfehlung aufzugreifen und die Vorbereitung einer Regierungsvorlage für das „InfoSiG neu" unter Berücksichtigung der verfügbaren Ressourcen zu unterstützen.

(2) Das Landwirtschaftsministerium begrüßte eine Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen.

[37] Die Informationssicherheitskommission war im Bundeskanzleramt eingerichtet, das Bundeskanzleramt war für die Angelegenheiten des Informationssicherheitsgesetzes zuständig (Anlage 1 Teil 2A Z 11 BMG).

Rechtliche Entwicklung: NIS–2–Richtlinie

9.1 Im Dezember 2022 erließen das Europäische Parlament und der Rat die NIS–2–Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU. Sie sollte die bisherige NIS–Richtlinie aus 2016 – zu dieser siehe den RH–Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13, TZ 2, TZ 4) – ersetzen und festgestellte Unterschiede in der Umsetzung durch die Mitgliedstaaten beseitigen. Die NIS–2–Richtlinie verpflichtete die Mitgliedstaaten, sie bis Oktober 2024 in nationales Recht umzusetzen. Die vorbereitenden Maßnahmen zur legistischen Umsetzung oblagen dem Bundeskanzleramt im Rahmen der strategischen Koordination der Cyber–Sicherheit.

Im Anwendungsbereich der NIS–2–Richtlinie liegen im Gegensatz zur bisherigen NIS–Richtlinie auch Einrichtungen der öffentlichen Verwaltung der Zentralregierungen der Mitgliedstaaten. In Österreich galt das NISG bereits für wichtige Dienste der Einrichtungen des Bundes (also insbesondere der Bundesministerien).[38] Die Pflichten dieser Einrichtungen waren jedoch im Vergleich zu jenen der Betreiber wesentlicher Dienste weniger weitreichend: Insbesondere beurteilte die Einrichtung selbst das Vorliegen eines wichtigen Dienstes, eine Überprüfung der Sicherheitsvorkehrungen war nicht vorgesehen.

Die NIS–2–Richtlinie verpflichtet die Mitgliedstaaten, sicherzustellen, dass die erfassten Einrichtungen Sicherheitsmaßnahmen (Risikomanagementmaßnahmen) ergreifen, um die Sicherheitsrisiken für die von einer Einrichtung genutzten Netz– und Informationssysteme zu beherrschen.[39] Dabei sind in einem gefahrenübergreifenden Ansatz einerseits sämtliche mögliche externe und interne Risiken und andererseits sämtliche Systeme zu berücksichtigen, nicht nur wie bisher die wesentlichen bzw. wichtigen Dienste. Ausdrücklich sollen die Leitungsorgane der Einrichtungen verpflichtet werden, die Risikomanagementmaßnahmen zu billigen und zu überwachen sowie an Schulungen teilzunehmen.[40] Auch für die Einrichtungen der öffentlichen Verwaltung sind grundsätzlich Aufsichtsmaßnahmen vorzusehen.[41]

9.2 Der RH stellte fest, dass die NIS–2–Richtlinie – vorbehaltlich der Umsetzung durch den österreichischen Gesetzgeber – durch den gefahrenübergreifenden Ansatz und den daraus folgenden Wegfall der Fokussierung auf wesentliche oder wichtige Dienste dazu führt, dass sich die Sicherheitsanforderungen an die Einrichtungen der öffentlichen Verwaltung des Bundes erhöhen und mögliche Aufsichtsmaßnahmen

[38] weiters Gerichtshöfe des öffentlichen Rechts, Rechnungshof, Volksanwaltschaft, Präsidentschaftskanzlei, Parlamentsdirektion

[39] Art. 21

[40] Art. 20

[41] Art. 31 ff.

vorzusehen sind. Dies erfordert die Einrichtung eines umfassenden Risiko– und Notfallmanagementsystems in jedem Bundesministerium.

Der RH empfahl dem Finanz–, dem Klimaschutz– und dem Landwirtschaftsministerium, sich auf die Anforderungen durch die Umsetzung der NIS–2–Richtlinie vorzubereiten und den nationalen Umsetzungsprozess zu begleiten, um die wesentlichen Themen – wie Risikomanagement, Notfallvorsorge, Krisenmanagement, Verantwortung der Ressortleitung – ressortintern zeitgerecht zu berücksichtigen.

Darüber hinaus empfahl der RH den drei überprüften Ministerien, das – alle Ministerien aus der NIS–2–Richtlinie treffende – Thema der Umsetzung der erforderlichen Sicherheitsanforderungen sowie die finanziellen Erfordernisse in die Konferenz der Generalsekretäre bzw. ein gleichwertiges Gremium (aus den internen administrativen Spitzen der Bundesministerien) zwecks ressortübergreifender Erörterung einzubringen.

9.3 (1) Das Finanzministerium verwies in seiner Stellungnahme auf das noch nicht abgeschlossene Projekt Security Framework Bund (TZ 7), das ein Zielbild zu organisatorischen und technischen Bestandteilen von Sicherheitsanforderungen schaffen solle. Weiters habe das Finanzministerium bereits Vorbereitungen im Zusammenhang mit den geänderten Anforderungen durch die Umsetzung der NIS–2–Richtlinie eingeleitet. In diesem Zusammenhang seien die wesentlichen Informationssicherheits– und Datenschutzerlässe des Finanzministeriums entsprechend angepasst worden. Die aktualisierten Erlässe würden nach Abschluss der ressortinternen Abstimmungsmaßnahmen voraussichtlich im Jänner 2024 in Kraft gesetzt.

(2) Das Landwirtschaftsministerium wies in seiner Stellungnahme darauf hin, dass die Umsetzung der NIS–2–Richtlinie noch nicht erfolgt sei und das NISG in der Fassung von 2018 vorliege. Die federführende Wahrnehmung des nationalen Umsetzungsprozesses liege nicht in seiner Zuständigkeit. Ein partizipativer Umsetzungsprozess, an dem das Landwirtschaftsministerium teilnehmen könnte, sei der IKT–Abteilung nicht bekannt. Das Landwirtschaftsministerium werde die wesentlichen Themen ressortintern berücksichtigen und Maßnahmen zur Umsetzung vorbereiten.

9.4 Der RH betonte die Notwendigkeit einer zeitgerechten, ressortinternen Vorbereitung auf die Themen der NIS–2–Richtlinie, da die erhöhten Sicherheitsanforderungen bereits ab Oktober 2024 gelten.

Er wies zudem auf den nunmehr vorliegenden Entwurf des Netz– und Informationssystemsicherheitsgesetzes 2024 (NISG 2024) zur Umsetzung der NIS–2–Richtlinie hin, der im April 2024 und somit nach Abschluss der Gebarungsüberprüfung versendet wurde.

IT–Sicherheitsstrategien der überprüften Bundesministerien

10.1 (1) Das Informationssicherheitshandbuch empfahl, eine schriftliche IT–Sicherheitsstrategie auf Ressortebene als Grundlage des IT–Sicherheitsmanagements zu erstellen und für alle Bediensteten transparent in Kraft zu setzen. Dieses strategische Dokument sollte klare Ziele, Verantwortlichkeiten einschließlich der Unterstützung durch die Ressortleitung („Management Commitment“) und nachvollziehbare Methoden des IT–Sicherheitsmanagements festlegen:

Tabelle 4: IT–Sicherheitsstrategien

Thema	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
IT–Sicherheitsstrategie vorhanden	ja, aktualisiert 2021	ja, aus 2002 (Grundsatzdokument, ausführende Dokumente aus 2020/21)	ja, aktualisiert 2022 (Grundsatzdokument, ausführende Dokumente aus 2019/20)
Erfassung des nachgeordneten Bereichs	ja	teilweise	teilweise
unterzeichnet von	Generalsekretär	Generalsekretär bzw. Abteilungsleitung	Sektions– bzw. Ressortleitung
Kundmachung mit Rundschreiben	ja	ja	nur die IT–Strategie
wesentliche Ziele der IT–Sicherheitsstrategie	Schutz von Vertraulichkeit, Integrität und Verfügbarkeit, Vermeidung von Sicherheitsvorfällen	Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit	Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit, Schadensminimierung, Ansehenswahrung
Verantwortung des obersten Organs	nicht festgelegt	grundsätzlich festgelegt (2002)	nicht festgelegt
Berücksichtigung von Organisation und Personal	ja	ja	ja

Quellen: BMF; BMK; BML

(2) Die Erlässe des Finanzministeriums hielten die Verantwortung der Ressortleitung für die Einhaltung der Vorschriften zur Informationssicherheit nicht ausdrücklich fest. Das Finanzministerium gab dazu an, dass sich die Letztverantwortung der Ressortleitung bereits aus dem Gesetz ergebe und die Präambel der IT–Sicherheitsstrategie ein Bekenntnis des Finanzministeriums zu einem integrierten Informationssicherheits– und Datenschutzmanagement enthalte.

Alle neun nachgeordneten Dienststellen[42] waren vom Geltungsbereich der relevanten Informationssicherheitsregelungen erfasst, einschließlich der Fernmeldebe-

[42] Bundesfinanzgericht, Finanzprokuratur, Finanzamt Österreich, Zollamt Österreich, Finanzamt für Großbetriebe, Amt für Betrugsbekämpfung, Prüfdienst für Lohnabgaben und Beiträge, Zentrale Services, Fernmeldebüro

hörde, die mit der BMG–Novelle 2022 in den Zuständigkeitsbereich des Finanzministeriums verschoben wurde.

(3) Im Klimaschutzministerium waren die allgemeinen „Grundsätze zur IT–Sicherheitspolitik“[43] aus dem Jahr 2002 – z.B. zu den Schutzzielen oder zum Risikomanagement – noch anwendbar; organisatorische Aspekte entsprachen aber nicht mehr den Gegebenheiten, einzelne Themen wie etwa Schulungen oder Notfallvorsorge sprach das Dokument nicht oder nur grundsätzlich an. Eine Aktualisierung war geplant. Die IT–Abteilung verwendete eine – zuletzt im März 2023 aktualisierte – vertrauliche interne Richtlinie mit Organisations– und Prozessbeschreibungen. Für alle Bediensteten waren die Datensicherheitsvorschrift aus 2020 und die IKT–Arbeitsplatzrichtlinie aus 2021 verbindlich, die einzelne konkrete Anweisungen hinsichtlich der IT–Sicherheit vorgaben.

Von den nachgeordneten Dienststellen erfasste das Regelwerk des Klimaschutzministeriums zur IT–Sicherheit die Sicherheitsuntersuchungsstelle des Bundes. Das nachgeordnete Österreichische Patentamt wurde IT–technisch nicht vom Ministerium betreut; es hatte eine eigene IT–Abteilung mit eigenen Regelungen zur IT–Sicherheit. Das Ministerium war über den Status der IT–Sicherheit im Österreichischen Patentamt nicht umfassend informiert.

(4) Das Landwirtschaftsministerium hatte nur seine IT–Strategie mit allgemeinen Zielen per Rundschreiben kundgemacht; nicht jedoch die interne IT–Sicherheitsstrategie mit Zielen, Verantwortlichkeiten sowie Organisation des IT–Sicherheitsmanagements. Die Verantwortung der Ressortleitung war in den strategischen Dokumenten nicht festgehalten. Die IKT–Abteilung des Landwirtschaftsministeriums verfügte intern über vertrauliche Richtlinien zur IT–Sicherheit, die zuletzt im Dezember 2022 aktualisiert wurden.

Für alle Bediensteten – auch im nachgeordneten Bereich[44] – galten die Datensicherheitsvorschrift und die BenutzerInnenrichtlinie (zuletzt aktualisiert 2019 bzw. 2020) mit einzelnen konkreten Anweisungen zu generellen Sicherheitsmaßnahmen. Die IKT–Abteilung des Landwirtschaftsministeriums erhielt jährlich eine (unterschiedlich ausgestaltete) Übersicht zum Status der IT–Sicherheit von den nachgeordneten Dienststellen.

[43] „Grundsätze zur IT–Sicherheitspolitik des BMVIT“, Juni 2002

[44] Bundesanstalt für Agrarwirtschaft und Bergbauernfragen, Bundesamt für Weinbau, Bundesamt für Wasserwirtschaft, Forsttechnischer Dienst für Wildbach– und Lawinenverbauung, Bundeskellereiinspektion, Erstanlaufstelle für Beschwerden betreffend Handelspraktiken im Zusammenhang mit dem Verkauf von Agrar– und Lebensmittelerzeugnissen, 13 Schulen; ausgenommen waren das Bundesamt für Ernährungssicherheit und das Bundesamt für Wald, deren IKT ausgegliederte Rechtsträger betreuten.

10.2 Der RH anerkannte, dass das Finanzministerium über eine IT–Sicherheitsstrategie für alle – auch die nachgeordneten – Dienststellen verfügte, die wesentliche Ziele, zentrale Rollen und Prozesse und nachvollziehbare Maßnahmen definierte und organisatorische und personelle Aspekte berücksichtigte. Diese IT–Sicherheitsstrategie hielt die Verantwortung der Ressortleitung für die IT–Sicherheit nicht ausdrücklich fest. Aus Sicht des RH würde der Hinweis auf die Verantwortung der Ministerin bzw. des Ministers – auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie – einen Beitrag zu einem erhöhten „Management Commitment" leisten und die Akzeptanz und den Umsetzungserfolg der IT–Sicherheitsstrategie steigern.

Der RH empfahl daher dem Finanzministerium, in der IT–Sicherheitsstrategie die Verantwortung der Ressortleitung für die IT–Sicherheit ausdrücklich festzuhalten.

Der RH kritisierte, dass die IT–Sicherheitsstrategie des Klimaschutzministeriums („Grundsätze zur IT–Sicherheitspolitik") aus 2002 stammte, weil damit die allgemeine IT–Sicherheitspolitik mit den Grundsätzen der IT–Sicherheit (Ziele, Verantwortlichkeiten, Organisation, Methoden) nicht mehr zur Gänze den aktuellen Gegebenheiten entsprach.

Er kritisierte, dass das Landwirtschaftsministerium keine intern kundgemachte, ressortweite IT–Sicherheitsstrategie mit Zielen, Verantwortlichkeiten, Organisation des IT–Sicherheitsmanagements und Methoden – ergänzend zu Datensicherheitsvorschrift und BenutzerInnenrichtlinie – erlassen hatte.

Der RH empfahl daher dem Klimaschutz– und dem Landwirtschaftsministerium, eine grundsätzliche Richtlinie zur IT–Sicherheit für alle Bediensteten zu erlassen, mit Zielen, Verantwortlichkeiten, Grundsätzen des IT–Risikomanagementsystems, Organisation und Methoden. Diese IT–Sicherheitsstrategie sollte die geltenden Grundsätze transparent und nachvollziehbar darstellen und das Bewusstsein (Awareness) für IT–Sicherheit bei den Bediensteten erhöhen. Sie wäre auch für die nachgeordneten Dienststellen für verbindlich zu erklären.

Der RH stellte fest, dass im Klimaschutz– und im Landwirtschaftsministerium die nachgeordneten Dienststellen nur teilweise in das IT–Sicherheitsmanagement der Zentralstellen eingebunden waren. Das Klimaschutzministerium verfügte über keine konkreten, regelmäßig aktualisierten Informationen zur IT–Sicherheit aus der nachgeordneten Dienststelle Österreichisches Patentamt. Das Landwirtschaftsministerium erhielt jährlich eine Übersicht der nachgeordneten Dienststellen zum Status der IT–Sicherheit, jedoch in unterschiedlicher Ausgestaltung.

Der RH empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, den nachgeordneten Dienststellen, denen die Gewährleistung der IT–Sicherheit eigenständig obliegt, (erweiterte) Berichtspflichten aufzuerlegen – insbesondere zu Abweichungen von den geltenden Strategien, Sicherheitsvorfällen, durchgeführten Audits und der Erfüllung von Sicherheitsstandards –, damit die Ressortleitung im Bedarfsfall ihre Steuerungsfunktion erfüllen kann.

10.3 (1) Das Finanzministerium teilte in seiner Stellungnahme mit, dass im Zuge der 2024 noch abzuschließenden Aktualisierung seiner Informationssicherheits– und Datenschutzerlässe die Empfehlung, die Verantwortung der Ressortleitung für die IT–Sicherheit ausdrücklich festzulegen, berücksichtigt sei.

(2) Laut Stellungnahme des Landwirtschaftsministeriums würden eine Überarbeitung der IT–Sicherheitsstrategie sowie eine Erweiterung der Berichtspflichten der nachgeordneten Dienststellen unter Berücksichtigung der Empfehlungen des RH in Aussicht genommen.

Management von IT–Sicherheitsrisiken

11.1 (1) Das Informationssicherheitshandbuch beschrieb drei verschiedene Ansätze zur Risikoanalyse:

- die detaillierte Risikoanalyse mit individuellen Sicherheitsmaßnahmen für jedes IT–System,
- den Grundschutz für alle IT–Systeme und
- den kombinierten Ansatz (Kombination von Grundschutzmaßnahmen und individuellen Sicherheitsmaßnahmen je nach Schutzbedarf).[45]

Nach dem NISG[46] hatten die Bundesministerien für wichtige Dienste risikoorientierte, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Die Identifizierung wichtiger Dienste, die jedem Bundesministerium selbst oblag, setzte daher eine Analyse[47] sämtlicher Dienste (IT–Verfahren und Systeme) voraus (TZ 8).

[45] Informationssicherheitshandbuch Version 4.3.3 Kapitel 4; siehe auch den RH–Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 8)

[46] § 22

[47] insbesondere zu den Auswirkungen eines Ausfalls, unter Berücksichtigung der Anzahl der Nutzerinnen und Nutzer, der verarbeiteten Daten, der Ersatzmöglichkeiten und des Vertrauensverlustes

Die Systematik des Managements von IT–Sicherheitsrisiken in den überprüften Bundesministerien stellte sich wie folgt dar:

Tabelle 5: Systematik des Managements von IT–Sicherheitsrisiken

Thema	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
strategische Verankerung	ja	ja	ja
Ansatz	detaillierte Risikoanalysen	kombinierter Ansatz	kombinierter Ansatz
Schutzbedarfs– und Risikoanalysen	ja	ja	ja
wichtige Dienste gemäß NISG	ja, 91 Dienste[1]	nein	nein

NISG = Netz– und Informationssystemsicherheitsgesetz Quellen: BMF; BMK; BML

[1] im April 2023, inklusive der zwölf Dienste, die mit der BMG–Novelle 2022 von den Bundesministerien für Digitalisierung und Wirtschaftsstandort bzw. für Landwirtschaft, Regionen und Tourismus übernommen wurden

(2) Das Finanzministerium erstellte und aktualisierte Risikoanalysen in einem fortlaufenden Prozess. Die Umsetzung der festgelegten Sicherheitsanforderungen und –maßnahmen hatte der Auftragsverarbeiter (hauptsächlich die BRZ GmbH) in einem Sicherheitskonzept zu dokumentieren. Bis Juli 2023 setzte das Ministerium den Risikoanalyseprozess auch für die ab Juli 2022 neu in seine Zuständigkeit übernommenen Bereiche fertig um.

(3) Das Klimaschutzministerium führte im Sinne eines kombinierten Ansatzes bei der Entwicklung neuer Anwendungen eine Schutzbedarfsanalyse sowie für einzelne kritische IT–Systeme bzw. IT–Anwendungen detaillierte Risikoanalysen durch; diese wurden anlassbezogen überprüft, etwa bei technischen Änderungen, aber mangels personeller Ressourcen nicht in regelmäßigen Intervallen. Die Ausführungen zum Risikomanagement in der IT–Sicherheitsstrategie des Klimaschutzministeriums stammten aus 2002.

Nach Ansicht des Klimaschutzministeriums lägen keine wichtigen Dienste im Sinne des NISG vor: Die IT–Anwendungen wie das Führerscheinregister oder das elektronische Datenmanagement nach dem Abfallwirtschaftsgesetz[48] könnten bei einem Ausfall ersetzt werden bzw. komme ihnen keine wesentliche Bedeutung für die Aufrechterhaltung öffentlicher Leistungen zu.[49]

(4) Die IT–Sicherheitsstrategie des Landwirtschaftsministeriums legte für das Management von IT–Sicherheitsrisiken den kombinierten Ansatz fest. Regelmäßige Überprüfungen von Risikoanalysen sah sie mangels personeller Ressourcen nicht vor, bei Weiterentwicklungen wurde die ursprüngliche Schutzbedarfsfeststellung überprüft. Die Wirksamkeit der für die IT–Verfahren des Ministeriums festgelegten

[48] BGBl. I 102/2002 i.d.g.F.

[49] Das Führerscheinregister und das Elektronische Datenmanagement in der Abfallwirtschaft (EDM) waren Register, in die Pflichtmeldungen von mehreren Gruppen von Nutzerinnen und Nutzern einzutragen waren.

Sicherheitsmaßnahmen überprüfte und dokumentierte es quartalsweise (Schutzbedarfsreport).

Das Landwirtschaftsministerium hatte für definierte Kernaufgaben besondere Sicherheitsvorkehrungen getroffen. Das betraf etwa bundesweit angewendete Systeme wie jene für die Haushalts– oder Aktenverwaltung. Nach Ansicht des Landwirtschaftsministeriums lagen keine wichtigen Dienste im Sinne des NISG vor, obwohl es z.B. das Wasserinformationssystem führte.[50]

11.2 Der RH anerkannte, dass das Finanzministerium ein umfassendes und detailliertes IT–Risikomanagementsystem eingerichtet hatte.

Er kritisierte, dass das IT–Risikomanagement des Klimaschutzministeriums in einer IT–Sicherheitsstrategie aus 2002 beschrieben war. Die Verankerung in einer aktuellen Strategie fehlte. Der RH kritisierte, dass das Landwirtschaftsministerium die Grundsätze des IT–Risikomanagements nur in die abteilungsinterne, regelmäßig aktualisierte IT–Sicherheitspolitik aufgenommen hatte. Die Verankerung in einer ressortweit kundgemachten Strategie fehlte. Zur zugehörigen Empfehlung für beide Bundesministerien verwies der RH auf TZ 10.

Weiters kritisierte der RH, dass das Klimaschutz– und das Landwirtschaftsministerium vorhandene Schutzbedarfs– und Risikoanalysen im Anlassfall bzw. bei Weiterentwicklungen, aber nicht regelmäßig überprüften.

Er empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, jene kritischen IT–Verfahren festzulegen, für die Risikoanalysen regelmäßig zu überprüfen und gegebenenfalls zu aktualisieren wären.

Der RH stellte fest, dass das Klimaschutz– und das Landwirtschaftsministerium nach ihrer Einschätzung keine wichtigen Dienste im Sinne des NISG identifiziert hatten. Er verwies auf den Umsetzungsleitfaden für öffentliche Einrichtungen vom September 2019[51], in dem das Bundeskanzleramt Kriterien für die Beurteilung wichtiger Dienste empfohlen hatte. Nach Ansicht des RH betraf dies nicht nur IT–Anwendungen zur Aufrechterhaltung der öffentlichen Daseinsvorsorge[52], sondern auch zur Aufrechterhaltung der Funktions– und Arbeitsfähigkeit eines Ministeriums als staatliche Einrichtung. Weiters wies er darauf hin, dass mit der Umsetzung der NIS–2–

[50] Die Datenbank zum Wasserinformationssystem Austria nach dem Wasserrechtsgesetz enthielt Daten zu Gewässerzustand, Wassernutzung und Hochwasserrisiko sowie ein elektronisches Register über Belastungen. Teile davon konnten auch öffentlich abgerufen werden. Weiters war das Landwirtschaftsministerium für die Weindatenbank verantwortlich, in die Erzeuger ab einer bestimmten Produktionsmenge Daten elektronisch zu übermitteln hatten.

[51] NIS Fact Sheet 9/2019, www.nis.gv.at (Rechtliches und Dokumente)

[52] in den Bereichen Gesundheit, Wasser, Energie, öffentlicher Verkehr

Richtlinie[53] die Bundesministerien – als wesentliche Einrichtung der öffentlichen Verwaltung der Zentralregierung – mit ihren IT–Anwendungen den von der Richtlinie geforderten Sicherheitsvorkehrungen sowie einer (allfällig neu einzurichtenden) Aufsicht unterliegen werden (TZ 9). Nach Ansicht des RH wird dies die Sicherheitsanforderungen zukünftig erhöhen.

Der RH empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, ihre IT–Anwendungen nach jenen Kriterien, die im Umsetzungsleitfaden des Bundeskanzleramts für die öffentlichen Einrichtungen nach dem NISG beschrieben sind, zu überprüfen und allfällig vorliegende wichtige Dienste zu identifizieren (z.B. das Führerscheinregister, das elektronische Datenmanagement nach dem Abfallwirtschaftsgesetz oder das Wasserinformationssystem). Dies wäre auch zweckmäßig als Vorbereitung auf die Umsetzung der NIS–2–Richtlinie.

11.3 Das Landwirtschaftsministerium teilte in seiner Stellungnahme mit, dass eine Überarbeitung des IT–Risikomanagementsystems und eine Definition von wichtigen Diensten unter Berücksichtigung der NIS–2–Richtlinie sowie der Empfehlungen des RH in Aussicht genommen würden.

[53] national umzusetzen bis Oktober 2024

Internes Berichtswesen

12.1 (1) Die verantwortliche Führungsebene benötigt regelmäßig bzw. im Anlassfall Informationen zu Sicherheitsanforderungen und deren Umsetzung, zu Sicherheitskennzahlen, aktuellen Sicherheitsrisiken, Sicherheitsschwachstellen oder Sicherheitsvorfällen. Durch ein solches internes Berichtswesen sollen Fehler, Risiken und Schwachstellen erkannt, bewertet und verringert sowie die IT–Sicherheitsstrategie und die darauf aufbauenden Vorgaben, Abläufe und Sicherheitsmaßnahmen optimiert werden (Punkt 18.1.2 Informationssicherheitshandbuch).

Das interne Berichtswesen in den überprüften Bundesministerien stellte sich wie folgt dar:

Tabelle 6: Internes Berichtswesen zur IT–Sicherheit

Berichtswesen	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
strategische Verankerung	ja, für regelmäßige und anlassbezogene Berichte	ja, für anlassbezogene Berichte[1]	ja, für anlassbezogene Berichte
Festlegung von Berichtsweg und Berichtsempfängerin bzw. –empfänger	ja	ja	ja
Erstellung von regelmäßigen Berichten	ja, jährlich	ja, halbjährlich	ja, quartalsweise
Empfängerin bzw. Empfänger regelmäßiger Berichte	jeweils verantwortliche Sektionsleitung, Kabinett der Bundesministerin bzw. des Bundesministers	Leitung IT–Abteilung	Leitung IT–Abteilung

[1] Regelmäßige Berichte waren in der IT–Sicherheitsstrategie aus 2002 nur grundsätzlich (TZ 10) erwähnt.

Quellen: BMF; BMK; BML

(2) Im Finanzministerium hatte die bzw. der Informationssicherheitsbeauftragte einen jährlichen Management–Bericht zur Informationssicherheit an die zuständige Sektionsleitung (bzw. an eine allfällige Generalsekretärin oder einen allfälligen Generalsekretär) zu erstatten. Ergänzend wurde der Bericht zur Information an das Kabinett der Bundesministerin bzw. des Bundesministers übermittelt. Der Bericht gab u.a. die Anzahl von Risikoanalysen, Audits und Sicherheitsvorfällen und das Ergebnis des Zertifizierungsaudits des Informationssicherheitsmanagementsystems an.

Auch für die Meldung von Sicherheitsvorfällen (anlassbezogene Berichterstattung) gab die IT–Sicherheitsstrategie die Strukturen, Inhalte und Berichtswege vor.

(3) Ein regelmäßiges Berichtswesen hatte das Klimaschutzministerium nur grundsätzlich in der IT–Sicherheitsstrategie aus 2002 verankert. Nach der internen Richtlinie der IT–Abteilung waren regelmäßig technische Prüfberichte innerhalb dieser Abteilung zu erstellen. Ein zusammenfassender Bericht mit Sicherheitskennzahlen

an die obere Führungsebene war nicht zu erstatten. Anlassbezogene Meldungen bzw. Berichte waren bei Sicherheitsvorfällen vorgesehen, Berichtsweg und Berichtsempfängerin bzw. –empfänger waren festgelegt.

(4) Das Landwirtschaftsministerium hatte ein regelmäßiges Berichtswesen in der IT–Sicherheitsstrategie nicht verankert. Quartalsweise erstellte die IT–Abteilung interne Berichte zum Schutzbedarf. Ein zusammenfassender Bericht mit Sicherheitskennzahlen an die obere Führungsebene lag nicht vor. Anlassbezogene Meldungen bzw. Berichte waren bei Sicherheitsvorfällen vorgesehen, Berichtsweg und Berichtsempfängerin bzw. –empfänger waren festgelegt.

12.2 Der RH anerkannte, dass das Finanzministerium ein regelmäßiges und ein anlassbezogenes Berichtswesen standardisiert eingerichtet hatte; ergänzend erhielt die Ressortleitung (über das Kabinett) jährliche Berichte zur Informationssicherheit.

Der RH empfahl dem Finanzministerium, in der IT–Sicherheitsstrategie neben der zuständigen Sektionsleitung auch die Ressortleitung als konkrete Berichtsempfängerin bzw. konkreten Berichtsempfänger festzulegen. Dies wäre auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie, die die Verantwortung der Leitungsorgane ausdrücklich fordert (Art. 20 Governance), zweckmäßig.

Der RH wies kritisch darauf hin, dass im Klimaschutz– und im Landwirtschaftsministerium die obere Führungsebene (Sektionsleitung, Generalsekretärin bzw. Generalsekretär, Ressortleitung) keine regelmäßigen, standardisierten Berichte mit Kennzahlen zur IT–Sicherheit erhielt und ihr somit relevante Informationen zur Steuerung des IT–Sicherheitsmanagements fehlten.

Der RH empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, in der IT–Sicherheitsstrategie ein regelmäßiges, standardisiertes Berichtswesen zur IT–Sicherheit unter Einbeziehung der oberen Führungsebene (Sektionsleitung, Generalsekretärin bzw. Generalsekretär, Ressortleitung) als Berichtsempfängerin bzw. Berichtsempfänger festzulegen. Dies wäre auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie, die die Verantwortung der Leitungsorgane ausdrücklich fordert (Art. 20 Governance), zweckmäßig.

12.3 (1) Das Finanzministerium teilte in seiner Stellungnahme mit, dass im Zuge der 2024 noch abzuschließenden Aktualisierung seiner Informationssicherheits– und Datenschutzerlässe die Empfehlung, auch die Ressortleitung als konkrete Berichtsempfängerin bzw. konkreten Berichtsempfänger festzulegen, berücksichtigt sei.

(2) Laut Stellungnahme des Landwirtschaftsministeriums werde eine Überarbeitung des Berichtswesens unter Berücksichtigung der Empfehlungen des RH in Aussicht genommen.

IT–Sicherheitsorganisation

Aufbau der IT–Sicherheitsorganisation

13.1 (1) In den drei überprüften Bundesministerien lagen die unmittelbare Leitung und Verantwortung für die IT auf Abteilungsebene; sie waren der Präsidialsektion zugeordnet.

(2) Im Finanzministerium fiel der Bereich IT–Sicherheit in die Zuständigkeit der Präsidialabteilung 6 „Multiprojektmanagement und IT–Koordination“.[54] Die Abteilung war u.a. für die Organisation, Evaluierung und Weiterentwicklung des Informationssicherheits– und Datenschutz–Managementsystems im gesamten Finanzressort (Ministerium und nachgeordnete Dienststellen) zuständig. Für den operativen Betrieb der IT–Anwendungen waren mehrere IT–Abteilungen in den Sektionen I und II (im Zusammenwirken mit dem Auftragnehmer BRZ GmbH) verantwortlich. In den mit der BMG–Novelle 2022 ins Finanzministerium übertragenen Sektionen V und VI lag die Budgetverantwortung für IT–Sicherheit in jeweils eigenen Abteilungen.

(3) Im Klimaschutzministerium war die unmittelbare Leitung für IT–Sicherheit bei der Präsidialabteilung 4 „Informations– und Kommunikationstechnik“ angesiedelt, die auch die IT–Angelegenheiten der nachgeordneten Dienststelle „Sicherheitsuntersuchungsstelle des Bundes“ verantwortete.[55]

(4) Im Landwirtschaftsministerium war die Präsidialabteilung 6 „IKT–Grundsatzangelegenheiten und IKT–Management“ für die IT–Sicherheit zuständig.

Nach der Konzeption der IT–Sicherheitsorganisation des Landwirtschaftsministeriums waren zwei Gremien vorgesehen: ein ressortweites Entscheidungsgremium (mit einem Arbeitsgremium[56], das der Genehmigungsinstanz[57] zuarbeitete) und ein IKT–Entscheidungsgremium (Mitglieder der IKT–Abteilung) (TZ 14). Da das Landwirtschaftsministerium das ressortweite Entscheidungsgremium nicht eingerichtet hatte, behandelte es Fragen der IKT–Sicherheit entweder je nach Anlass durch unterschiedliche einzelne Akteure oder im abteilungsinternen IKT–Entscheidungsgremium. Damit fehlte ein ressortweites Gremium, das neben der IKT–Abteilung andere Abteilungen und Hierarchien in die Themen und Entscheidungen der IT–Sicherheit einband.

[54] Mit der Auflösung des Generalsekretariats kam die Abteilung „GS/PM – Multiprojektmanagement und IT–Koordination“ als Präsidialabteilung 6 – „Multiprojektmanagement und IT–Koordination“ in die mit 18. Juli 2022 neu geschaffene Präsidialsektion.

[55] Die zweite nachgeordnete Dienststelle, das Österreichische Patentamt, war für seine IT–Angelegenheiten einschließlich IT–Sicherheit selbst verantwortlich.

[56] Informationssicherheitsbeauftragter, Chief Digital Officer, Chief Information Officer, IKT–Sicherheitsbeauftragter, Datenschutzbeauftragte und Sicherheitsbeauftragte des Ressorts

[57] Sektionsleitung, Generalsekretärin oder Generalsekretär bzw. politische Ebene

13.2 Der RH hielt fest, dass die IKT–Abteilungen der Bundesministerien die IT–Angelegenheiten und das Management der IT–Sicherheit jeweils innerhalb ressortspezifischer organisatorischer Rahmenbedingungen wahrnahmen.

Er hielt weiters fest, dass das Landwirtschaftsministerium das ressortweite Entscheidungsgremium, das in seiner IT–Sicherheitsorganisation vorgesehen war, nicht umgesetzt hatte. Der RH sah ein derartiges Gremium, das ressortweite Themen der IKT–Sicherheit behandeln und unter Mitwirkung weiterer damit befasster Abteilungen Strategien und Ziele setzen sollte, grundsätzlich als Benchmark zur ressortinternen effektiven Abstimmung und Gestaltung der IT–Sicherheit.

Er empfahl dem Landwirtschaftsministerium, das von ihm geplante ressortweite Entscheidungsgremium für IKT–Sicherheit in die Praxis umzusetzen und über den Nutzen und die Effektivität einer derartigen Organisation in den Gremien CDO–Task–Force[58] und IKT–Bund zu berichten.

13.3 Das Landwirtschaftsministerium teilte in seiner Stellungnahme mit, dass im Rahmen der Umsetzung der Maßnahmen zur Verbesserung der IT–Sicherheit auch die Bemühungen zur verstärkten internen Mitbefassung anderer Organisationseinheiten als der IKT–Abteilung intensiviert würden und auch die Umsetzung des ressortweiten Entscheidungsgremiums in Aussicht genommen werde.

Funktionen und Rollen in der IT–Sicherheitsorganisation

14.1 (1) Für die effiziente Wahrnehmung der operativen Aufgaben der IT–Sicherheit ist es notwendig, Rollen und klare Verantwortlichkeiten festzulegen. Dafür haben sich Standardfunktionen etabliert, denen entsprechende Aufgaben zugeordnet sind:

1. Für alle Fragen der Informations– und IT–Sicherheit ist der Chief Information Security Officer (CISO) verantwortlich.

2. Der Leiter der für die gesamte Infrastruktur und den Betrieb verantwortlichen IT–Abteilung wird auch als Chief Information Officer (CIO) bezeichnet.

3. Der Informationssicherheitsbeauftragte (ISB) ist gemäß Informationssicherheitsgesetz in jedem Bundesministerium einzurichten und überwacht primär die Einhaltung dieses Bundesgesetzes.

4. Der Chief Digital Officer (CDO) ist für die Digitalisierungsstrategie und Digitalisierungsmaßnahmen eines Bundesministeriums zuständig.

[58] **CDO** = Chief Digital Officer

(2) In den überprüften Bundesministerien waren die folgenden für die IT–Sicherheit relevanten Funktionen (Rollen) eingerichtet:

Tabelle 7: Funktionen der IT–Sicherheitsorganisation

Inhaber der Funktion – Rolle (in Klammer: Abteilung bzw. Sektion)			
Funktion	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
Chief Information Security Officer (CISO) verantwortlich für die Informationssicherheit (somit auch für die IT–Sicherheit) im Bundesministerium	Referent/in (Präs. 6)	–	Abteilungsleitung (PR/6)
Leiter der IT–Abteilung (Chief Information Officer – CIO) verantwortlich für die IT–Infrastruktur des Bundesministeriums	Abteilungsleitung (Präs. 6)	Abteilungsleitung (Präs. 4)	Abteilungsleitung (PR/6)
Informationssicherheitsbeauftragter (ISB) gemäß Informationssicherheitsgesetz Überwachung der Einhaltung des Informationssicherheitsgesetzes	Referent/in (Präs. 6)	Referent/in (Präs. 3)	Referent/in (PR/7)
Chief Digital Officer (CDO) Entwicklung und Umsetzung einer grundlegenden Digitalisierungsstrategie im Bundesministerium	stellvertretender Kabinettschef des Bundesministers	Abteilungsleitung (Präs. 8)	Sektionsleitung (Präsidium)

Quellen: BMF; BMK; BML

Die Organisation der IT–Sicherheit wies folgende Besonderheiten auf:

- Das Finanzministerium hatte neben den in Tabelle 7 ausgewiesenen Funktionen auch die Funktionen der Informationssicherheitsexpertinnen bzw. –experten und der Informationssicherheitskoordinatorinnen bzw. –koordinatoren besetzt. Die in der Präsidialabteilung 6 angesiedelten Informationssicherheitsexpertinnen bzw. –experten waren für den Betrieb und die Weiterentwicklung des Informationssicherheitsmanagementsystems zuständig; die Koordinatorinnen bzw. Koordinatoren fungierten in den IT–Abteilungen der anderen Sektionen des Finanzministeriums als Ansprechpersonen in Angelegenheiten der Informationssicherheit.
- Das Klimaschutzministerium hatte keinen für die Informations– und IT–Sicherheit gesamtverantwortlichen Chief Information Security Officer (CISO), die Einrichtung dieser Rolle war jedoch geplant. Die Aufgaben des CISO waren im überprüften Zeitraum auf Mitarbeiterinnen und Mitarbeiter der IKT–Abteilung aufgeteilt (Chief Information Officer (CIO), Teamkoordinatorinnen bzw. –koordinatoren und technische Expertinnen bzw. Experten).
- Im Landwirtschaftsministerium war der Chief Information Security Officer (CISO) gleichzeitig mit der Leitung der IT–Abteilung betraut (CIO); damit war die Funktion nicht unabhängig von der operativen IT eingerichtet.

14.2 Der RH hielt kritisch fest, dass das Klimaschutzministerium über keinen Chief Information Security Officer (CISO) verfügte.

Er empfahl dem Klimaschutzministerium, die Funktion des Chief Information Security Officers rasch zu besetzen.

Der RH hielt kritisch fest, dass im Landwirtschaftsministerium die Rolle des Chief Information Security Officers (CISO) mit der Rolle des IT–Abteilungsleiters (CIO) ident war.

Er empfahl dem Landwirtschaftsministerium, die Funktion des Chief Information Security Officers unabhängig von der IT–Abteilungsleitung einzurichten.

14.3 Laut Stellungnahme des Landwirtschaftsministeriums werde eine Änderung hinsichtlich der Funktion des Chief Information Security Officers in Aussicht genommen.

Informationssicherheitsmanagement–Team

15.1 (1) Für die Umsetzung der IT–Sicherheitsziele ist die organisationsweite Koordinierung der IT–Sicherheit wesentlich. Die Koordinierung sollte jedenfalls die Führungskräfte, die für die IT–Sicherheit verantwortlichen Funktionsträgerinnen und –träger sowie ausgewählte Vertretungen der Anwenderinnen und Anwender umfassen. Bei Bedarf können auch weitere Expertisen, etwa zum Risikomanagement, sowie die nachgeordneten Dienststellen eingebunden werden.

In größeren Organisationen ist es daher, wie im Informationssicherheitshandbuch dargestellt, zweckmäßig, ein Informationssicherheitsmanagement–Team aufzubauen, das die Verantwortlichen unterstützt, die übergreifenden Belange der IT–Sicherheit koordiniert sowie Pläne, Vorgaben und Richtlinien erarbeitet, z.B. Schutzmaßnahmen, Klassifizierung und Kennzeichnung von Informationen. Laut Informationssicherheitshandbuch sollen neben dem Chief Information Security Officer (CISO) und seiner Stellvertretung auch Anwenderinnen und Anwender Mitglieder dieses Teams sein.

Die internen Koordinationsstrukturen stellten sich im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium wie folgt dar:

Tabelle 8: Interne Koordination des Informationssicherheitsmanagements

Gestaltung des Informationssicherheits-management–Teams	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
Informationssicherheits-management–Team eingerichtet	ja, gemäß Managementhandbuch	in die IT–Sicherheits– und Sachverständigenkommission eingegliedert	ja, gemäß IT–Sicherheitspolitik
Aufgaben des Informa-tionssicherheits-management–Teams	u.a. Risikomanagement, Vorfallsmanagement, Compliance (Umsetzung Sicherheits-standard ISO 27001)[1]	Festlegung von IT–Sicher-heitszielen und –strategie, Erstellung IT–Sicherheits-konzept und Desaster–Recovery–Strategie, Informations– und Trainingsprogramme	Aufbau der Sicherheits-architektur, Risikomanage-ment, Durchführung von Sicherheitsberatungen und –prüfungen
Vorsitz durch	Vorsitz je nach Gremium Abteilungsleitung (Präs. 6) oder CISO/ISB	nicht definiert, in der Praxis Abteilungsleitung IKT (Präs. 4)	Abteilungsleitung IKT (PR/6)
vorgesehene Sitzungsfrequenz	je nach Gremium wöchentlich bis jährlich	nicht definiert, im Anlassfall	jährlich bzw. im Anlassfall
Einbindung der für die IT–Sicherheit verantwort-lichen Funktionsträgerin-nen und –träger	ja	ja	bei Bedarf
Einbindung nachge-ordneter Dienststellen	ja	ja: Sicherheitsuntersuchungs-stelle nein: Österreichisches Patent-amt	nein
Einbindung der Anwende-rinnen und Anwender	nein	nein	bei Bedarf
Einbindung Externer	ja	im Anlassfall	bei Bedarf: externe Expertinnen und Experten

CISO = Chief Information Security Officer
IKT = Informations– und Kommunikationstechnologie
ISB = Informationssicherheitsbeauftragte bzw. –beauftragter

Quellen: BMF; BMK; BML

[1] Die Norm ISO 27001 spezifizierte die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems.

(2) Das Informationssicherheitsmanagement–Team des Finanzministeriums bestand aus dem Chief Information Security Officer (CISO), der bzw. dem Informationssicherheitsbeauftragten samt Stellvertretung und zwei Informationssicherheitsexpertinnen bzw. –experten. Neben dem wöchentlichen ISMS–Jour–fixe[59], der zur Information und Abstimmung aktueller Themen unter dem Vorsitz von CISO und Infor-

[59] ISMS = Informationssicherheitsmanagementsystem

mationssicherheitsbeauftragter bzw. –beauftragtem diente, waren weitere Gremien im Rahmen des Informationssicherheitsmanagement–Teams eingerichtet:

- Informationssicherheits– und Datenschutz–Jour–fixe: Information und Abstimmung zwischen Informationssicherheitsmanagement–Team und Datenschutzmanagement–Team,
- Security Board: Information und Abstimmung zwischen Finanzministerium und BRZ GmbH,
- Abteilungs–Jour–fixe,
- Informationssicherheits– und Datenschutzmanagement–Review: jährlich zur Prüfung der Leistungsfähigkeit des Informationssicherheits– und Datenschutz–Managementsystems.

(3) Im Klimaschutzministerium war laut dem Dokument „Grundsätze zur IT–Sicherheitspolitik“ vom Juni 2002 die Einrichtung eines Informationssicherheitsmanagement–Teams vorgesehen. Die im internen IKT–Organisationshandbuch definierte IT–Sicherheits– und Sachverständigenkommission – ursprünglich für den ordnungsgemäßen Umgang mit Bundeseigentum gegründet – übernahm die Aufgaben des Informationssicherheitsmanagement–Teams. Sie bestand aus den Teamkoordinatorinnen bzw. –koordinatoren sowie der IKT–Abteilungsleitung; im Anlassfall wurden Expertinnen und Experten wie die bzw. der Informationssicherheitsbeauftragte hinzugezogen; ein Vorsitz war nicht festgelegt. Im überprüften Zeitraum vor der COVID–19–Pandemie tagte die Kommission regelmäßig meist monatlich, seitdem anlassbezogen.

(4) Im Landwirtschaftsministerium war das Informationssicherheitsmanagement–Team als Teil des IT–Sicherheits–Managements eingerichtet. Die IKT–Abteilung betreute die Aufgaben der Informationssicherheit mit; neben der Abteilungsleitung (IT–Management) war die bzw. der IKT–Sicherheitsbeauftragte Mitglied des Kernteams. Die bzw. der Informationssicherheitsbeauftragte gemäß Informationssicherheitsgesetz war der Präsidialabteilung 7 zugeordnet. Das Informationssicherheitsmanagement–Team tagte im Anlassfall, aber zumindest einmal im Jahr. Bei Bedarf konnten auch betroffene Bereichsbeauftragte der IT–Sicherheit, externe Expertinnen und Experten sowie die bzw. der Informationssicherheitsbeauftragte hinzugezogen werden.

15.2 Der RH stellte fest, dass im Informationssicherheitsmanagement–Team des Finanzministeriums – entgegen der Empfehlung des Informationssicherheitshandbuchs – keine Anwenderinnen und Anwender vertreten waren.

Er empfahl dem Finanzministerium, Anwenderinnen und Anwender in das Informationssicherheitsmanagement–Team aufzunehmen.

Der RH hielt fest, dass im Klimaschutzministerium die Einrichtung eines Informationssicherheitsmanagement–Teams laut den 2002 verfassten „Grundsätzen zur IT–Sicherheitspolitik“ vorgesehen war. Er stellte jedoch kritisch fest, dass dieses Team nur unzureichend als Teil der IT–Sicherheits– und Sachverständigenkommission umgesetzt war, weil Sitzungen nicht regelmäßig abgehalten wurden, Anwenderinnen und Anwender nicht eingebunden waren und kein Vorsitz definiert war.

Der RH empfahl dem Klimaschutzministerium, ein Informationssicherheitsmanagement–Team einzurichten und dabei auf eine zweckentsprechende Einbindung der Anwenderinnen und Anwender sowie der nachgeordneten Dienststellen zu achten. Er empfahl zudem, wieder regelmäßig Sitzungen abzuhalten und den Vorsitz klar zu definieren (z.B. mittels Geschäftsordnung).

15.3 Das Finanzministerium teilte in seiner Stellungnahme mit, die Empfehlung des RH zu prüfen und gegebenenfalls unter Berücksichtigung der verfügbaren Ressourcen aufzugreifen.

IT–Sicherheit und Telearbeit

IT–Arbeitsplätze

16.1 (1) Mit der Dienstrechts–Novelle 2004[60] wurde die Möglichkeit, (regelmäßig) Telearbeit zu verrichten, im öffentlichen Dienst des Bundes ab Jänner 2005 gesetzlich verankert[61]. Mit der 2. Dienstrechts–Novelle 2018[62] führte der Gesetzgeber die anlassbezogene Telearbeit ein (Inkrafttreten 1. Jänner 2019)[63]. Die konkrete Ausgestaltung der gesetzlich verankerten Telearbeit war von weiteren ressortspezifischen Regelungen (in Form von Richtlinien bzw. generellen Weisungen) abhängig.

Die gesetzlichen Regelungen legten u.a. fest, dass der Bund als Dienstgeber den Bediensteten die zur Verrichtung von Telearbeit erforderliche technische Ausstattung zur Verfügung zu stellen hat. Mit der Dienstrechts–Novelle 2021[64] ergänzte der Gesetzgeber diese Regelungen dahingehend, dass mit Zustimmung der betroffenen Bediensteten die Ausstattung auch die bzw. der Bedienstete zur Verfügung stellen kann, soweit nicht dienstliche oder sonstige öffentliche Interessen entgegenstehen.[65] Zur ausführlichen Darstellung der Rechtsgrundlagen der Telearbeit im öffentlichen Dienst des Bundes verwies der RH auf seinen Bericht „Dienstrechtliche und technische Umsetzung von Telearbeit in ausgewählten Bundesministerien“ (Reihe Bund 2022/27, TZ 2 und TZ 9).

(2) Das Finanzministerium und das Klimaschutzministerium verfügten auch vor dem pandemiebedingten Home–Office über eine Vollausstattung mit dienstlichen mobilen IT–Arbeitsplätzen (Laptops), das Landwirtschaftsministerium erreichte die Vollausstattung Ende 2020. Die Möglichkeit der Nutzung eines privaten IT–Arbeitsplatzes (PC oder Laptop) für Telearbeit bestand nicht.

Teilweise stellten die drei Bundesministerien den Bediensteten für die Telearbeit Smartphones oder andere Mobiltelefone zur Verfügung. Für den Internetzugang nutzten die Bediensteten bei Telearbeit grundsätzlich den privaten Internetanschluss; war ein solcher nicht vorhanden, bestand in der Regel die Möglichkeit, eine Internetverbindung mit einem Hotspot über ein dienstliches Mobiltelefon herzustellen.

60 BGBl. I 176/2004

61 § 36a Beamten–Dienstrechtsgesetz 1979, BGBl. 333/1979 i.d.g.F.; § 5c Vertragsbedienstetengesetz 1948, BGBl. 86/1948 i.d.g.F.

62 BGBl. I 102/2018

63 Während die regelmäßige Telearbeit unter Berücksichtigung der gesetzlich umschriebenen Voraussetzungen jeweils für ein Jahr im Voraus (bei Beamtinnen und Beamten) angeordnet bzw. (mit Vertragsbediensteten) vereinbart werden konnte, sollte die anlassbezogene Telearbeit ausdrücklich nicht regelmäßig und nur für einzelne (ganze) Tage stattfinden. Mit der Dienstrechts–Novelle 2020, BGBl. I 153/2020, wurde die anlassbezogene Telearbeit auf Anlassfälle erweitert, die sich über einen längeren Zeitraum erstrecken können.

64 BGBl. I 136/2021

65 § 36a Abs. 4 und 5 Beamten–Dienstrechtsgesetz 1979 bzw. § 5c Abs. 4 und 5 Vertragsbedienstetengesetz 1948 i.d.F. der Dienstrechts–Novelle 2021

(3) Die folgende Tabelle zeigt IT–Ausstattung und Inanspruchnahme von Telearbeit in den drei überprüften Bundesministerien an den Stichtagen 29. Februar 2020 (vor der COVID–19–Pandemie), 31. Dezember 2020 (während der COVID–19–Pandemie), 31. Dezember 2021 und 31. Dezember 2022:

Tabelle 9: Telearbeit im Finanzministerium (BMF), Klimaschutzministerium (BMK) und Landwirtschaftsministerium (BML) – Ausstattung und Inanspruchnahme

Telearbeit an vier Stichtagen 2020 bis 2022						
	am 29. Februar 2020 (vor COVID–19–bedingtem Home–Office)			am 31. Dezember 2020 (Telearbeit bzw. Home–Office während COVID–19–Pandemie)		
	BMF	BMK	BML	BMF	BMK	BML
Bedienstete[2]	Anzahl					
Ministerium (ohne nachgeordnete Dienststellen) gesamt	765	791	811	764	854	797
davon						
mit Telearbeitsanordnung bzw. –vereinbarung	*83 (11 %)*	*158 (20 %)*	*114 (14 %)*	*222 (29 %)*	*220 (26 %)*	*110 (14 %)*
mobiler dienstlicher, für Telearbeit geeigneter IT–Arbeitsplatz	*765 (100 %)*	*791 (100 %)*	*494 (61 %)*	*764 (100 %)*	*854 (100 %)*	*772 (97 %)*
Anzahl der in diesem Monat tatsächlich geleisteten Tage in Telearbeit	597	458	635	7.401	2.269	6.699
Anzahl der Bediensteten, die in diesem Monat Telearbeit in Anspruch nahmen (regelmäßig oder anlassbezogen)	188 (25 %)	106 (13 %)	105 (13 %)	639 (84 %)	188 (22 %)	684 (86 %)
	am 31. Dezember 2021			am 31. Dezember 2022		
	BMF	BMK	BML	BMF[1]	BMK	BML
Bedienstete[2]	Anzahl					
Ministerium (ohne nachgeordnete Dienststellen) gesamt	747	842	816	964	872	677
davon						
mit Telearbeitsanordnung bzw. –vereinbarung	*332 (44 %)*	*499 (59 %)*	*106 (13 %)*	*461 (48 %)*	*612 (70 %)*	*207 (31 %)*
mobiler dienstlicher, für Telearbeit geeigneter IT–Arbeitsplatz	*747 (100 %)*	*842 (100 %)*	*791 (97 %)*	*964 (100 %)*	*872 (100 %)*	*677 (100 %)*
Anzahl der in diesem Monat tatsächlich geleisteten Tage in Telearbeit	7.280	4.840	6.296	2.882	3.220	2.481
Anzahl der Bediensteten, die in diesem Monat Telearbeit in Anspruch nahmen (regelmäßig oder anlassbezogen)	627 (84 %)	454 (54 %)	667 (82 %)	661 (69 %)	544 (62 %)	485 (72 %)

BMF = Finanzministerium
BMK = Klimaschutzministerium
BML = Landwirtschaftsministerium

Quellen: BMF; BMK; BML

[1] ohne Fernmeldebüro
[2] Eine Vergleichbarkeit der Zeitreihe der Personalstände ist aufgrund der Kompetenzverschiebungen zwischen diesen Bundesministerien (siehe Tabelle 2 und Abbildung 1) nicht gegeben.

Der Anteil der Bediensteten, die Telearbeit in Anspruch nahmen, war im Regelbetrieb im Dezember 2022 gegenüber Februar 2020 deutlich angestiegen und betrug zwischen 62 % im Klimaschutzministerium und 72 % im Landwirtschaftsministerium.

16.2 Der RH stellte fest, dass im Dezember 2022 alle Bediensteten der drei überprüften Bundesministerien einen mobilen dienstlichen, für Telearbeit geeigneten IT–Arbeitsplatz hatten. Dadurch fielen bestimmte Sicherheitsrisiken weg, die typischerweise mit der Verwendung eines privaten IT–Arbeitsplatzes (PC oder Laptop) verbunden sind, wie die Speicherung dienstlicher Daten auf privaten Endgeräten und geringere IT–Sicherheitsmaßnahmen.

Maßnahmen zur Erhöhung der IT–Sicherheit am IT–Arbeitsplatz bei Telearbeit

17.1 (1) Zusätzlich zu den IT–Sicherheitsrisiken eines IT–Arbeitsplatzes an der Dienststelle ergaben sich bei der Telearbeit weitere spezifische Risiken. Zu diesen zählten etwa der Verlust der mobilen IT–Ausstattung, der unbemerkte Zugang nicht berechtigter Personen zu den mobilen Arbeitsplatzrechnern, das Ausspähen von Zugangsdaten oder eine allfällige, infrastrukturbedingt geringere IT–Sicherheit als beim IT–Arbeitsplatz an der Dienststelle. Ein Teil dieser Risiken kann durch geeignete, dem Stand der Technik entsprechende technische sowie organisatorische Maßnahmen reduziert werden:

- Verschlüsselung der Daten auf den Festplatten der mobilen Arbeitsplätze: Diese Maßnahme reduzierte das Risiko, dass bei einem Verlust des Arbeitsplatzrechners (z.B. durch Diebstahl) bzw. bei einem unerlaubten Zugang zum Arbeitsplatzrechner die auf diesem Computer gespeicherten Daten missbräuchlich verwendet oder manipuliert werden konnten.
- Verhinderung des Startens eines Betriebssystems (Booten) von externen Datenträgern auf den mobilen IT–Arbeitsplätzen: Diese Maßnahme reduzierte das Risiko eines missbräuchlichen Zugangs zu den auf diesem Arbeitsplatzrechner gespeicherten Daten bzw. das Risiko der Veränderung dieser Daten.
- Eine USB–Port–Deaktivierung[66] bzw. USB–Port–Kontrolle konnte USB–Port–spezifische Risiken reduzieren.
- Applikations–Whitelisting gewährleistete, dass nur explizit erlaubte Anwendungen auf den IT–Arbeitsplätzen gestartet werden konnten.
- Ein verschlüsselter Datenaustausch zwischen mobilem Arbeitsplatz und zentraler IT–Infrastruktur reduzierte das Risiko, dass Unbefugte die übertragenen Daten ausspähen konnten.

[66] **USB** = Universal Serial Bus

- Virenschutz bzw. Schutz vor Schadsoftware schützte IT–Arbeitsplätze vor Viren, Trojanern, Ransomware, Spyware etc.
- Durch ein Endpoint–Protection–System sollte ein aktiver Schutz für sämtliche Endgeräte gewährleistet werden, um Cyber–Bedrohungen direkt am Endgerät – dort, wo sensible Daten gespeichert wurden bzw. gespeichert werden konnten – effektiv zu identifizieren, einzudämmen und zu eliminieren.
- Durch die Auto–VPN–Funktionalität[67] wurde automatisch (sobald eine Netzwerkverbindung aufgebaut wurde) eine verschlüsselte VPN–Verbindung vom Arbeitsplatzrechner zu den zentralen IT–Systemen des jeweiligen Bundesministeriums aufgebaut. Dadurch war gewährleistet, dass sämtliche Verbindungen ins Internet über die zentralen IT–Systeme geroutet und die Sicherheitsmechanismen der zentralen IT–Systeme genutzt werden.
- Durch (automatisierte) Software–Updates der Arbeitsplatzrechner wurde grundsätzlich sichergestellt, dass die installierten Softwarekomponenten (inklusive Betriebssystem) nicht veraltet waren und dadurch keine zusätzlichen Sicherheitsrisiken entstanden.
- Die Zwei–Faktor–Authentifizierung diente dem zusätzlichen Schutz gegen unbefugte Verwendung der IT–Arbeitsplätze (TZ 18).

(2) Die folgende Tabelle zeigt, welche dieser Maßnahmen in den überprüften Bundesministerien zur Zeit der Gebarungsüberprüfung im Einsatz waren:

Tabelle 10: Maßnahmen zur Erhöhung der IT–Sicherheit am IT–Arbeitsplatz

Maßnahmen	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
Festplatten–Verschlüsselung	eingerichtet	eingerichtet	eingerichtet
Unterbinden des Startens (Booten) von externen Datenträgern	eingerichtet	teilweise eingerichtet (bei älteren Geräten nicht eingerichtet)	eingerichtet
USB–Port–Deaktivierung bzw. USB–Port–Kontrolle	eingerichtet	nicht eingerichtet, Policies	nicht eingerichtet
Applikations–Whitelisting	eingerichtet	eingerichtet	nicht eingerichtet
verschlüsselter Datenaustausch	eingerichtet	eingerichtet	eingerichtet
Schutz vor Schadsoftware am mobilen Arbeitsplatz	eingerichtet	eingerichtet	eingerichtet
Endpoint–Protection am Arbeitsplatz	eingerichtet	teilweise eingerichtet[1]	eingerichtet
Auto–VPN	eingerichtet	nicht eingerichtet	nicht eingerichtet
automatisches Update bei Arbeitsplatzrechnern	eingerichtet	eingerichtet	eingerichtet

USB = Universal Serial Bus
VPN = Virtual Private Network

Quellen: BMF; BMK; BML

[1] Das Klimaschutzministerium verwies hierzu auf sein Schwachstellenmanagement (Software Vulnerability Management).

[67] **VPN** = Virtual Private Network

17.2 Das Finanzministerium, das Klimaschutzministerium und das Landwirtschaftsministerium hatten in unterschiedlichem Ausmaß wichtige technische Maßnahmen für die IT–Sicherheit am IT–Arbeitsplatz umgesetzt.

Der RH hielt kritisch fest,

- dass im Klimaschutzministerium das Unterbinden des Startens von externen Datenträgern bei älteren Geräten aus technischen Gründen nicht möglich war.
- dass im Klimaschutzministerium und Landwirtschaftsministerium weder eine USB–Port–Deaktivierung noch eine USB–Port–Kontrolle für die IT–Arbeitsplätze implementiert war.
- dass im Landwirtschaftsministerium Applikations–Whitelisting für die IT–Arbeitsplätze nicht implementiert war.
- dass im Klimaschutzministerium kein umfassendes Endpoint–Protection–System implementiert war.

Er empfahl

- dem Klimaschutzministerium, jene älteren Geräte zu ersetzen, bei denen das Unterbinden des Startens von externen Datenträgern aus technischen Gründen nicht möglich ist.
- dem Klimaschutz– und dem Landwirtschaftsministerium, eine USB–Port–Deaktivierung bzw. eine USB–Port–Kontrolle für die IT–Arbeitsplätze einzusetzen.
- dem Landwirtschaftsministerium, Applikations–Whitelisting für die IT–Arbeitsplätze einzusetzen, um zu gewährleisten, dass ausschließlich vorgesehene Applikationen gestartet werden können.
- dem Klimaschutzministerium, den Einsatz eines umfassenden Endpoint–Protection–Systems als Beitrag zur IT–Sicherheit der IT–Arbeitsplätze zu prüfen und erforderlichenfalls ein solches System einzusetzen.

Der RH hielt anerkennend fest, dass im Finanzministerium bei dezentraler Inbetriebnahme des mobilen IT–Arbeitsplatzes (und Aufbau einer Netzwerkverbindung) automatisch eine gesicherte VPN–Verbindung mit den zentralen Systemen aufgebaut wurde (Auto–VPN–Funktionalität); damit war sichergestellt, dass die Sicherheitsmaßnahmen der zentralen Systeme z.B. für den Zugang zum Internet auch außerhalb der Dienststelle wirksam waren.

17.3 Das Landwirtschaftsministerium teilte in seiner Stellungnahme mit, dass es die Empfehlung des RH prüfen und auch weiterhin den Fokus auf die Verbesserung der IT–Sicherheit richten werde.

Zwei–Faktor–Authentifizierung und Benutzerverwaltung

18.1 (1) Durch die Benutzerverwaltung und Zugriffskontrolle sollte sichergestellt werden, dass ausschließlich befugte Personen Zugang zu den entsprechenden Daten, IT–Systemen und IT–Diensten erhielten. Hierzu arbeiteten die drei überprüften Bundesministerien Berechtigungskonzepte aus und führten auch Überprüfungen der Benutzerkonten durch.

(2) Bei der Zwei–Faktor–Authentifizierung[68] erfolgt der Identitätsnachweis eines Bediensteten mittels einer Kombination aus zwei unterschiedlichen und insbesondere unabhängigen Komponenten (Faktoren wie z.B. Wissen bzw. Passwort; Besitz; biometrische Eigenschaften). Dadurch kann das Risiko einer unbefugten Verwendung wesentlich reduziert werden.

(3) Die Bediensteten des Finanzministeriums authentifizierten sich am IT–Arbeitsplatz mit der chipbasierten Dienstkarte sowie dem Benutzernamen und dem benutzerspezifischen Passwort; das entsprach einer Zwei–Faktor–Authentifizierung. Diese technische Lösung war nicht auf die Nutzung des Endgeräts beschränkt, das der Person zugeteilt war.

(4) Die Bediensteten des Klimaschutzministeriums authentifizierten sich am IT–Arbeitsplatz mit Benutzername und Passwort. Darüber hinaus war eine Pre–Boot–PIN–Eingabe[69] implementiert: Vor einem Startvorgang[70] musste eine für den spezifischen IT–Arbeitsplatz der oder des Bediensteten spezifische PIN eingegeben werden.[71]

(5) Die Bediensteten des Landwirtschaftsministeriums authentifizierten sich am IT–Arbeitsplatz grundsätzlich mit Benutzername und Passwort. Darüber hinaus war eine Pre–Boot–Authentisierung implementiert: Vor einem Startvorgang[72] musste ein gerätespezifisches nicht veränderbares Passwort eingegeben werden. Während der Gebarungsüberprüfung lief im Landwirtschaftsministerium ein Pilotbetrieb zur Zwei–Faktor–Authentifizierung.

[68] Authentisierung ist das Nachweisen einer Identität (z.B. durch Eingabe eines Passwortes), die Überprüfung dieses Identitätsnachweises auf seine Authentizität nennt man Authentifizierung. Nach einer erfolgreichen Authentifizierung werden entsprechende Rechte, Ressourcen etc. im Rahmen der Autorisierung vergeben.

[69] **PIN** = Personal Identification Number

[70] Nach dem „Ruhezustand“ musste die PIN eingegeben werden.

[71] Diese durfte individualisiert werden.

[72] Nach dem „Ruhezustand“ musste kein Pre–Boot–Passwort eingegeben werden.

18.2 Der RH anerkannte, dass das Klimaschutz– und das Landwirtschaftsministerium das Risiko einer missbräuchlichen Verwendung von Identitäten wesentlich reduzieren konnten, indem neben der Authentifizierung mittels Benutzername und Passwort zusätzlich die Pre–Boot–Authentisierung zum Einsatz kam. Allerdings entsprachen diese Sicherheitsvorkehrungen nach Ansicht des RH noch nicht einer Zwei–Faktor–Authentifizierung. Der RH wies die beiden Ressorts auf das Risiko hin, dass Bedienstete auf ihrem IT–Arbeitsplatz mit der Zugangskennung (Benutzername und Passwort) einer anderen Person einen unerlaubten Zugriff auf deren Daten erhalten.

Der RH empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, ihre jeweiligen Authentifizierungsmethoden einer Risikoanalyse zu unterziehen, den Bedarf nach einer Zwei–Faktor–Authentifizierung zu prüfen und diese allenfalls einzusetzen.

18.3 Das Landwirtschaftsministerium teilte in seiner Stellungnahme mit, dass es die Empfehlung berücksichtigen und nach Möglichkeit eine Zwei–Faktor–Authentifizierung umsetzen werde.

Nutzung von Videokonferenzen bei der Telearbeit

19.1 (1) Aufgrund des in der COVID–19–Pandemie angeordneten Home–Office war es ab März 2020 für die Bundesministerien wichtig, rasch Videokonferenzsoftware zu beschaffen, um die interne Zusammenarbeit zu unterstützen. In den drei überprüften Bundesministerien waren im April 2023 insgesamt fünf unterschiedliche Videokonferenzsysteme im Einsatz:

Tabelle 11: Eingesetzte Videokonferenzsysteme (Stand April 2023)

Produkt	Finanz-ministerium	Klimaschutz-ministerium	Landwirtschafts-ministerium
A	X	X	X
B		X	
C		X	X
D		X	
E – Teststellung für ein einheitliches Videokonferenzsystem	X	X	X

Quellen: BMF; BMK; BML

(2) In seinem Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31) hatte der RH festgestellt, dass unterschiedliche Videokonferenzsysteme innerhalb eines Ressorts, aber auch zwischen den Ressorts die Durchführung von Videokonferenzen erschwerten. Er hatte daher

empfohlen, ressortintern eine einheitliche Software–Lösung für Videokonferenzen vorzusehen und darüber hinaus einen gemeinsamen Videokonferenz–Standard für den Bund zu erstellen. Dieser sollte die Kommunikation in der Bundesverwaltung sicherstellen und IT–Sicherheitsaspekte besonders berücksichtigen.

Das mit 1. Jänner 2021 im Rahmen des IT–Konsolidierungsprogramms gestartete Projekt „Videokonferenzsystem Bund" stand unter der Projektleitung bzw. in der Zuständigkeit des Bundeskanzleramts und des Digitalisierungsministeriums. Ziel war es, bis Ende 2021 eine einheitliche Videokonferenzlösung für den Bund bereitzustellen.

Im Juni 2023 war das Projekt nicht abgeschlossen. Nach Auskunft des (seit der BMG–Novelle 2022) zuständigen Finanzministeriums sei ein Testbetrieb, an dem alle Bundesministerien sowie die Parlamentsdirektion und die Präsidentschaftskanzlei teilnahmen, zwischen November 2021 und Februar 2022 durchgeführt worden; einzelne Ressorts hätten zum Teil detaillierte Rückmeldungen gegeben. Laut Planung sollte das Videokonferenzsystem Bund im Sommer 2023 in Betrieb gehen. In der finalen Phase der Überführung vom eingeschränkten in den Produktionsbetrieb trat ein technisches Problem auf, an dessen Behebung im Juni 2023 gearbeitet wurde.

19.2 Der RH wies kritisch darauf hin, dass mit Stand April 2023 in den drei überprüften Bundesministerien fünf unterschiedliche Videokonferenzsysteme im Einsatz waren, wobei das Klimaschutz– und das Landwirtschaftsministerium jeweils mehr als ein Videokonferenzsystem in Verwendung hatten.

Er empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, die Anzahl der eingesetzten Videokonferenzsysteme auf das erforderliche Maß zu verringern.

Der RH bewertete die Bestrebungen des Bundes zum Einsatz eines einheitlichen Videokonferenzsystems mit dem im Jänner 2021 gestarteten Projekt „Videokonferenzsystem Bund" als zweckmäßig. Er stellte allerdings kritisch fest, dass das Projekt im Juni 2023 noch nicht abgeschlossen war; somit hatte sich der für Ende 2021 geplante Abschluss bereits um eineinhalb Jahre verzögert.

Der RH empfahl dem seit Mai 2024 für die IT–Koordination zuständigen Bundeskanzleramt, das bundeseinheitliche Videokonferenzsystem bis zur Fertigstellung im erweiterten Testbetrieb mit anderen Bundesministerien zu erproben.

19.3 (1) Das zum Stellungnahmezeitpunkt (Februar 2024) zuständige Finanzministerium hielt in seiner Stellungnahme fest, dass das im Rahmen des Programms IT–Konsolidierung entwickelte Videokonferenzsystem des Bundes (VIKO) bis zu seiner Fertigstellung im Bundeskanzleramt und im Finanzministerium pilotiert worden sei. Mit

31. Oktober 2023 sei das Projekt abgeschlossen und in den Regelbetrieb in der BRZ GmbH übergeben worden; Rollouts in anderen Bundesministerien seien geplant.

(2) Das Landwirtschaftsministerium teilte in seiner Stellungnahme mit, die Bestrebungen, ein einheitliches Videokonferenzsystem im Bund zu etablieren, zu unterstützen.

Regelungen für Bedienstete zur Gewährleistung der IT–Sicherheit bei Telearbeit

20.1 (1) In den Richtlinien zur Informations– und Datensicherheit wiesen die drei überprüften Bundesministerien darauf hin, dass die Nutzung der dienstlichen IKT–Infrastruktur außerhalb von Diensträumen (z.B. bei Telearbeit) erhöhte Aufmerksamkeit hinsichtlich der Einhaltung datenschutzrechtlicher Vorschriften und gesetzlicher Geheimhaltungs– und Verschwiegenheitspflichten erforderte. Die Richtlinien enthielten u.a. konkrete Regelungen für Zutritts– und Zugriffsbeschränkungen, zur Clear Desk Policy[73], zur sicheren Datenspeicherung, zur Verwahrung dienstlicher Unterlagen sowie zur Sicherung der Arbeitsgeräte am Transportweg.

In ihren Telearbeitsrichtlinien verwiesen die drei Bundesministerien zunächst auf ihre Richtlinien zur Informations– und Datensicherheit. Weiters legten sie fest, dass der Dienstgeber den für Telearbeit erforderlichen mobilen dienstlichen IT–Arbeitsplatz zur Verfügung stellte und dass der Zugriff auf zentrale IT–Anwendungen auch am Telearbeitsplatz bereitstand.[74]

Die drei überprüften Bundesministerien brachten ihre Richtlinien den Bediensteten mit Schreiben zur Kenntnis; zusätzlich wurden die Richtlinien wie auch allfällige Änderungen im Intranet des Bundesministeriums bzw. im Finanzministerium in der ressorteigenen Finanzdokumentation veröffentlicht.

(2) Die im Mai 2023 gültigen Telearbeitsanordnungen bzw. –vereinbarungen der drei Bundesministerien verwiesen jeweils auf die Telearbeitsrichtlinie bzw. auf die sinngemäße Geltung von Rechtsvorschriften, Erlässen und Weisungen. Telearbeitsanordnungen bzw. –vereinbarungen waren im Finanz– und im Landwirtschaftsministerium nur bei regelmäßiger Telearbeit abzuschließen, so dass in diesen beiden Bundesministerien bei anlassbezogener Telearbeit ein solcher Hinweis entfiel.

[73] Vermeidung der Einsehbarkeit von Dokumenten, insbesondere klassifizierten Informationen, in gedruckter Form auf Schreibtisch, Drucker bzw. Kopiergerät, Vernichtung nicht mehr benötigter Informationen

[74] Das Finanzministerium stellte zusätzlich – für gelegentliche Zugriffe von privaten Geräten aus – eine eingeschränkte dienstliche Umgebung für gleichzeitig maximal 300 Bedienstete zur Verfügung.

Eine Festlegung von konkreten dienstlichen Aufgaben, die aus Sicherheitsgründen an der Dienststelle zu verrichten wären bzw. die für Telearbeit aus Sicherheitsgründen nicht geeignet sind, erfolgte hingegen nicht. Die Telearbeitsrichtlinien enthielten nur die Aussagen, dass die übertragenen Aufgaben für Telearbeit geeignet sein müssen.[75]

20.2 Der RH stellte fest, dass die überprüften Bundesministerien Regelungen zur Informations– und Datensicherheit in allgemeinen Richtlinien zur Informations– und Datensicherheit und in Telearbeitsrichtlinien erlassen hatten. Diese brachten sie den Bediensteten mit Schreiben und zusätzlich auf ressortinternen Informationsplattformen zur Kenntnis.

Allerdings bestand nur bei Abschluss einer Telearbeitsanordnung bzw. –vereinbarung die Möglichkeit eines gesonderten Hinweises auf die Verpflichtung, die Informations– und Datensicherheitsvorschriften einzuhalten. Telearbeitsanordnungen bzw. –vereinbarungen waren im Finanz– und im Landwirtschaftsministerium nur bei regelmäßiger Telearbeit vorgesehen, im Klimaschutzministerium auch für anlassbezogene Telearbeit.

Der RH empfahl daher dem Finanz– und dem Landwirtschaftsministerium, auch Bedienstete ohne Telearbeitsanordnung bzw. –vereinbarung im Falle der anlassbezogenen Telearbeit auf geeignete Weise gesondert darauf hinzuweisen, dass die Datensicherheitsvorschriften und die Vorschriften für die IT–Sicherheit einzuhalten sind.

Der RH stellte weiters fest, dass die überprüften Bundesministerien keine konkreten dienstlichen Aufgaben, die aus Sicherheitsgründen an der Dienststelle zu verrichten wären bzw. die aus Sicherheitsgründen für Telearbeit nicht geeignet sind, festgelegt hatten.

Wie schon in seinem Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 18) empfahl der RH dem Finanz–, dem Klimaschutz– und dem Landwirtschaftsministerium, konkret festzulegen, ob bestimmte dienstliche Aufgaben jedenfalls aus Sicherheitsgründen an der Dienststelle zu verrichten sind.

20.3 (1) Das Finanzministerium führte in seiner Stellungnahme aus, dass es die wesentlichen Informationssicherheits– und Datenschutzerlässe bereits an die geänderten Anforderungen durch die NIS–2–Richtlinie angepasst habe, wodurch u.a. die Schlussempfehlungen 10, 15, 29 und 30 berücksichtigt worden seien. Die aktualisierten Erlässe würden voraussichtlich im Jänner 2024 nach Abschluss der ressortinternen Abstimmungsmaßnahmen in Kraft gesetzt.

[75] Das Klimaschutzministerium konkretisierte dies dahingehend, dass Ortsungebundenheit gegeben und keine persönliche Anwesenheit (insbesondere wegen Parteienverkehr) erforderlich sein dürfe.

Die gesetzlichen Vorschriften würden als Voraussetzung für die Telearbeit u.a. die Verpflichtung des oder der Bediensteten vorsehen, die für die Wahrung der Datensicherheit, Verschwiegenheitspflichten und anderer Geheimhaltungspflichten erforderlichen Vorkehrungen zu treffen. Weiters sehe die Telearbeitsrichtlinie des Finanzministeriums vor, dass anlassbezogene Telearbeit nach Maßgabe u.a. dieser gesetzlichen Bestimmung im Voraus mittels E–Mail, mündlich oder telefonisch vereinbart werden könne. Damit sei auf die Regelungen im Zusammenhang mit der Datensicherheit in Kombination mit den sicherheitstechnischen Voraussetzungen bei Telearbeit in ausreichendem Maß hingewiesen worden.

Bereits ex ante prüfe das Finanzministerium, ob aufgrund der Aufgaben und Tätigkeiten des Arbeitsplatzes die Voraussetzungen für Telearbeit vorlägen, andernfalls sei Telearbeit nicht möglich.

(2) Das Landwirtschaftsministerium teilte in seiner Stellungnahme mit, eine Klarstellung hinsichtlich Geltung und Einhaltungspflicht der Datensicherheitsvorschriften und der Vorschriften für die IT–Sicherheit auch im Rahmen der anlassbezogenen Telearbeit zu prüfen.

Hinsichtlich der Eignung konkreter dienstlicher Aufgaben zur Verrichtung in Telearbeit verwies es auf seine Telearbeitsrichtlinie, wonach diese Festlegung im Zuständigkeitsbereich der oder des Vorgesetzten liege. Weiters seien gemäß Telearbeitsrichtlinie Regelungen über die Zulässigkeit der Mitnahme bzw. des Transports von Arbeitsunterlagen zum Telearbeitsplatz individuell zwischen den Vorgesetzten und den Bediensteten festzulegen. Unterlagen mit klassifizierten Informationen gemäß Informationssicherheitsgesetz dürften nicht an den Telearbeitsplatz transportiert werden. Bei Vorliegen einer für alle Bediensteten des Ressorts geltenden Festlegung würden mit der Personalvertretung Verhandlungen zur Adaptierung der Telearbeitsrichtlinie geführt.

20.4 (1) Der RH entgegnete dem Finanzministerium, dass er einen allgemeinen Hinweis auf die gesetzliche Regelung und auf allfällige weitere Datensicherheits– und IT–Sicherheitsvorschriften in den Telearbeitsrichtlinien für nicht ausreichend hielt. Daher sollte ein konkreter Hinweis auf die Verpflichtung zur Einhaltung dieser Vorschriften in Einzelanordnungen bzw. –vereinbarungen über die Telearbeit aufgenommen werden. In der Regel wurden – wie auch im Finanzministerium – solche Anordnungen bzw. Vereinbarungen aber dann nicht getroffen, wenn Bedienstete keine regelmäßige, aber ausnahmsweise anlassbezogene Telearbeit verrichteten. In diesen Fällen sollte ein gesonderter Hinweis auf die Einhaltung der genannten Vorschriften erfolgen.

(2) Zur Stellungnahme des Finanzministeriums und des Landwirtschaftsministeriums betreffend die Beurteilung der Eignung des konkreten Arbeitsplatzes für Tele-

arbeit wiederholte der RH seine Empfehlung, aus Sicherheitsgründen für Telearbeit nicht geeignete konkrete Aufgaben zu identifizieren und festzulegen.

IT–Sicherheit Personal

Regelungen

21.1 (1) Der RH überprüfte das Management der personellen IT–Sicherheit der Bundesministerien in den Bereichen

- wesentliche Regelungen,
- Maßnahmen vor, während und nach Beendigung des Dienstverhältnisses (TZ 22) sowie
- Maßnahmen für Personal von externen IT–Dienstleistern (TZ 23).

Die Überprüfung orientierte sich an den Vorgaben des Informationssicherheitshandbuchs.

(2) Die folgende Tabelle fasst das vorhandene Regelwerk zur personellen IT–Sicherheit in den drei überprüften Bundesministerien zusammen:

Tabelle 12: Wesentliche Regelungen zur personellen IT–Sicherheit

wesentliche Regelungen	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
Dienstrecht, gesetzliche Regelungen	Amtsverschwiegenheit, Einhaltung einschlägiger Gesetze (z.B. Datenschutz)	Amtsverschwiegenheit, Einhaltung einschlägiger Gesetze (z.B. Datenschutz)	Amtsverschwiegenheit, Einhaltung einschlägiger Gesetze (z.B. Datenschutz)
Richtlinie zur Nutzung der IKT	vorhanden	vorhanden	vorhanden
Passwort–Richtlinie	vorhanden	vorhanden	vorhanden
Richtlinie zu mobilen Endgeräten	vorhanden	vorhanden	vorhanden
Erläuterungen zum Datenschutz	vorhanden	vorhanden	vorhanden
Regelungen zur Telearbeit	vorhanden	vorhanden	vorhanden
Regelungen zur elektronischen Kommunikation	vorhanden	vorhanden	vorhanden
Regelungen zur Privatnutzung	Informationssicherheit und Datenschutz im Arbeitsalltag, Nutzungsbedingungen für dienstliche Smartphones und Tablets	IKT–Arbeitsplatzrichtlinie, Datensicherheitsvorschrift	Benutzerrichtlinie
Umgang mit klassifizierten Informationen	Informationssicherheits-gesetz und –verordnung, Informationssicherheit und Datenschutz im Arbeitsalltag	Informationssicherheits-gesetz und –verordnung, Datensicherheitsvorschrift, Merkblatt Informations-sicherheit	Informationssicherheits-gesetz und –verordnung, individuelle Unterweisungen betroffener Mitarbeiterinnen und Mitarbeiter durch Informationssicherheitsbeauftragte bzw. –beautragten

IKT = Informations– und Kommunikationstechnologie

Quellen: BMF; BMK; BML

Die überprüften Bundesministerien legten die wesentlichen Regelungen in ihren Richtlinien und Vorgaben fest. Im Einzelnen war festzuhalten:

- Für das Klimaschutzministerium waren Regelungen in den „Grundsätzen zur IT–Sicherheitspolitik“ aus 2002 in Kraft (TZ 10).
- Das Landwirtschaftsministerium machte keine Vorgaben zum Umgang mit klassifizierten Informationen[76] in seinen Richtlinien und Regelungen zur IT–Sicherheit, sondern verwies auf einschlägige gesetzliche Vorschriften und Verordnungen. Es unterwies jene Bediensteten im Umgang mit klassifizierten Informationen, die damit konkret befasst waren.

21.2 Der RH hielt wiederholt kritisch fest, dass im Klimaschutzministerium das maßgebliche Dokument „Grundsätze zur IT–Sicherheitspolitik“ aus dem Jahr 2002 stammte, und verwies auf die zugehörige Empfehlung in TZ 10.

[76] Informationen, die einer besonderen Geheimhaltung unterliegen (die vier Stufen der Klassifizierung sind: eingeschränkt, vertraulich, geheim, streng geheim)

Der RH kritisierte, dass das Landwirtschaftsministerium den Umgang mit klassifizierten Informationen in seinen Dokumenten bzw. Vorgaben zur IT–Sicherheit nicht regelte, sondern lediglich auf geltende gesetzliche Regelungen verwies. Bedienstete wurden über den Umgang mit klassifizierten Informationen nur unterwiesen, wenn sie mit diesen befasst waren. Das Informationssicherheitshandbuch erachtet jedoch den Umgang mit klassifizierten Informationen als wesentlich. Daher sollte dieser auch in den Regelungen und Vorgaben zur IT–Sicherheit explizit behandelt werden.

Der RH empfahl dem Landwirtschaftsministerium, Regelungen über den Umgang mit klassifizierten Informationen in den Vorgaben zur IT–Sicherheit – der Datensicherheitsvorschrift – zu ergänzen.

21.3 Das Landwirtschaftsministerium führte in seiner Stellungnahme aus, dass es die Möglichkeit prüfe, Informationen zum Umgang mit klassifizierten Informationen in die allgemeinen Vorgaben zur IT–Sicherheit (Datensicherheitsvorschrift) zu integrieren.

Maßnahmen vor, während und nach Dienstverhältnissen

22.1 Nachfolgende Tabellen geben die Maßnahmen der überprüften Bundesministerien zur personellen IT–Sicherheit vor Beginn des Dienstverhältnisses, während des Dienstverhältnisses und nach Beendigung des Dienstverhältnisses wieder:

Tabelle 13: Maßnahmen zur personellen IT–Sicherheit vor Beginn des Dienstverhältnisses

Maßnahmen vor Beginn des Dienstverhältnisses	Finanzministerium	Klimaschutzministerium	Landwirtschafts-ministerium
Überprüfung der Qualifikation der Bediensteten im Aufnahmeverfahren	vorgesehen	vorgesehen	vorgesehen
Arbeitsplatzbeschreibungen mit IT–sicherheitsrelevanten Aufgaben[1] (z.B. Mitglieder des IT–Sicherheits-management–Teams)	Anforderungen, Aufgaben und Qualifikation ausgewiesen	Anforderungen, Aufgaben und Qualifikation ausgewiesen	Anforderungen, Aufgaben und Qualifikation ausgewiesen
Überprüfung der Vertrauenswürdigkeit (z.B. Strafregisterauszug, Sicherheitsüberprüfung nach Informationssicherheitsgesetz)	vorgesehen	vorgesehen	vorgesehen
Verpflichtungserklärung hinsichtlich Geheimhaltung	vorgesehen	vorgesehen	vorgesehen
Verpflichtungserklärung hinsichtlich IKT–Nutzung	vorgesehen	vorgesehen	vorgesehen

IKT = Informations– und Kommunikationstechnologie Quellen: BMF; BMK; BML

[1] Diese Feststellung bezieht sich auf einzelne vom RH ausgewählte und überprüfte Arbeitsplatzbeschreibungen.

Tabelle 14: Maßnahmen zur personellen IT–Sicherheit während des aufrechten Dienstverhältnisses

Maßnahmen während des Dienstverhältnisses	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
laufende Awareness–Schulungen	regelmäßiges Angebot online (verpflichtende Teilnahme)	regelmäßiges Angebot[1] online (verpflichtende Teilnahme)	regelmäßiges Angebot[2] (freiwillige Teilnahme)
Weiterbildung IT–Personal	nach Bedarf[3]	nach Bedarf	nach Bedarf
Informationen zu Support, Anforderungs– und Meldewegen	Intranet	Intranet, ELAK	Intranet, IKT–Helpdesk, Organisationshandbuch
Informationen zu aktuellen Nutzungsregelungen	vorgesehen	vorgesehen	vorgesehen
Vertretungsregelungen IT–Personal	in Geschäfts– und Personaleinteilung, Intranet	in Geschäfts– und Personaleinteilung bzw. Geschäftsordnung, in Arbeitsplatzbeschreibungen, in IKT–Organisationshandbuch	in Geschäfts– und Personaleinteilung, in Arbeitsplatzbeschreibungen
Informationen über Sicherheitsvorfälle	im Anlassfall über Intranet, E–Mail	im Anlassfall über E–Mail	im Anlassfall über Intranet, E–Mail

ELAK = elektronischer Akt
IKT = Informations– und Kommunikationstechnologie

Quellen: BMF; BMK; BML

[1] Das Angebot umfasste die Bereiche Datenschutz und Umgang mit klassifizierten Informationen.
[2] Das Angebot umfasste die Bereiche Datenschutz und IT–Sicherheitsinformationen für alle Bediensteten.
[3] Für das Informationssicherheitsmanagement–Team des Finanzministeriums sind Personenzertifizierungen und deren Aufrechterhaltung vorgesehen (Zertifizierter Informationssicherheits–Manager; Zertifizierter Informationssicherheits–Auditor).

- Im Finanzministerium (ohne nachgeordnete Dienststellen) hatten, nach der Eingliederung von zwei neuen Sektionen[77], mit Stand 1. April 2023 rd. 60 % der Bediensteten die Awareness–Schulungen für IT–Sicherheit absolviert.
- Das Klimaschutzministerium hatte das Thema „IT–Sicherheit im Arbeitsalltag“ noch nicht in die laufenden Awareness–Schulungen integriert.
- Im Landwirtschaftsministerium waren Bedienstete nicht verpflichtet, die angebotenen Awareness–Schulungen für IT–Sicherheit zu absolvieren.

Tabelle 15: Maßnahmen zur personellen IT–Sicherheit nach Ende des Dienstverhältnisses

Maßnahmen nach Ende des Dienstverhältnisses	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
Personalprozess	definiert	definiert	definiert
Prozessablauf	automatisiert	automatisiert	automatisiert
Sicherstellung von Daten und Ausstattung	vorgesehen	vorgesehen	vorgesehen
Entzug von Zugangs– und Zugriffsberechtigungen	vorgesehen	vorgesehen	vorgesehen

Quellen: BMF; BMK; BML

[77] Im Finanzministerium waren durch Umgliederung der Bundesministerien aufgrund der BMG–Novelle 2022 zwei zusätzliche Sektionen zu integrieren (TZ 4).

22.2 Der RH wies kritisch darauf hin, dass im Finanzministerium (ohne nachgeordnete Dienststellen) nach Eingliederung der zwei neuen Sektionen mit Stand 1. April 2023 erst rd. 60 % der Bediensteten die Awareness–Schulungen für IT–Sicherheit absolviert hatten.

Er empfahl dem Finanzministerium, den Absolvierungsgrad der Awareness–Schulungen für IT–Sicherheit durch geeignete Maßnahmen zu erhöhen.

Der RH stellte fest, dass das Klimaschutzministerium das Thema IT–Sicherheit im Arbeitsalltag noch nicht in die Awareness–Schulungen integriert hatte und das Landwirtschaftsministerium die Teilnahme an Awareness–Schulungen zu IT–Sicherheit für die Bediensteten lediglich freiwillig vorsah.

Er empfahl

- dem Klimaschutzministerium, die Awareness–Schulungen um das Thema „IT–Sicherheit im Arbeitsalltag“ zu ergänzen.
- dem Landwirtschaftsministerium, Awareness–Schulungen zu IT–Sicherheit regelmäßig und für die Bediensteten verpflichtend durchzuführen.

22.3 (1) Das Finanzministerium wies in seiner Stellungnahme darauf hin, dass insbesondere Awareness– und Schulungsmaßnahmen aufgrund der hohen Anzahl von Bediensteten und allfälliger Reorganisationen, Karenzierungen oder Dauerkrankenständen fortlaufende Prozesse darstellten, die in ihrer Umsetzung eine angemessene Vor– und Durchlaufzeit erforderten.

Der Absolvierungsgrad der verpflichtenden Awareness–Schulung „Informationssicherheit und Datenschutz im Arbeitsalltag“ in der Zentralstelle habe von 60 % (Stichtag 1. April 2023) auf 72 % (Stichtag 1. Oktober 2023) angehoben werden können. Der Absolvierungsgrad für das gesamte Finanzressort sei bereits zum Stichtag 1. April 2023 bei 89 % gelegen und habe bis 1. Oktober 2023 auf 90 % erhöht werden können.

Eine Aktualisierung der verpflichtenden elektronischen Lernprogramme sei vorgesehen, die durch Kommunikations– und Monitoringmaßnahmen begleitet werde.

(2) Das Landwirtschaftsministerium hielt in seiner Stellungnahme fest, dass die Einführung der verpflichtenden Teilnahme an Awareness–Schulungen geprüft werde.

Externes Personal

23.1 (1) Das Finanz–, das Klimaschutz– und das Landwirtschaftsministerium setzten externes Personal von IT–Dienstleistern in unterschiedlichem Ausmaß ein:

Tabelle 16: Maßnahmen zur personellen IT–Sicherheit bei Einsatz von externem Personal

Maßnahmen externes Personal	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
IT–Sicherheitsanforderungen Vertragsbestandteil	ja	ja	ja
Qualifikationen des externen Personals	vertraglich festgelegt	vertraglich festgelegt	vertraglich festgelegt; Feststellung auch individuell durch Bewerbungsgespräche
Geheimhaltungspflichten	BRZ–GmbH–Gesetz; vertraglich festgelegt	BRZ–GmbH–Gesetz; vertraglich festgelegt	BRZ–GmbH–Gesetz; vertraglich festgelegt
Pflichten hinsichtlich Datenschutz	vertraglich festgelegt	vertraglich festgelegt	vertraglich festgelegt
Überprüfung der Vertrauenswürdigkeit	Sicherheitsüberprüfung nach § 55 Sicherheitspolizeigesetz	Sicherheitsüberprüfung nach § 55 Sicherheitspolizeigesetz	Sicherheitsüberprüfung nach § 55 Sicherheitspolizeigesetz
Einhaltung der IT–Sicherheitsvorgaben des Ressorts	Überbindung der wesentlichen Regelungen	Überbindung der wesentlichen Regelungen	Überbindung der wesentlichen Regelungen
Informationssicherheits–managementsystem beim Auftragnehmer	ja	ja	ja

BRZ–GmbH–Gesetz = Bundesgesetz über die Bundesrechenzentrum GmbH

Quellen: BMF; BMK; BML

(2) Das Finanzministerium setzte externes Personal der BRZ GmbH für den Betrieb und Support vor Ort ein. Um die personelle IT–Sicherheit sicherzustellen, galten vertragliche Regelungen zu Anforderungen, Qualifikation, Geheimhaltung und Datenschutz. Darüber hinaus legte das Bundesgesetz über die Bundesrechenzentrum GmbH[78] für Mitarbeiterinnen und Mitarbeiter der BRZ GmbH Verschwiegenheitspflichten[79] fest und verfügte die BRZ GmbH über ein nach ISO–Norm 27001[80] zertifiziertes eigenes Informationssicherheitsmanagementsystem.

(3) Das Klimaschutzministerium bezog IT–Dienstleistungen vor Ort von einem externen IT–Dienstleister. Um die personelle IT–Sicherheit sicherzustellen, galten auch hier neben gesetzlichen Vorgaben vertragliche Regelungen zu Anforderungen, Qualifikation, Geheimhaltung und Datenschutz. Neben der Überprüfung der Vertrauens-

[78] § 17, BGBl. 757/1996 i.d.g.F.

[79] mit Verweis auf Regelungen im Beamten–Dienstrechtsgesetz 1979 sowie auf die Geheimhaltungspflicht in der Bundesabgabenordnung

[80] Die Norm ISO 27001 spezifizierte die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems.

würdigkeit nach dem Sicherheitspolizeigesetz[81] musste externes Personal eine Verpflichtungserklärung zur Einhaltung der IT–Sicherheit im Klimaschutzministerium – samt Kenntnisnahme des diesbezüglichen Regelwerks – unterzeichnen. Es wurde auch in den Informationsfluss[82] zur IT–Sicherheit des Ministeriums eingebunden.

Das Klimaschutzministerium setzte zur Betreuung von Server–Systemen Fremdpersonal eines IT–Dienstleisters ein. Das Fremdpersonal war mit permanenten privilegierten Zugriffsrechten für operative Tätigkeiten – wie Monitoring, Aktualisierungen der Systeme oder sonstige Support–Arbeiten – ausgestattet. Diese Zugriffsrechte beinhalteten auch Administrationsrechte über einen Fernwartungszugriff.

(4) Das Landwirtschaftsministerium setzte zwei IT–Dienstleister für den Vor–Ort–Support ein. Diese Dienstleistungen wurden über Abrufe aus Rahmenverträgen der Bundesbeschaffung GmbH bezogen. Der Inhalt der vertraglichen Vereinbarungen umfasste die Verpflichtung zur Verschwiegenheit und zum Datenschutz. Darüber hinaus kamen zusätzliche individuelle Maßnahmen zum Einsatz, um die Qualifikation des Personals, die Geheimhaltung durch diese und ihre Vertrauenswürdigkeit sicherzustellen.

23.2 Der RH stellte fest, dass das Klimaschutzministerium im Bereich der Server–Betreuung externes Personal mit permanenten Fernwartungszugriffen ausstattete. Er merkte kritisch an, dass ein permanenter Fernwartungszugriff mit privilegierten Rechten Risiken für die Organisation und das Netzwerk barg.

Der RH empfahl daher dem Klimaschutzministerium, Fernwartungszugriffe auf zentrale Systeme nur anlassbezogen und nur zeitlich begrenzt zu gewähren. Daher wäre zu überprüfen, ob die permanenten privilegierten Zugriffe auf Server–Systeme (im Bereich Server–Betreuung), die auch Fernwartung beinhalten, erforderlich sind.

[81] BGBl. 566/1991 i.d.g.F.

[82] E–Mail, ELAK, Intranet, Awareness–Schulungen

IT–Sicherheit der IT–Infrastruktur

Technische Maßnahmen zur Erhöhung der IT–Sicherheit

24.1 (1) Ziel von technischen und organisatorischen Maßnahmen ist es, die IT–Sicherheit der zentralen IT–Komponenten bzw. der IT–Anwendungen zu erhöhen. Dabei sollten Maßnahmen eingesetzt werden, die unter Berücksichtigung von Kosten–Nutzen–Erwägungen die Erreichung eines hohen Sicherheitsniveaus erwarten lassen.

Im Einzelnen waren beispielhaft folgende technische Maßnahmen geeignet, die IT–Sicherheitsrisiken für die zentrale IT–Infrastruktur zu reduzieren:

- ein (netzwerkbasiertes) Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS) zur Erkennung und Verhinderung von Angriffen,
- Firewalls, um unerwünschte Netzwerkverbindungen vom Internet in das lokale Netz des Bundesministeriums und umgekehrt zu unterbinden,
- Spamfilter zur Unterdrückung unerwünschter E–Mails,
- Schutz vor Schadsoftware (Viren, Trojaner, Ransomware, Spyware etc.) für die zentralen Systeme – z.B. Serversysteme,
- DDoS[83]–Schutz gegen gebündelte Angriffe auf den Server, deren Ziel es ist, diesen mithilfe einer Vielzahl von Anfragen zu blockieren oder funktionsunfähig zu machen; ein DDoS–Schutz erfordert im Allgemeinen Unterstützung durch den Internetdienstanbieter durch Blockieren von IP–Adressen,
- ein Security Information and Event Management (SIEM) zur strukturierten Analyse der verfügbaren Daten, um Angriffe bzw. ungewöhnliches Verhalten im Netz zu erkennen und gegebenenfalls Gegenmaßnahmen ergreifen zu können; diese Systeme klassifizieren und protokollieren teilweise automatisiert sicherheitskritische Vorfälle,
- ein Security Operation Center (SOC), das in der Regel auf Grundlage der Ergebnisse des Security Information and Event Management (SIEM) laufend alle sicherheitsrelevanten Systeme (Netzwerke, Server, Clients, Webservices etc.) überwacht und analysiert.

[83] **DDoS** = Distributed–Denial–of–Service

Tabelle 17: Maßnahmen zur Erhöhung der IT–Sicherheit der zentralen IT–Infrastruktur

Maßnahmen	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
IDS bzw. IPS (Intrusion Detection System bzw. Intrusion Prevention System)	eingerichtet	nicht eingerichtet (im Aufbau: Integration 2023 geplant)	eingerichtet
Firewall	eingerichtet	eingerichtet	eingerichtet
Spamfilter	eingerichtet	eingerichtet	eingerichtet
Schutz vor Schadsoftware	eingerichtet	eingerichtet	eingerichtet
DDoS–Schutz (Schutz vor Distributed–Denial–of Service–Angriffen)	eingerichtet	eingerichtet	eingerichtet
SIEM (Security Information and Event Management)	eingerichtet	nicht eingerichtet	eingerichtet (ohne Einbindung der Arbeitsplatzrechner)
SOC (Security Operation Center)	in Vorbereitung[1]	nicht eingerichtet	nicht eingerichtet

[1] Die Aufgaben und Tätigkeiten des Security Operation Centers (SOC) wurden ersatzweise durch das Computer Emergency Response Team (Computer–Notfallteam) der BRZ GmbH wahrgenommen; der Einsatz eines eigenen SOC in der BRZ GmbH war in Vorbereitung.

Quellen: BMF; BMK; BML

(2) Das Finanzministerium hatte umfangreiche Maßnahmen zur Verbesserung der IT–Sicherheit bei den zentralen IT–Systemen implementiert. Der Einsatz eines eigenen Security Operation Centers (SOC) durch die BRZ GmbH als zentralen IT–Dienstleister befand sich im Juni 2023 in Vorbereitung. Im überprüften Zeitraum nahm diese Aufgaben noch das Computer–Notfallteam der BRZ GmbH wahr. Weiters erarbeitete das Finanzministerium einen regelmäßig aktualisierten Sicherheitstechnologiekatalog, der geeignete Technologien und Protokolle festlegte.

(3) Das Klimaschutzministerium hatte zahlreiche Maßnahmen zur IT–Sicherheit implementiert; ein System zur Erkennung bzw. Verhinderung von Angriffen – Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS) – befand sich erst im Aufbau. Die wichtigen aus dem Internet erreichbaren Dienste, etwa Websites, wurden von externen Dienstleistern, z.B. der BRZ GmbH, betrieben, die über einen DDoS–Schutz verfügten. Das Klimaschutzministerium hatte weder ein Security Information and Event Management (SIEM) noch ein Security Operation Center (SOC) eingerichtet. Für zwei sicherheitskritische Anwendungen war die Unterstützung durch ein externes SOC in Planung.

(4) Auch das Landwirtschaftsministerium hatte zahlreiche Maßnahmen zur IT–Sicherheit der zentralen IT–Systeme implementiert, ein Security Operation Center (SOC) war allerdings nicht eingerichtet. Der Internetprovider des Landwirtschaftsministeriums verfügte über einen DDoS–Schutz.

24.2 Das Finanzministerium, das Klimaschutzministerium und das Landwirtschaftsministerium hatten in unterschiedlichem Ausmaß wichtige technische Maßnahmen zur IT–Sicherheit der zentralen IT–Systeme umgesetzt.

Der RH hielt allerdings kritisch fest,

- dass im Klimaschutzministerium das System zur Erkennung bzw. Abwehr von Angriffen (IDS/IPS) erst im Aufbau und kein Security Information and Event Management (SIEM) eingerichtet war.
- dass im Klimaschutz– und im Landwirtschaftsministerium kein Security Operation Center (SOC) eingerichtet war.

Er empfahl dem Klimaschutzministerium,

- ein System zur Erkennung bzw. Abwehr von Angriffen zu implementieren (Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS)).
- zu prüfen, ob ein Security Information and Event Management (SIEM) einen effektiven Beitrag zur Verbesserung der IT–Sicherheit mit sich bringen würde, und erforderlichenfalls ein solches einzuführen.

Dem Klimaschutz– und dem Landwirtschaftsministerium empfahl der RH, zu prüfen, ob ein Security Operation Center (SOC) einen effektiven Beitrag zur Verbesserung der IT–Sicherheit mit sich bringen würde, und erforderlichenfalls ein solches einzuführen.

24.3 Das Landwirtschaftsministerium hielt in seiner Stellungnahme fest, dass es die Umsetzung dieser Empfehlung evaluieren werde.

IT–Sicherheitsüberprüfungen

25.1 (1) Ziel von IT–Sicherheitsüberprüfungen (IT–Sicherheits–Audits) war es, die Wirksamkeit der getroffenen technischen und organisatorischen IT–Sicherheitsmaßnahmen zu überprüfen. Diese Überprüfungen sollten auf einer umfangreichen Risikoanalyse beruhen und konnten – bei vorhandener Expertise – durch die jeweilige Organisation selbst oder von externen Spezialistinnen bzw. Spezialisten, zum Teil automatisiert, durchgeführt werden. Einem Best–Practice–Ansatz entsprachen u.a. folgende spezifischen IT–Sicherheitsüberprüfungen:

- Prozess–Audits zur Betrachtung einzelner Prozesse,
- System–Audits zur Betrachtung des IT–Managementsystems,
- Netzwerk–Audits zur Analyse von Netzwerken, IT und Infrastruktur,
- Social–Engineering–Audits zur Überprüfung von Verhaltensregeln von Mitarbeiterinnen und Mitarbeitern,
- Datenschutz–Audits, z.B. zur Überprüfung, ob die Anforderungen der Datenschutz–Grundverordnung erfüllt werden,
- Vulnerability Scannings zur Analyse und Identifizierung von Schwachstellen,

- Penetration Testing zur Überprüfung von Systemen aus der Sicht eines möglichen Angreifers,
- Compliance–Audits zur Überprüfung, ob gesetzliche Vorschriften und Richtlinien im IT–Bereich eingehalten werden,
- technische Audits zur Betrachtung technischer Systeme,
- Produkt–Audits zur Betrachtung eines Produkts anhand der Kundenerwartungen,
- Projekt–Audits zur Betrachtung der Einhaltung der Projektvorgaben.

Die folgende Tabelle zeigt, welche IT–Sicherheitsüberprüfungen die drei Bundesministerien im Zeitraum 2018 bis 2022 durchgeführt hatten:

Tabelle 18: IT–Sicherheitsüberprüfungen 2018 bis 2022

Maßnahmen	Finanz-ministerium	Klimaschutz-ministerium	Landwirtschafts-ministerium
Prozess–Audits	ja	nein	nein
System–Audits	ja	nein	ja
Netzwerk–Audits	ja	nein	ja
Social–Engineering–Audits	nein	nein	nein[2]
Datenschutz–Audits	ja	nein	nein
Vulnerability Scannings	ja[1]	ja	ja
Penetration Testing	ja	ja	ja
Compliance–Audits	ja	nein	nein; in Planung
technische Audits	ja	nein	ja
Produkt–Audits	ja	nein	ja
Projekt–Audits	ja	nein	ja

[1] Vulnerability Scans der Server, die die BRZ GmbH im Auftrag des Finanzministeriums betreibt (monatlich sowie initial bei der Inbetriebnahme)
[2] Social–Engineering–Audits wurden vor dem überprüften Zeitraum 2018 bis 2022 durchgeführt.

Quellen: BMF; BMK; BML

(2) Das Finanzministerium war gemäß ISO 27001 „Informationssicherheit/ Informationssicherheitsmanagement“ sowie ISO 27701 „Datenschutz“ zertifiziert. Im Zeitraum 2018 bis 2022 wurden 255 Sicherheitsüberprüfungen durchgeführt (davon drei interne und 252 externe) sowie zusätzlich monatlich Vulnerability Scannings durch den zentralen IT–Dienstleister BRZ GmbH. Social–Engineering–Audits führte das Finanzministerium nicht durch, weil aus dem operativen Sicherheitsmanagement (TZ 13 und TZ 15) aktuelle Risiken im Zusammenhang mit Social Engineering erfasst wurden.

(3) Das Klimaschutzministerium ließ acht externe und 57 interne IT–Sicherheitsüberprüfungen durchführen.

(4) Das Landwirtschaftsministerium führte zwei externe und fünf interne IT–Sicherheitsüberprüfungen durch. Zusätzlich nahm es intern quartalsweise eine Schutzbedarfs–Analyse (SBA) vor, ein Compliance–Audit war in Vorbereitung.

25.2 Der RH anerkannte, dass das Finanzministerium durch die Zertifizierungen und die zahlreichen IT–Sicherheitsüberprüfungen die IT–Sicherheitsrisiken in einem hohen Ausmaß detektieren, analysieren und durch geeignete Maßnahmen reduzieren konnte.

Der RH kritisierte, dass die vom Landwirtschaftsministerium und Klimaschutzministerium durchgeführten IT–Sicherheitsüberprüfungen nicht alle wesentlichen Bereiche abdeckten. Weiters erfolgten sie überwiegend ohne externe Expertinnen und Experten.

Er empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, zunächst den Bedarf an IT–Sicherheitsüberprüfungen basierend auf einer umfassenden Risikoanalyse zu erheben, sodann die notwendigen IT–Sicherheitsüberprüfungen zu priorisieren und diese Überprüfungen schließlich zeitnah unter Berücksichtigung der verfügbaren Ressourcen sowie bedarfsgerecht unter Einbindung von externem Fachwissen durchzuführen.

25.3 Das Landwirtschaftsministerium stellte in seiner Stellungnahme in Aussicht, auf der Grundlage einer umfassenderen Risikoanalyse die Umsetzung dieser Empfehlungen zu prüfen.

Notfallkonzepte, Notfallszenarien und Notfallorganisation

26.1 (1) Der RH überprüfte das Notfallmanagement des Finanz–, des Klimaschutz– und des Landwirtschaftsministeriums anhand von drei Themenbereichen. Er orientierte sich hierbei an den Inhalten des Informationssicherheitshandbuchs bzw. des Standards zum Notfallmanagement in den IT–Grundschutzkatalogen des deutschen Bundesamtes für Sicherheit in der Informationstechnik.

(2) Die drei überprüften Bundesministerien definierten die für die Gewährleistung der IT–Sicherheit wichtigen IT–Systeme, IT–Dienste und IT–Verfahren. Darauf aufbauend sollte eine Risikobewertung anhand der definierten Notfallszenarien erfolgen (TZ 11). Diese sollte Grundlage für die festzulegenden IT–Notfallprozesse und –Maßnahmen sein.

Die nachfolgende Tabelle gibt einen Überblick, ob die drei Bundesministerien für die eingesetzten IT–Systeme, IT–Dienste und IT–Verfahren ein Notfallhandbuch (Notfallkonzept), Notfallszenarien, Kriterien für den Eintritt eines Notfalls und eine Notfallorganisation festgelegt hatten:

Tabelle 19: Notfallkonzepte, Notfallszenarien, Notfallorganisation

	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
IT–Notfallhandbuch bzw. Notfallkonzepte	vorhanden	vorhanden	nicht vorhanden
IT–Notfallszenarien bzw. IT–Notfallpläne	vorhanden; IT–Notfallpläne waren auf Basis der einzelnen IT–Verfahren definiert	vorhanden (auf Basis wichtiger IT–Systeme)	vorhanden (auf Basis wichtiger IT–Systeme)
Definition der Kriterien für den Eintritt eines IT–Notfalls	vorhanden; IT–Notfallpläne waren auf Basis der einzelnen IT–Verfahren definiert	vorhanden (auf Basis wichtiger IT–Systeme)	vorhanden (auf Basis wichtiger IT–Systeme)
Definition einer IT–Notfallorganisation (Festlegung zuständiger Organisationseinheiten)	vorhanden	vorhanden (auf Basis wichtiger IT–Systeme)	vorhanden (auf Basis wichtiger IT–Systeme)

Quellen: BMF; BMK; BML

Das Finanzministerium setzte ein umfangreiches Notfallmanagement auf Ebene der eingesetzten IT–Verfahren ein.

Im Klimaschutzministerium lag ein umfassendes Konzept zur Notfallplanung und Notfallvorsorge aus dem Jahr 2005 vor.

Im Landwirtschaftsministerium fehlten ein umfassendes Notfallhandbuch bzw. Notfallkonzepte. Es startete im April 2023 ein Projekt, in dem ein umfassendes Notfallmanagementkonzept erarbeitet werden sollte.

26.2 Der RH hielt kritisch fest, dass im Klimaschutzministerium das vorliegende Konzept zur Notfallplanung und Notfallvorsorge aus dem Jahr 2005 stammte. Er merkte dazu an, dass ein umfassendes Konzept zum Notfallmanagement als grundlegendes Dokument für die IT–Sicherheit aktuell sein sollte.

Der RH kritisierte, dass das Landwirtschaftsministerium noch kein umfassendes Notfallmanagementkonzept in Kraft gesetzt hatte. Er hielt aber fest, dass ein Projekt zur Umsetzung eines solchen Konzepts bereits gestartet worden war.

Der RH empfahl dem Klimaschutz– und dem Landwirtschaftsministerium, für definierte IT–Systeme, IT–Dienste und IT–Verfahren ein Notfallmanagementkonzept zu erstellen und umzusetzen.

26.3 Das Landwirtschaftsministerium hielt in seiner Stellungnahme fest, bereits an der Erstellung eines IT–Notfallhandbuchs zu arbeiten.

Kritische Systeme und Notfallprozesse

27.1 Die drei überprüften Bundesministerien definierten kritische bzw. wichtige IT–Systeme, IT–Dienste und IT–Verfahren, um dafür Notfallprozesse, Wiederanlauf– bzw. Wiederherstellungsverfahren sowie Systemüberwachung und Reporting vorzugeben:

Tabelle 20: Kritische Systeme und Notfallprozesse

	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
Definition der wichtigen bzw. kritischen IT–Systeme und IT–Dienste	durchgeführt	durchgeführt	durchgeführt
Definition der IT–Notfallprozesse	vorhanden (auf Ebene der einzelnen IT–Verfahren)	vorhanden (auf Ebene der wichtigen IT–Systeme)	vorhanden (auf Ebene der wichtigen IT–Systeme)
Wiederherstellungsverfahren	vorhanden (auf Ebene der einzelnen IT–Verfahren)	vorhanden (auf Ebene der wichtigen IT–Systeme)	vorhanden (auf Ebene der wichtigen IT–Systeme)
Systeme zur laufenden Überwachung sowie Dokumentation durch Berichtswesen	vorhanden (auf Ebene der einzelnen IT–Verfahren)	vorhanden (für alle wichtigen IT–Systeme)	vorhanden (für alle wichtigen IT–Systeme)

Quellen: BMF; BMK; BML

Im Klimaschutzministerium waren Datensicherungs– und Wiederherstellungsmechanismen für Systeme und Daten auf Basis eines Konzepts aus 2013 im Einsatz; im Landwirtschaftsministerium stammte das Konzept aus 2015.

27.2 Der RH wies kritisch darauf hin, dass die Datensicherungs– und Wiederherstellungskonzepte des Klimaschutzministeriums bzw. des Landwirtschaftsministeriums aus 2013 bzw. 2015 stammten und seitdem nicht mehr aktualisiert worden waren. Er hielt dazu fest, dass grundlegende wichtige Konzepte, wie sie Datensicherungs– und Wiederherstellungskonzepte für die IT–Sicherheit darstellen, regelmäßig im Rahmen einer Qualitätssicherung zu aktualisieren bzw. zu überarbeiten sind.

Der RH empfahl daher dem Klimaschutz– und dem Landwirtschaftsministerium, aktuelle Datensicherungs– und Wiederherstellungskonzepte zu erstellen.

27.3 Das Landwirtschaftsministerium hielt in seiner Stellungnahme fest, eine Aktualisierung des Datensicherungs– und des Datenwiederherstellungs–Konzepts in Aussicht zu nehmen.

Überprüfung des IT–Notfallmanagements

28.1 Die folgende Tabelle vergleicht Art und Frequenz von Überprüfungen des IT–Notfallmanagements in den drei Bundesministerien:

Tabelle 21: Überprüfung Notfallmanagement

	Finanzministerium	Klimaschutzministerium	Landwirtschaftsministerium
Testung Notfallszenarien	regelmäßig	regelmäßig	regelmäßig
Überprüfungen (Audits für das Notfallmanagement)	regelmäßig	noch keine externen Audits für das Notfallmanagement durchgeführt	noch keine externen Audits für das Notfallmanagement durchgeführt

Quellen: BMF; BMK; BML

Das Finanzministerium testete Notfallszenarien regelmäßig und überprüfte auch mithilfe externer Audits das eingesetzte Notfallmanagement.

Das Klimaschutz– und das Landwirtschaftsministerium testeten Notfallszenarien ebenfalls regelmäßig; ein externes Audit für das Notfallmanagement fand allerdings noch nicht statt.

28.2 Der RH hielt fest, dass das Finanzministerium neben den regelmäßigen Testungen auch mithilfe von externen Audits das Notfallmanagement überprüfen ließ. Auch das Klimaschutzministerium und das Landwirtschaftsministerium testeten ihre definierten Notfallszenarien. Eine Überprüfung des Notfallmanagements durch externe Audits wurde allerdings nicht durchgeführt. Der RH sah in einem externen Audit für das Notfallmanagement die Möglichkeit, eine unabhängige und objektive Bewertung durchzuführen und durch diese Qualitätskontrolle potenzielle Mängel und Schwachstellen zu identifizieren.

Er empfahl daher dem Klimaschutz– und dem Landwirtschaftsministerium, das eingesetzte Notfallmanagement auch durch externe Audits überprüfen zu lassen.

28.3 Das Landwirtschaftsministerium hielt in seiner Stellungnahme fest, dass es nach Fertigstellung des IT–Notfallhandbuchs eine externe Überprüfung beauftragen werde.

Schlussempfehlungen

29 Zusammenfassend empfahl der RH

- dem Bundesministerium für Finanzen (**BMF**),
- dem Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (**BMK**),
- dem Bundesministerium für Land– und Forstwirtschaft, Regionen und Wasserwirtschaft (**BML**) und
- dem Bundeskanzleramt (**BKA**):

		BMF	BMK	BML	BKA
(1)	Eine Regierungsvorlage wäre zu erarbeiten, mit der im Bundesministeriengesetz 1986 eine Kompetenz zur Koordination der IT–Sicherheit klar und ausdrücklich festgelegt wird. (TZ 3)				X
(2)	Die im IKT–Konsolidierungsgesetz vorgesehene Verordnung wäre zu erlassen. (TZ 5)				X
(3)	Im Hinblick auf die zu erlassende(n) Verordnung(en) mit IKT–Standards wäre auch eine Regierungsvorlage zur Aktualisierung der Aufzählung von betroffenen IKT–Lösungen und IT–Verfahren in § 2 Abs. 1 IKT–Konsolidierungsgesetz vorzubereiten. (TZ 5)				X
(4)	Die im Programm IT–Konsolidierung erstellten Konzepte von den einzelnen Ressorts wären auf ihre Umsetzbarkeit zu prüfen und analysieren zu lassen, ob die Umsetzung schrittweise in Teilprojekten erfolgen sollte. (TZ 6)				X
(5)	Die Bundesministerien wären zur Teilnahme und aktiven Mitwirkung an den Projekten der IT–Konsolidierung zu motivieren. (TZ 6)				X
(6)	Das für die Koordination der IT zuständige Bundeskanzleramt sollte die nötige Teilnahme der Bundesministerien an der Umsetzung der im Projekt Security Framework Bund zu erarbeitenden Sicherheitsstandards fördern. Dies wäre über eine Einbeziehung in die Themen der Konferenz der Generalsekretäre bzw. eines gleichwertigen Gremiums (aus den internen administrativen Spitzen der Bundesministerien) zu begleiten. (TZ 7)				X
(7)	Die Vorbereitung der Regierungsvorlage für das „Informationssicherheitsgesetz neu“ wäre in der Informationssicherheitskommission sowie im Abstimmungsprozess mit den Bundesministerien zu unterstützen, um die Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen abzuschließen. (TZ 8)	X	X	X	

		BMF	BMK	BML	BKA
(8)	Die drei überprüften Ministerien sollten sich auf die Anforderungen durch die Umsetzung der 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**) vorbereiten. Der nationale Umsetzungsprozess wäre zu begleiten, um die wesentlichen Themen – wie Risikomanagement, Notfallvorsorge, Krisenmanagement, Verantwortung der Ressortleitung – ressortintern zeitgerecht zu berücksichtigen. (TZ 9)	X	X	X	
(9)	Es wären das – alle Ministerien aus der NIS–2–Richtlinie treffende – Thema der Umsetzung der erforderlichen Sicherheitsanforderungen sowie die finanziellen Erfordernisse in die Konferenz der Generalsekretäre bzw. ein gleichwertiges Gremium (aus den internen administrativen Spitzen der Bundesministerien) zwecks ressortübergreifender Erörterung einzubringen. (TZ 9)	X	X	X	
(10)	In der IT–Sicherheitsstrategie wäre die Verantwortung der Ressortleitung für die IT–Sicherheit ausdrücklich festzuhalten. (TZ 10)	X			
(11)	Es wäre eine grundsätzliche Richtlinie zur IT–Sicherheit für alle Bediensteten zu erlassen, mit Zielen, Verantwortlichkeiten, Grundsätzen des IT–Risikomanagementsystems, Organisation und Methoden. Diese IT–Sicherheitsstrategie sollte die geltenden Grundsätze transparent und nachvollziehbar darstellen und das Bewusstsein (Awareness) für IT–Sicherheit bei den Bediensteten erhöhen. Sie wäre auch für die nachgeordneten Dienststellen für verbindlich zu erklären. (TZ 10)		X	X	
(12)	Den nachgeordneten Dienststellen, denen die Gewährleistung der IT–Sicherheit eigenständig obliegt, wären (erweiterte) Berichtspflichten aufzuerlegen – insbesondere zu Abweichungen von den geltenden Strategien, Sicherheitsvorfällen, durchgeführten Audits und der Erfüllung von Sicherheitsstandards –, damit die Ressortleitung im Bedarfsfall ihre Steuerungsfunktion erfüllen kann. (TZ 10)		X	X	
(13)	Es wären jene kritischen IT–Verfahren festzulegen, für die Risikoanalysen regelmäßig zu überprüfen und gegebenenfalls zu aktualisieren wären. (TZ 11)		X	X	
(14)	Die IT–Anwendungen wären nach jenen Kriterien, die im Umsetzungsleitfaden des Bundeskanzleramts für die öffentlichen Einrichtungen nach dem Netz– und Informationssystemsicherheitsgesetz beschrieben sind, zu überprüfen und allfällig vorliegende wichtige Dienste zu identifizieren (z.B. das Führerscheinregister, das elektronische Datenmanagement nach dem Abfallwirtschaftsgesetz oder das Wasserinformationssystem). Dies wäre auch zweckmäßig als Vorbereitung auf die Umsetzung der NIS–2–Richtlinie. (TZ 11)		X	X	

		BMF	BMK	BML	BKA
(15)	In der IT–Sicherheitsstrategie wäre neben der zuständigen Sektionsleitung auch die Ressortleitung als konkrete Berichtsempfängerin bzw. konkreter Berichtsempfänger festzulegen. Dies wäre auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie, die die Verantwortung der Leitungsorgane ausdrücklich fordert (Art. 20 Governance), zweckmäßig. (TZ 12)	X			
(16)	In der IT–Sicherheitsstrategie wäre ein regelmäßiges, standardisiertes Berichtswesen zur IT–Sicherheit unter Einbeziehung der oberen Führungsebene (Sektionsleitung, Generalsekretärin bzw. Generalsekretär, Ressortleitung) als Berichtsempfängerin bzw. Berichtsempfänger festzulegen. Dies wäre auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie, die die Verantwortung der Leitungsorgane ausdrücklich fordert (Art. 20 Governance), zweckmäßig. (TZ 12)		X	X	
(17)	Das vom Ministerium geplante ressortweite Entscheidungsgremium für IKT–Sicherheit wäre in die Praxis umzusetzen. Über den Nutzen und die Effektivität einer derartigen Organisation wäre in den Gremien CDO–Task–Force und IKT–Bund zu berichten. (TZ 13)			X	
(18)	Die Funktion des Chief Information Security Officers (CISO) wäre rasch zu besetzen. (TZ 14)		X		
(19)	Die Funktion des Chief Information Security Officers (CISO) wäre unabhängig von der IT–Abteilungsleitung einzurichten. (TZ 14)			X	
(20)	In das Informationssicherheitsmanagement–Team wären Anwenderinnen und Anwender aufzunehmen. (TZ 15)	X			
(21)	Ein Informationssicherheitsmanagement–Team wäre einzurichten und dabei auf eine zweckentsprechende Einbindung der Anwenderinnen und Anwender sowie der nachgeordneten Dienststellen zu achten. Zudem wären wieder regelmäßig Sitzungen abzuhalten und der Vorsitz klar festzulegen (z.B. mittels Geschäftsordnung). (TZ 15)		X		
(22)	Jene älteren Geräte, bei denen das Unterbinden des Startens von externen Datenträgern aus technischen Gründen nicht möglich ist, wären zu ersetzen. (TZ 17)		X		
(23)	Es wäre eine USB–Port–Deaktivierung bzw. eine USB–Port–Kontrolle für die IT–Arbeitsplätze einzusetzen. (TZ 17)		X	X	
(24)	Für die IT–Arbeitsplätze wäre Applikations–Whitelisting einzusetzen, um zu gewährleisten, dass ausschließlich vorgesehene Applikationen gestartet werden können. (TZ 17)			X	
(25)	Der Einsatz eines umfassenden Endpoint–Protection–Systems wäre als Beitrag zur IT–Sicherheit der IT–Arbeitsplätze zu prüfen; erforderlichenfalls wäre ein solches System einzusetzen. (TZ 17)		X		

		BMF	BMK	BML	BKA
(26)	Die jeweiligen Authentifizierungsmethoden für die IT–Arbeitsplätze wären einer Risikoanalyse zu unterziehen. Der Bedarf nach einer Zwei–Faktor–Authentifizierung wäre zu prüfen und diese allenfalls einzusetzen. (TZ 18)		X	X	
(27)	Die Anzahl der eingesetzten Videokonferenzsysteme wäre auf das erforderliche Maß zu verringern. (TZ 19)		X	X	
(28)	Das bundeseinheitliche Videokonferenzsystem wäre bis zur Fertigstellung im erweiterten Testbetrieb mit anderen Bundesministerien zu erproben. (TZ 19)				X
(29)	Auch Bedienstete ohne Telearbeitsanordnung bzw. –vereinbarung wären im Falle der anlassbezogenen Telearbeit auf geeignete Weise gesondert darauf hinzuweisen, dass die Datensicherheitsvorschriften und die Vorschriften für die IT–Sicherheit einzuhalten sind. (TZ 20)	X		X	
(30)	In Bezug auf Telearbeit wäre konkret festzulegen, ob bestimmte dienstliche Aufgaben jedenfalls aus Sicherheitsgründen an der Dienststelle zu verrichten sind. (TZ 20)	X	X	X	
(31)	Regelungen über den Umgang mit klassifizierten Informationen wären in den Vorgaben zur IT–Sicherheit – der Datensicherheitsvorschrift – zu ergänzen. (TZ 21)			X	
(32)	Der Absolvierungsgrad der Awareness–Schulungen für IT–Sicherheit im Ministerium wäre durch geeignete Maßnahmen zu erhöhen. (TZ 22)	X			
(33)	Die Awareness–Schulungen wären um das Thema „IT–Sicherheit im Arbeitsalltag“ zu ergänzen. (TZ 22)		X		
(34)	Awareness–Schulungen zu IT–Sicherheit wären regelmäßig und für die Bediensteten verpflichtend durchzuführen. (TZ 22)			X	
(35)	Fernwartungszugriffe auf zentrale Systeme wären nur anlassbezogen und nur zeitlich begrenzt zu gewähren. Daher wäre zu überprüfen, ob die permanenten privilegierten Zugriffe auf Server–Systeme (im Bereich Server–Betreuung), die auch Fernwartung beinhalten, erforderlich sind. (TZ 23)		X		
(36)	Es wäre ein System zur Erkennung bzw. Abwehr von Angriffen zu implementieren (Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS)). (TZ 24)		X		
(37)	Es wäre zu prüfen, ob ein Security Information and Event Management (SIEM) einen effektiven Beitrag zur Verbesserung der IT–Sicherheit mit sich bringen würde. Erforderlichenfalls wäre ein solches einzuführen. (TZ 24)		X		
(38)	Es wäre zu prüfen, ob ein Security Operation Center (SOC) einen effektiven Beitrag zur Verbesserung der IT–Sicherheit mit sich bringen würde. Erforderlichenfalls wäre ein solches einzuführen. (TZ 24)		X	X	

		BMF	BMK	BML	BKA
(39)	Zunächst wäre der Bedarf an IT–Sicherheitsüberprüfungen basierend auf einer umfassenden Risikoanalyse zu erheben, sodann wären die notwendigen IT–Sicherheitsüberprüfungen zu priorisieren und schließlich diese Überprüfungen zeitnah unter Berücksichtigung der verfügbaren Ressourcen sowie bedarfsgerecht unter Einbindung von externem Fachwissen durchzuführen. (TZ 25)		X	X	
(40)	Für definierte IT–Systeme, IT–Dienste und IT–Verfahren wäre ein Notfallmanagementkonzept zu erstellen und umzusetzen. (TZ 26)		X	X	
(41)	Aktuelle Datensicherungs– und Wiederherstellungskonzepte wären zu erstellen. (TZ 27)		X	X	
(42)	Das eingesetzte Notfallmanagement wäre auch durch externe Audits überprüfen zu lassen. (TZ 28)		X	X	

Rechnungshof
Österreich

Wien, im Mai 2024
Die Präsidentin:

Dr. Margit Kraker

R
H