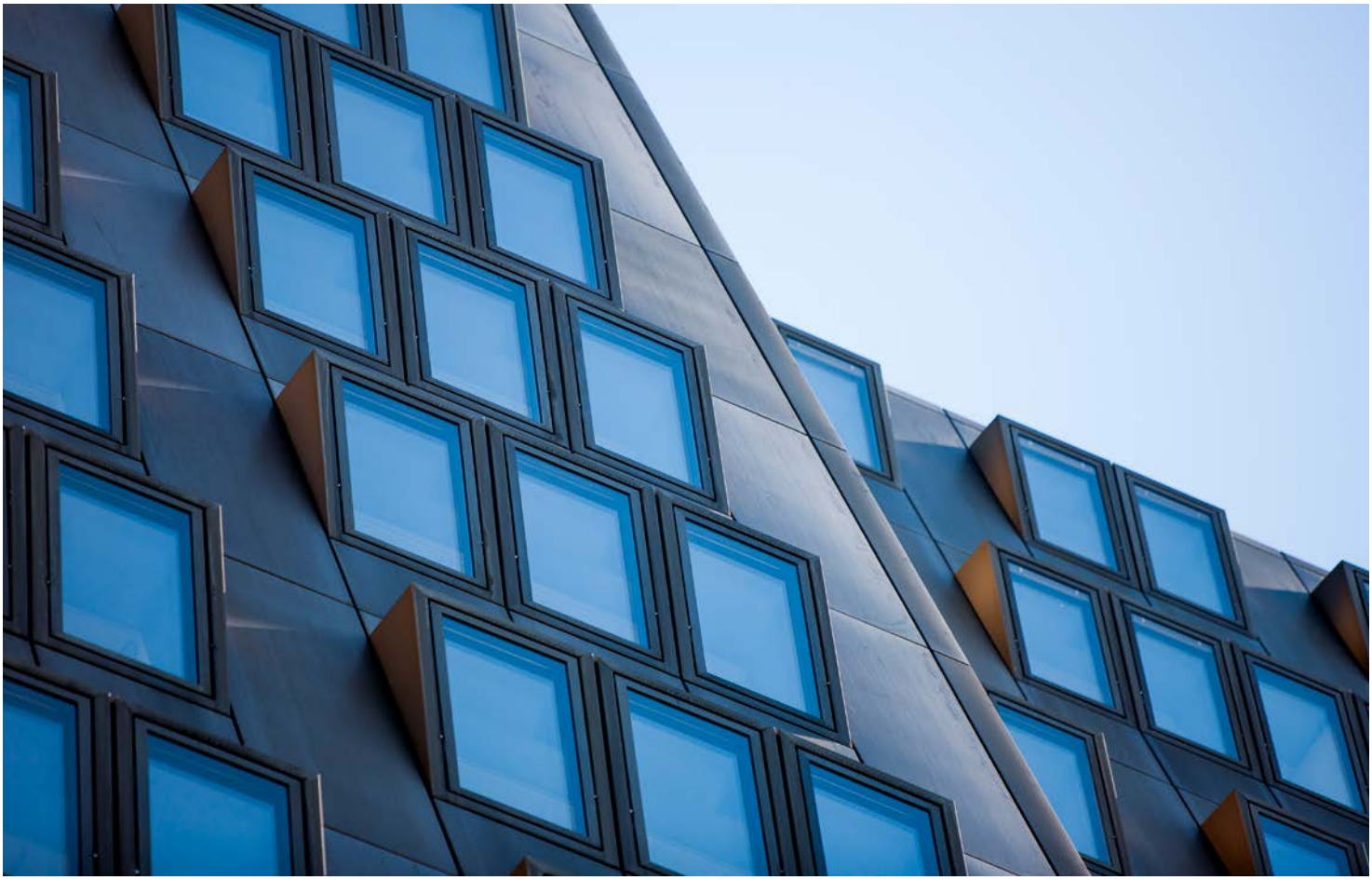
Rechnungshof Österreich

Unabhängig und objektiv für Sie.

Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien

Reihe BUND 2021/31

Bericht des Rechnungshofes



III–410 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP
Rechnungshof GZ 004.753/012–PR3/21

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
1031 Wien, Dampfschiffstraße 2
www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im September 2021

AUSKÜNFTE

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

FOTOS

Cover: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
Art.	Artikel
BDG 1979	Beamten–Dienstrechtsgesetz 1979
BGBl.	Bundesgesetzblatt
BKA	Bundeskanzleramt
BMAFJ	Bundesministerium für Arbeit, Familie und Jugend
BMASGK	Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BMEIA	Bundesministerium für europäische und internationale Angelegenheiten
BMF	Bundesministerium für Finanzen
BMG	Bundesministeriengesetz
BMGF	Bundesministerium für Gesundheit und Frauen
BMJ	Bundesministerium für Justiz
BMKÖS	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport
BMöDS	Bundesministerium für öffentlichen Dienst und Sport
BMSGPK	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
BMVRDJ	Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz
BRZ GmbH	Bundesrechenzentrum Gesellschaft mit beschränkter Haftung
BSI	Bundesamt für Sicherheit und Informationstechnik (Deutschland)
bzw.	beziehungsweise
CDO	Chief Digital Officer
CERT	Computer Emergency Response Team (Computer–Notfallteam)
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DSGVO	Datenschutz–Grundverordnung
d.h.	das heißt
ELAK	elektronischer Akt/elektronisches Aktenverwaltungssystem
ENISA	Agentur der Europäischen Union für Cybersicherheit
etc.	et cetera
EU	Europäische Union
EUR	Euro

GmbH	Gesellschaft mit beschränkter Haftung
ID	Identifikation
i.d.(g.)F.	in der (geltenden) Fassung
IKT	Informations– und Kommunikationstechnologie
InfoSiG	Informationssicherheitsgesetz
InfoSiV	Informationssicherheitsverordnung
ISMT	Informationssicherheitsmanagement–Team
IT	Informationstechnologie
lit.	litera (Buchstabe)
Mio.	Million(en)
NISG	Netz– und Informationssystemsicherheitsgesetz
Nr.	Nummer
PC	Personal Computer
rd.	rund
RH	Rechnungshof
TZ	Textzahl(en)
u.a.	unter anderem
VBG	Vertragsbedienstetengesetz 1948
vgl.	vergleiche
VPN	Virtual Private Network (sichere, verschlüsselte Verbindung zwischen zwei oder mehreren Geräten)
z.B.	zum Beispiel

Glossar

Applikation Whitelisting

Durch den Einsatz der Applikation Whitelisting können ausschließlich explizit erlaubte Programme bzw. Applikationen auf einem Computer gestartet werden.

Authentifizierung

Die Authentifizierung ist die Überprüfung der behaupteten Authentizität.

Authentisierung

Die Authentisierung dient zur Überprüfung der Identität, z.B. durch Eingabe von Kennwörtern oder der „Personal–Identification–Number". Die Authentisierungs–Verfahren unterscheiden sich nach Wissen (Passwort), Besitz (Smartcard, Chip) oder Eigenschaft (biometrische Verfahren). Man spricht von einer Zwei–Faktor–Authentisierung (häufig auch als Zwei–Faktor–Authentifizierung), wenn der Identitätsnachweis mittels der Kombination von zwei unterschiedlichen und insbesondere unabhängigen Komponenten erfolgt, z.B. Fingerabdruck und Kennwort. Für sicherheitskritische Anwendungsbereiche, dazu zählt auch der Zugang von einem externen Arbeitsplatz in ein Unternehmensnetz, sollte eine Zwei–Faktor–Authentisierung verpflichtend sein.

Autorisierung

Die Autorisierung ist die Einräumung der speziellen Rechte an die Benutzerin bzw. den Benutzer.

Denial of Service–Angriff

Bei Denial of Service–Angriffen (DoS, Verweigerung eines Dienstes) wird ein Dienst durch eine Vielzahl von Anfragen, z.B. an einen Web–Server, blockiert. Der Dienst steht dann den Anwendern nicht bzw. stark eingeschränkt zur Verfügung. Der Grad der Verfügbarkeit bzw. Nicht–Verfügbarkeit des Dienstes hängt dabei von der Intensität der störenden Anfragen im Verhältnis zur Bearbeitungskapazität des Dienstes ab.

Distributed Denial of Service–Angriff

Das Grundprinzip beim Distributed Denial of Service–Angriff (DDoS) ist gleich wie bei einem Denial of Service, allerdings wird die Intensität der störenden Anfragen dadurch drastisch erhöht, dass diese von einer Vielzahl von Rechnern generiert werden.

Endpoint–Protection–System

Ein Endpoint–Protection–System soll die verschiedenen Endgeräte (PC, Tablets, Laptops, Smartphones etc.) im lokalen Netz vor Gefahren schützen. Hierbei handelt es sich um eine integrierte Lösung, welche aus mehreren optionalen Komponenten, z.B. Schutz vor Schadsoftware, Schutz vor Phishing, Firewall, Intrusion Detection System, Intrusion Prevention System, Datenträgerverschlüsselung oder Applikation Whitelisting, besteht. Durch das Endpoint–Protection–System soll gewährleistet werden, dass ein aktiver Schutz für sämtliche Endgeräte gegeben ist, um Cyberbedrohungen direkt am Endgerät effektiv zu identifizieren, einzudämmen und zu eliminieren. Der Mehrwert eines umfassenden modernen Endpoint–Protection–Systems kann auch darin liegen, die Log–Daten des Endpoint–Protection–Systems direkt in ein Security Information and Event Management System (SIEM) in Echtzeit einfließen zu lassen.

Firewall

Eine Firewall ist eine technische Schutzmaßnahme, um unerwünschte Verbindungsversuche aus dem öffentlichen Netz (Internet) ins lokale Netz zu unterbinden. Mit einer Firewall lässt sich der Datenverkehr (in beide Richtungen) kontrollieren, protokollieren, sperren und freigeben.

Identifikation

Die Benutzerin bzw. der Benutzer identifiziert sich durch Eingabe des Benutzernamens oder der Kontonummer.

Intrusion Detection Systeme

Intrusion Detection Systeme (IDS) analysieren und überwachen den Netzwerkverkehr auf Anzeichen, ob Angriffe im Gange sind. Sie vergleichen die laufende Netzwerkaktivität mit einer Datenbank bekannter Bedrohungen, um auffällige Aktivitäten wie Verstöße gegen Sicherheitsrichtlinien, Malware und Port–Scanner zu erkennen.

Intrusion Prevention Systeme

Intrusion Prevention Systeme (IPS) analysieren den Netzwerkverkehr ähnlich wie Intrusion Detection Systeme, allerdings sind sie in der Lage, den Netzwerkverkehr auf der Grundlage eines Sicherheitsprofils aktiv abzulehnen, wenn eine Bedrohung erkannt wird.

Phishing

Mit Phishing wird beispielsweise über gefälschte Websites, E–Mails oder andere Messenger–Nachrichten versucht, an persönliche Daten zu gelangen. Phishing steht häufig im Zusammenhang mit Betrugshandlungen und Identitätsmissbrauch.

Proxy

Ein Proxy ist eine als Vermittler arbeitende Kommunikationsschnittstelle in einem Netzwerk. Auf der einen Seite nimmt der Proxy Anfragen entgegen, um diese dann über seine eigene Adresse zur anderen Seite weiterzuleiten.

Ransomware

Als Ransomware wird Schadsoftware bezeichnet, die den Zugriff auf Daten und elektronische Systeme einschränkt oder verhindert. Diese Ressourcen werden erst wieder nach Bezahlung eines Lösegelds („ransom“) freigegeben.

Security Information and Event Management

Security Information and Event Management (SIEM) ist eine Software–Lösung, die eine ganzheitliche Sicht auf die Sicherheit der Informationstechnologie einer Organisation bieten soll. Ein SIEM–System fasst die Funktionalitäten der Systeme für Security Information Management (SIM) und für Security Event Management (SEM) zur Echtzeitanalyse zusammen. Im SIM–System werden Daten an einer zentralen Stelle zur Analyse gesammelt (Log Management), dafür werden Daten (Protokolle und andere sicherheitsrelevante Dokumente) über verschiedene Quellen hinweg erfasst und überwacht. Im SEM–System werden die gesammelten Daten korreliert, mit definierten Richtlinien abgeglichen und entsprechende Alarmierungen durchgeführt.

Social Engineering

Unter Social Engineering werden Angriffe, die sich nicht direkt auf technische Systeme, sondern auf deren Benutzerinnen und Benutzer richten, bezeichnet.

Spamfilter

Ein Spamfilter dient zum Ausfiltern von unerwünschter Werbung bzw. unerwünschten E–Mails.

Spyware

Als Spyware wird Software bezeichnet, die Daten eines Computernutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software oder an Dritte sendet bzw. die dazu genutzt wird, der Benutzerin oder dem Benutzer über Werbeeinblendungen Produkte anzubieten.

Thin–Client

Ein Thin–Client ist ein einfach aufgebauter Computer, der keinen eigenen Festspeicher besitzt und meistens direkt über das Netzwerk bootet. Er bildet im Prinzip nur die Benutzerschnittstelle zur Anwenderin bzw. zum Anwender (Tastatur, Maus, Monitor), weshalb die Anwendungen nicht lokal (am Client selbst), sondern am zentralen Applikationsserver laufen.

Trojaner

Als Trojaner bezeichnet man ein Computerprogramm, das als nützliche oder harmlose Anwendung getarnt ist, im Hintergrund aber ohne Wissen der Anwenderin bzw. des Anwenders eine schädliche Funktion erfüllt.

Verschlüsselung

Verschlüsselung ist die mit einem Verschlüsselungsverfahren und einem Schlüssel (Key) vorgenommene Umwandlung von „Klartext" in einen verschlüsselten Text.

Viren

Bei (Computer–)Viren handelt es sich um Schadsoftware, die sich selbst verbreiten und unterschiedliches Schadenspotenzial in sich tragen. Sie treten in Kombination mit einem Wirt auf, d.h. mit einem infizierten Dokument oder einer Applikation.

Virtual Private Network

Ein Virtual Private Network (VPN) ist eine sichere, verschlüsselte Verbindung (VPN–Tunnel) zwischen zwei oder mehreren Geräten. Meistens werden VPN–Tunnel eingesetzt, um von einem beliebigen externen Standort einen vollen Zugriff auf ein internes Netz (z.B. ein lokales Unternehmensnetz) zu ermöglichen.

Zugriffskontrolle

Die vier wesentlichen Bestandteile der Zugriffskontrolle sind die Identifikation, die Authentisierung, die Authentifizierung und die Autorisierung.

WIRKUNGSBEREICH

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

Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien

Prüfungsziel

Der RH überprüfte von Juni bis Oktober 2020 ausgewählte Aspekte des Managements der IT–Sicherheit in der Verwaltung des Bundes. Prüfungsziele waren die Darstellung und Beurteilung der Konzeption und Umsetzung ausgewählter Aspekte des Managements der IT–Sicherheit in den Zentralstellen des Bundeskanzleramts (**BKA**), des Bundesministeriums für Kunst, Kultur, öffentlichen Dienst und Sport (**BMKÖS**), des Bundesministeriums für Digitalisierung und Wirtschaftsstandort (**BMDW**) sowie des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz (**BMSGPK**). Dies betraf insbesondere die IT–Sicherheitsstrategie, die IT–Sicherheitsorganisation, das Personal für IT–Sicherheit und das IT–Sicherheitsmanagement. Darüber hinaus überprüfte der RH in diesen Ressorts den in der COVID–19–Pandemie erfolgten Übergang auf Homeoffice im Hinblick auf die IT–Sicherheit. Der überprüfte Zeitraum umfasste die Jahre 2018 bis 2020.

Kurzfassung

IT–Betreuung

Bei der Bildung oder Umbildung von Bundesregierungen werden meist auch Kompetenzen zwischen den Ressorts verschoben. In den von dieser Gebarungsüberprüfung umfassten Bundesministerien betraf die Verschiebung im Jänner 2020 beispielhaft die Agenden Familie und Jugend vom BKA zum damals neuen Bundesministerium für Arbeit, Familie und Jugend (**BMAFJ**), die Agenden Kunst/Kultur vom BKA zum BMKÖS, die Agenden Integration vom Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**) zum BKA, die Agenden Staatliche Verfassung vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz (**BMVRDJ**) zum BKA sowie die Agenden Arbeit vom Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz (**BMASGK**) zum damals neuen BMAFJ. Dabei wurden auch

IT–Arbeitsplätze verschoben, was generell einen hohen Aufwand in der neu zuständigen IT–Abteilung bei der Integration der neu dazugekommenen IT–Ausstattung der Arbeitsplätze, der IT–Fachanwendungen und der IT–Infrastruktur bedeutete. In der Phase der Überleitung können sich IT–Sicherheitsrisiken ergeben, weil innerhalb eines Bundesministeriums parallel unterschiedliche Systeme zur Gewährleistung der IT–Sicherheit anzuwenden sind. Im September 2020 – neun Monate nach Verschiebung von Ressortkompetenzen anlässlich der Regierungsbildung im Jänner 2020 – waren im BKA, im BMKÖS und im BMSGPK bei der IT–Betreuung noch keine ressorteinheitlichen IT–Zuständigkeiten gegeben. Die Bundesministeriengesetz–Novelle 2021 brachte eine neuerliche Verschiebung der Agenden Familie und Jugend in das BKA. (TZ 2, TZ 3)

Mit dem IKT–Konsolidierungsgesetz bestand seit 2012 die Grundlage für die Vereinheitlichung der Informations– und Kommunikationstechnologie (**IKT**). Auch der zum Statusbericht betreffend die Heterogenität der IT–Ausstattung gefasste Beschluss der Bundesregierung im November 2019 unterstützte die Umsetzung von Konsolidierungsmaßnahmen. Dennoch fehlte zur Zeit der Gebarungsüberprüfung die zum Konsolidierungsgesetz vorgesehene Verordnung; die Zuständigkeit hierfür oblag bis 2017 dem BKA, ab 2018 dem BMDW. (TZ 2, TZ 3)

Die Konsolidierung der IT–Ausstattung der Arbeitsplätze wäre ein Beitrag, die Kosten der IT–Beschaffung und der Lizenzgebühren zu reduzieren, die Heterogenität der generellen Bürosoftwareausstattung zu reduzieren und die Betreuung der IT–Ausstattung der Arbeitsplätze zu bündeln. Darüber hinaus ermöglicht die Verwendung einheitlicher Bürosoftware sowie die einheitliche und zeitgerechte Installierung der zugehörigen Sicherheits–Updates auch die Bündelung des für die IT–Sicherheit zuständigen Personals und leistet dazu ebenfalls einen Beitrag zur Erhöhung der IT–Sicherheit. (TZ 2, TZ 3)

Gemäß Bundesministeriengesetz ist das BKA u.a. für Angelegenheiten der strategischen Netz– und Informationssicherheit (gemäß NIS–Gesetz) zuständig, das BMDW für die Koordination und zusammenfassende Behandlung in Angelegenheiten der Informationstechnologie. 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 festgelegt. (TZ 2)

Die IT–Abteilung Gesundheit des BMSGPK betreute u.a. in diesem Bundesministerium die IT der zwei die Gesundheit betreffenden Sektionen und darüber hinaus aufgrund eines Verwaltungsübereinkommens seit 2018 auch die IT des Bundesministeriums für öffentlichen Dienst und Sport (**BMöDS**) bzw. seit 2020 des nunmehrigen BMKÖS. (TZ 3)

Im BMKÖS lagen auch im Oktober 2020 noch keine eigenen grundlegenden Dokumente betreffend das Management der IT–Sicherheit, etwa zu den Themen IT–Strategie, –Risikomanagement, –Berichtswesen und –Organisation, vor, obwohl dieses Bundesministerium im Wesentlichen im Jänner 2018 eingerichtet worden war. Hierzu kam der Umstand, dass die Verantwortung für die IT–Sicherheit, die IKT–Infrastruktur und den IKT–Betrieb des BMöDS (ab 2018) bzw. des BMKÖS (ab 2020) trotz des mit dem BMSGPK geschlossenen Verwaltungsübereinkommens bei der Abteilung I/3 (Rechtskoordination, Informations–, Organisations– und Verwaltungsmanagement) des nunmehrigen BMKÖS lag. (TZ 4)

Der IT–Abteilung Gesundheit waren zur Zeit der Gebarungsüberprüfung aufgrund ihrer umfangreichen Aufgaben im Zusammenhang mit der Bewältigung der COVID–19–Pandemie die Beantwortung der vom RH übermittelten Fragebögen sowie die Erstellung weiterer für diese Gebarungsüberprüfung relevanter Ausarbeitungen für den Wirkungsbereich des BMKÖS faktisch nicht möglich. Der RH nahm daher von einer Beurteilung der IT–Sicherheit im BMKÖS Abstand, wird aber im Rahmen einer Follow–up–Überprüfung diese Aspekte überprüfen. (TZ 4)

Die zusätzliche Betreuung des BMKÖS durch die IT–Abteilung Gesundheit des BMSGPK war aufgrund der Doppelbelastung für beide Bundesministerien nachteilig und brachte das Risiko eines nicht ausreichenden Managements der IT–Sicherheit des BMKÖS mit sich. (TZ 4)

Grundlagen der IT–Sicherheit

Die IT–Sicherheitsstrategien des BKA, des BMDW und des BMSGPK verfolgten die wesentlichen für eine umfassende IT–Sicherheit relevanten Ziele; die darin festgelegten Maßnahmen waren nachvollziehbar und berücksichtigten organisatorische und personelle Aspekte. (TZ 7)

IT–Sicherheitsorganisation

Im BMSGPK gab es zwei IT–Abteilungen – eine für den Bereich Soziales und eine für den Bereich Gesundheit. Die IT–Abteilung Soziales war Teil der Präsidialsektion, die IT–Abteilung Gesundheit Teil der Sektion VI – Humanmedizinrecht und Gesundheitstelematik. Die Koordination für die gesamte IT des BMSGPK war daher erst in der Funktion der Generalsekretärin organisatorisch zusammengeführt. Durch die Aufteilung des IT–Betriebs auf zwei Abteilungen in zwei getrennten Sektionen entstand das Risiko einer uneinheitlichen Umsetzung der IT–Sicherheitsstrategie. Auch entsprach es nicht der typischen Aufgabe einer Generalsekretärin, die Tätigkeit von zwei operativen IT–Abteilungen zu koordinieren. (TZ 10)

Eine IT–Sicherheitsorganisation umfasst folgende Standardfunktionen: Für alle Fragen der Informations– und IT–Sicherheit ist der „Chief Information Security Officer", für die IT–Sicherheit der „IT–Sicherheitsbeauftragte" verantwortlich. Die Leitung der für die gesamte Infrastruktur und für den Betrieb verantwortlichen IT–Abteilung wird auch als „Chief Information Officer" bezeichnet. Weiters ist ein „Informationssicherheitsbeauftragter" gemäß Informationssicherheitsgesetz in jedem Bundesministerium einzurichten. Der „Chief Digital Officer" ist schließlich für die Digitalisierungsstrategie und Digitalisierungsmaßnahmen des jeweiligen Bundesministeriums gesamtverantwortlich. Im BMDW und BMSGPK war die Funktion „IT–Sicherheitsbeauftragter" eingerichtet und besetzt, nicht aber ein „Chief Information Security Officer"; im BMSGPK war auch die Funktion des „Chief Digital Officers" nicht besetzt. (TZ 11)

IT–Arbeitsplätze und Telearbeit/Homeoffice

Zusätzlich zu den IT–Sicherheitsrisiken eines IT–Arbeitsplatzes an der Dienststelle ergaben sich im Zusammenhang mit Telearbeit weitere spezifische Risiken. Zu diesen zählten etwa der Verlust des mobilen IT–Geräts, das Ausspähen von Zugangsdaten oder eine allfällige, gegenüber dem IT–Arbeitsplatz an der Dienststelle infrastrukturell bedingt herabgesetzte IT–Sicherheit. Um diese Risiken zu reduzieren, sollte etwa eine Zwei–Faktor–Authentifizierung für Zugriffe von außen auf das Netz des Bundesministeriums oder eine Verschlüsselung der Daten auf den Festplatten der Arbeitsplatzrechner eingerichtet sein. Die Einführung einer Zwei–Faktor–Authentifizierung für die Arbeitsplatzrechner des Ressorts war im BKA und BMDW noch nicht abgeschlossen. (TZ 14)

Im BKA, BMDW und BMSGPK kamen insgesamt vier unterschiedliche, innerhalb eines Bundesministeriums zum Teil mehrere Videokonferenz–Softwareprodukte zur Anwendung. Damit war die Durchführung von Videokonferenzen zwischen Bediensteten unterschiedlicher Bundesministerien, teilweise selbst zwischen Bediensteten innerhalb eines Bundesministeriums, erschwert. Der Einsatz einer Vielzahl von Softwareprodukten bedeutete auch einen erhöhten Betreuungsaufwand. (TZ 15)

Die Nutzung privater IT–Ausstattung für Telearbeit war gesetzlich nicht vorgesehen, weil der Dienstgeber die erforderliche IT–Ausstattung für die Telearbeit zur Verfügung zu stellen hat. Für die während des umfangreicheren Homeoffice in der COVID–19–Pandemie teilweise Nutzung privater IT–Ausstattung fehlten im BKA, BMDW und BMSGPK ausreichende Vorgaben zur IT–Sicherheit. Die für die reguläre Telearbeit angeordneten Sicherheitsvorkehrungen waren aufgrund der geringen Anzahl von Telearbeitsanordnungen bzw. –vereinbarungen nur einem Teil der Bediensteten im Homeoffice nachweislich zur Kenntnis gebracht. Im BKA lagen Richtlinien zur sicheren Nutzung mobiler Endgeräte sowie eine zusammenfassende Richtlinie zur Telearbeit noch nicht vor. (TZ 17, TZ 18, TZ 20)

IT–Sicherheit Personal

Das BKA, BMDW und BMSGPK bezogen IT–Dienstleistungen von externen Unternehmen in unterschiedlichem Ausmaß. Im BKA und BMSGPK kam das externe Personal aus der Bundesrechenzentrum Gesellschaft mit beschränkter Haftung (**BRZ GmbH**). Das BMDW setzte hingegen im Wege seines externen Dienstleisters auch externes Personal – mit Zugriff im Second–Level–Support auf IT–Systeme des BMDW – ein, das seinen Arbeitsort im EU–Ausland hatte. Die notwendigen Sicherheitsüberprüfungen des Personals erfolgten im EU–Ausland mit Hilfe sicherheitspolizeilicher Unterstützung der Behörden vor Ort. Da das externe IT–Personal mit Arbeitsort im EU–Ausland auch Zugriff auf wichtige Dienste des BMDW hatte, lag darin auch ein Risiko hinsichtlich der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der vom BMDW verarbeiteten Daten. Durch den genannten Arbeitsort war auch eine unmittelbare Aufsicht bzw. Kontrolle des externen Personals weder für den externen Dienstleister noch für den Auftraggeber BMDW direkt möglich. (TZ 22)

IT–Sicherheit Infrastruktur

Die drei Bundesministerien hatten wesentliche technische Maßnahmen betreffend die IT–Sicherheit umgesetzt. (TZ 23)

Die Notfallszenarien zur Sicherstellung der Kontinuität des IT–Betriebs für die vom BKA selbst betriebenen IT–Anwendungen waren noch nicht ausreichend festgelegt. So gab es kein IT–Notfallhandbuch, nur zwei IT–Notfallszenarien, keine klaren Kriterien für den Eintritt von IT–Notfällen und keine eigene IT–Notfallorganisation. Auch im BMDW fehlten Notfallkonzepte wie IT–Notfallhandbücher, IT–Notfallszenarien oder IT–Notfallpläne für die selbst betriebenen IT–Systeme. Die Notfallszenarien des BKA, BMDW und BMSGPK waren nicht ausreichend getestet worden und das Notfallmanagement wurde in den externen IT–Audits nicht berücksichtigt. (TZ 25, TZ 27)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

ZENTRALE EMPFEHLUNGEN

- Das Bundeskanzleramt und das Bundesministerium für Digitalisierung und Wirtschaftsstandort sollten eine Regierungsvorlage erarbeiten, mit der im Bundesministeriengesetz eine Kompetenz zur Koordination der IT–Sicherheit klar und ausdrücklich festgelegt wird. (TZ 2)

- Das Bundesministerium für Digitalisierung und Wirtschaftsstandort sollte im Einvernehmen mit dem Bundeskanzleramt die im IKT–Konsolidierungsgesetz vorgesehene Verordnung erlassen. Darüber hinaus wären im Bundeskanzleramt, im Bundesministerium für Digitalisierung und Wirtschaftsstandort, im Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz und im Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport jeweils in einem Projekt die Konsolidierung der IT–Ausstattung der Arbeitsplätze des Ressorts zu behandeln, um die Kosten der IT–Beschaffung und der Lizenzgebühren zu reduzieren, die Heterogenität der generellen Bürosoftwareausstattung zu verringern und die Betreuung der IT–Ausstattung der Arbeitsplätze zu bündeln. (TZ 3)

- Im Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport wären das Management der IT und deren Sicherheit so zu gestalten, dass die grundlegenden Aufgaben der IT–Sicherheit selbst wahrgenommen werden können. (TZ 4)

- Die Telearbeit im regulären Dienstbetrieb des Bundeskanzleramts, des Bundesministeriums für Digitalisierung und Wirtschaftsstandort und des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz wäre nur dann vorzusehen, wenn eine geeignete dienstliche IT–Ausstattung zur Verfügung steht und die technischen Sicherheitsvorkehrungen erfüllt sind, um die IT–Sicherheit zu gewährleisten. Im Hinblick auf mögliche weitere Phasen von krisenbedingtem Homeoffice wäre die IT–Ausstattung der Arbeitsplätze künftig so einzurichten, dass in dem zur Aufrechterhaltung des Dienstbetriebs erforderlichen Umfang eine Dienstverrichtung außerhalb der Dienststelle mit dienstlichen Geräten möglich ist. (TZ 17)

- Das Bundeskanzleramt, das Bundesministerium für Digitalisierung und Wirtschaftsstandort und das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz sollten insbesondere im Hinblick auf einen allfällig neuerlich notwendigen Übergang des Dienstbetriebs auf Homeoffice

  – ausdrückliche organisatorische und technische Vorgaben betreffend die allfällig notwendige Nutzung privater IT–Ausstattung im Netz des Bundesministeriums erstellen,

  – den Bediensteten die in den verschiedenen Regelungen vorgesehenen IT–Sicherheitsmaßnahmen für eine Dienstverrichtung auf IT–Arbeitsplätzen außerhalb der Dienststelle nachweislich zur Kenntnis bringen und

  – konkret festlegen, ob bestimmte dienstliche Aufgaben jedenfalls aus Sicherheitsgründen an der Dienststelle zu verrichten sind. (TZ 18)

Zahlen und Fakten zur Prüfung

IT–Einsatz in der Zentralstelle von BKA, BMDW und BMSGPK						
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.					
	BKA[1]		**BMDW**		**BMSGPK**	
	2019	**2020**	**2019**	**2020**	**2019**	**2020**
	Anzahl zum 31. Dezember					
Arbeitsplatzrechner	1.124	1.052	760	820	1.058	978
Tablets	84	86	24	40	11	27
Smartphones	322	565	343	468	149	413
	2020					
verwendete spezifische Fachanwendungen	28		32		13	
	2019	**2020**	**2019**	**2020**	**2019**	**2020**
	in Vollbeschäftigungsäquivalenten zum 31. Dezember					
Bedienstete der operativen IKT–Abteilung	34,5[2]	34,5[2]	15,6	15,6	29,5	31,5
	in Mio. EUR					
Aufwand für IKT (Dienstleistungen, Hardware, Software etc.)	5,53	6,84	3,74	4,14	7,12	6,16
IKT–Beschaffungen für das Homeoffice aufgrund der COVID–19–Pandemie	**März bis Juni 2020**					
	in EUR					
Hardware (u.a. Laptops)	419.925		173.793		258.261	
zugehörige Software	67.744		63.698		59.516	

IKT = Informations– und Kommunikationstechnologie

Quellen: BKA; BMDW; BMSGPK

[1] inklusive Familie und Jugend, Kunst und Kultur

[2] zuzüglich von fünf Bediensteten für das Informationssicherheitsmanagement–Team und den Chief Information Security Officer

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von Juni 2020 bis Oktober 2020 ausgewählte Aspekte des Managements der IT–Sicherheit in den Ressorts Bundeskanzleramt (**BKA**), Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (**BMKÖS**), Bundesministerium für Digitalisierung und Wirtschaftsstandort (**BMDW**) und Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (**BMSGPK**).

Der überprüfte Zeitraum umfasste insbesondere die Jahre 2018 bis 2020. Soweit erforderlich, nahm der RH auch auf frühere Entwicklungen Bezug.

(2) Im überprüften Zeitraum änderten sich die Bezeichnung der überprüften Bundesministerien und die Zuordnung der Angelegenheiten durch zwei Novellen des Bundesministeriengesetzes (**BMG**)[1]. Die folgende Tabelle enthält die Namen dieser Bundesministerien und in Klammer die in der Folge vom RH verwendeten Abkürzungen:

Tabelle 1: Bezeichnung der überprüften Bundesministerien im Zeitraum 2018 bis 2020

Bezeichnung laut Bundesministeriengesetz		
bis 7. Jänner 2018	8. Jänner 2018 bis 28. Jänner 2020	29. Jänner 2020 bis 31. Jänner 2021[1]
Bundeskanzleramt (BKA)	Bundeskanzleramt (BKA)	Bundeskanzleramt (BKA)
–	Bundesministerium für öffentlichen Dienst und Sport (BMöDS)	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS)
Bundesministerium für Arbeit, Soziales und Konsumentenschutz (BMASK)	Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz (BMASGK)	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
		Bundesministerium für Arbeit, Familie und Jugend (BMAFJ)
Bundesministerium für Wissenschaft, Forschung und Wirtschaft (BMWFW)	Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW)	Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW)

[1] Mit BGBl. I 30/2021, in Kraft getreten am 1. Februar 2021, wurde die Bezeichnung des Bundesministeriums für Arbeit, Familie und Jugend in Bundesministerium für Arbeit geändert; die Angelegenheiten Familie und Jugend wurden der Bundesministerin für Frauen und Integration im BKA übertragen.

Quelle: RH

[1] BGBl. I 164/2017, in Kraft getreten am 8. Jänner 2018; BGBl. I 8/2020, in Kraft getreten am 29. Jänner 2020

(3) Ziele der Gebarungsüberprüfung waren die Darstellung und Beurteilung der Konzeption und Umsetzung ausgewählter Aspekte des Managements der IT–Sicherheit in den Zentralstellen des BKA, BMKÖS, BMDW und BMSGKP. Dies betraf insbesondere die Themen

- IT–Sicherheitsstrategie,
- IT–Sicherheitsorganisation,
- IT–Sicherheit Personal,
- IT–Sicherheitsmanagement.

Darüber hinaus wurde in diesen Ressorts der im Zusammenhang mit der COVID–19–Pandemie vorgenommene Übergang auf Homeoffice im Hinblick auf die IT–Sicherheit überprüft.

Nicht Thema der Gebarungsüberprüfung waren das Management der IT–Sicherheit in den Dienstleistern (beispielsweise der BRZ GmbH oder der Statistik Austria) der genannten Bundesministerien oder die in diesen Dienstleistern betriebenen Verfahren wie das Unternehmensserviceportal oder das Ergänzungsregister für sonstige Betroffene (TZ 28).

(4) Zu dem im März 2021 übermittelten Prüfungsergebnis nahmen das BKA im Mai 2021, das BMDW und das BMSGPK jeweils im Juni 2021 Stellung.

Das BMKÖS nahm im Juni 2021 von einer Stellungnahme mit der Begründung Abstand, dass der RH keine Beurteilung der IT–Sicherheit im BMKÖS vorgenommen habe. Der RH wies demgegenüber darauf hin, dass er an das BMKÖS sogar zwei Empfehlungen gerichtet hatte: Diese betrafen die Konsolidierung der IT–Ausstattung der Arbeitsplätze und die Gestaltung des Managements der IT und deren Sicherheit in der Weise, dass die grundlegenden Aufgaben der IT–Sicherheit durch das BMKÖS selbst wahrgenommen werden können.

Der RH erstattete seine Gegenäußerungen im September 2021.

IT–Betreuung

Änderung der Ressortkompetenzen

2.1 (1) Die Betreuung der Anwenderinnen und Anwender umfasste insbesondere die IT–Arbeitsplätze, die Fachanwendungen und das Management der IT–Sicherheit.

(a) IT–Ausstattung der Arbeitsplätze

Die IT–Ausstattung der Arbeitsplätze in den Zentralstellen der Bundesministerien setzte sich aus mobilen oder Standgeräten und den dazugehörigen Betriebssystemen, der Bürosoftware (beispielsweise für Textverarbeitung), dem Mailprogramm und dem Browser (Programm zur Darstellung von Websites) zusammen. Das Ressortprinzip ermöglichte es, auch auf diesen generellen Arbeitsplätzen der Verwaltung ressortspezifische IT–Lösungen im Hinblick auf die Infrastruktur und Software einzusetzen. Gemäß dem Bericht IT–Konsolidierung der Österreichischen Bundesregierung (veröffentlicht vom Bundesministerium für Finanzen und BMDW, November 2019) lag in den Zentralstellen der Bundesministerien keine einheitliche IT–Ausstattung der Arbeitsplätze vor.

Die Betreuung der IT–Ausstattung der Arbeitsplätze erfolgte – in jeder Zentralstelle individuell organisiert – durch die jeweils eigene IT–Abteilung, durch die BRZ GmbH oder durch andere externe Dienstleister.

(b) IT–Fachanwendungen

Darüber hinaus setzten die Bundesministerien spezifische[2] IT–Fachanwendungen und spezifische Systeme für die zentrale Infrastruktur (z.B. Datenserver, Applikationsserver, Netz, zentrale Speicher) ein. Die IT–Abteilungen der Zentralstellen spezialisierten sich in der Folge in hohem Maße auf die jeweils in ihrer Zentralstelle konkret vorliegende IT–Ausstattung und IT–Fachanwendungen. Die Betreuung der zentralen IT–Infrastruktur erfolgte – wiederum in jeder Zentralstelle individuell organisiert – durch die jeweils eigene IT–Abteilung, durch die BRZ GmbH oder durch andere externe Dienstleister.

[2] Einheitlich technisch umgesetzt sind die zentral betriebenen Systeme für den elektronischen Akt (**ELAK**), die elektronische Personalverwaltung/–besoldung und die elektronische Haushaltsverrechnung.

(c) Management der IT–Sicherheit

Die IT–Sicherheit der IT–Arbeitsplätze, der IT–Fachanwendungen sowie der IT–Infrastruktur war grundsätzlich durch organisatorische Maßnahmen und Einsatz technischer Systeme im Bundesministerium bzw. durch die externen Dienstleister zu gewährleisten. Die individuelle Gestaltung der IT führte im Allgemeinen auch zu einer individuellen Gestaltung der technischen Maßnahmen und der dafür verwendeten spezifischen Produkte zur Gewährleistung der IT–Sicherheit.

(2) Im Rahmen von Regierungsbildungen bzw. –umbildungen werden auch Kompetenzen zwischen den Bundesministerien verschoben. Tabelle 2 zeigt beispielhaft die 2018 bzw. 2020 vorgenommenen Kompetenzänderungen gemäß dem BMG, um das Ausmaß der Änderungen für alle Ressorts darzustellen. Hierbei werden nur jene Agenden angeführt, die Teile des Namens des Bundesministeriums oder ganze Sektionen betrafen.

Tabelle 2: Beispielhafte Kompetenzänderungen nach dem Bundesministeriengesetz

Kompetenz nach dem Bundesministeriengesetz	Bundesministerium		
	ab 1. Juli 2016	ab 8. Jänner 2018	ab 29. Jänner 2020
Kunst/Kultur	Bundeskanzleramt[1]	Bundeskanzleramt[1]	Kunst, Kultur, öffentlicher Dienst und Sport
Staatliche Verfassung	Bundeskanzleramt	Verfassung, Reformen, Deregulierung und Justiz	Bundeskanzleramt[1]
Regionen (Koordination von Regionalfonds und Regionalpolitik)	Bundeskanzleramt	Nachhaltigkeit und Tourismus	Landwirtschaft, Regionen und Tourismus
Digitalisierung	Bundeskanzleramt	Digitalisierung und Wirtschaftsstandort	Digitalisierung und Wirtschaftsstandort
Öffentlicher Dienst	Bundeskanzleramt	Öffentlicher Dienst und Sport	Kunst, Kultur, öffentlicher Dienst und Sport
Integration	Europa, Integration und Äußeres	Europa, Integration und Äußeres	Bundeskanzleramt[1]
Arbeit	Arbeit, Soziales und Konsumentenschutz	Arbeit, Soziales, Gesundheit und Konsumentenschutz	Arbeit, Familie und Jugend (ab 1. Februar 2021: Arbeit)
Familie und Jugend	Familie und Jugend	Bundeskanzleramt[1]	Arbeit, Familie und Jugend (ab 1. Februar 2021: Bundeskanzleramt[1])
Gesundheit[2]	Gesundheit und Frauen	Arbeit, Soziales, Gesundheit und Konsumentenschutz	Soziales, Gesundheit, Pflege und Konsumentenschutz
Frauen	Gesundheit und Frauen	Bundeskanzleramt[1]	Bundeskanzleramt[1]
Zivildienst	Inneres	Inneres	Landwirtschaft, Regionen und Tourismus
Sport	Landesverteidigung und Sport	Öffentlicher Dienst und Sport	Kunst, Kultur, öffentlicher Dienst und Sport

Kompetenz nach dem Bundesministeriengesetz	Bundesministerium		
	ab 1. Juli 2016	ab 8. Jänner 2018	ab 29. Jänner 2020
Klima– und Umweltschutz[3]	Land– und Forstwirtschaft, Umwelt und Wasserwirtschaft	Nachhaltigkeit und Tourismus	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Post– und Telekommunikationswesen	Verkehr, Innovation und Technologie	Verkehr, Innovation und Technologie	Landwirtschaft, Regionen und Tourismus
Energiewesen	Wissenschaft, Forschung und Wirtschaft	Nachhaltigkeit und Tourismus	Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bergwesen	Wissenschaft, Forschung und Wirtschaft	Nachhaltigkeit und Tourismus	Landwirtschaft, Regionen und Tourismus
Tourismus	Wissenschaft, Forschung und Wirtschaft	Nachhaltigkeit und Tourismus	Landwirtschaft, Regionen und Tourismus
Wissenschaft	Wissenschaft, Forschung und Wirtschaft	Bildung, Wissenschaft und Forschung	Bildung, Wissenschaft und Forschung

[1] Die Kompetenz oblag einer eigenen Kanzleramtsministerin bzw. einem eigenen Kanzleramtsminister. Quelle: BMG
[2] einschließlich Veterinärwesen, Nahrungsmittelkontrolle
[3] einschließlich Abfallwirtschaft und Altlastensanierung, Artenschutz, Natur– und Landschaftsschutz, Schutz vor ionisierenden Strahlen, Giftverkehr

Der Wechsel der jeweiligen Agenden in andere Bundesministerien führte im Allgemeinen auch zu einer Übertragung der dafür zuständigen Organisationseinheiten, der zugehörigen Bediensteten und der IT–Ausstattung der Arbeitsplätze in das neue Ressort[3]. In der Folge wechselte auch die Zuständigkeit der für die IT–Betriebsführung grundsätzlich zuständigen IT–Abteilung vom abgebenden Bundesministerium zum aufnehmenden Bundesministerium.

Die nach dem Wechsel neu zuständige IT–Abteilung stand somit vor der Aufgabe,

1. die IT–Ausstattung der Arbeitsplätze der übernommenen Bediensteten mit jener des aufnehmenden Bundesministeriums zu vereinheitlichen oder innerhalb eines Bundesministeriums unterschiedliche IT–Arbeitsplätze und deren Software parallel zu betreuen,

2. die mit den (übertragenen) Agenden verbundenen IT–Fachanwendungen im neu zuständigen Bundesministerium zu integrieren und die weitere 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.

[3] Die Analyse und Quantifizierung dieses Aufwands war nicht Gegenstand dieser Gebarungsüberprüfung.

4. Alternativ blieben die IT–Ausstattung der Arbeitsplätze, die IT–Fachanwendungen, das Netz und die dazugehörigen IT–Sicherheitsvorkehrungen trotz der Übertragung in das aufnehmende Bundesministerium in der Betreuung der ursprünglich zuständigen IT–Abteilung des abgebenden Bundesministeriums (siehe dazu auch TZ 3).

In den überprüften Ressorts BKA, BMKÖS und BMSGPK war die technische Integration der IT–Systeme der nach der Regierungsbildung im Jänner 2020 neu verteilten Ressortagenden teilweise auch nach neun Monaten noch nicht vollzogen bzw. abgeschlossen (siehe dazu TZ 3).

(3) Gemäß BMG ist das BKA u.a. für Angelegenheiten der strategischen Netz– und Informationssicherheit (gemäß Netz– und Informationssystemsicherheitsgesetz (**NISG**)) zuständig, das BMDW für die Koordination und zusammenfassende Behandlung in Angelegenheiten der Informationstechnologien und für allgemeine Angelegenheiten der Koordination, der Planung und des Einsatzes der automationsunterstützten Datenverarbeitung. Für die ressorteigene IT und IT–Sicherheit war hingegen jedes Bundesministerium selbst verantwortlich; eine Kompetenz zur Koordination der IT–Sicherheit war im BMG nicht ausdrücklich festgelegt.

2.2 Die Verschiebung von Kompetenzen und den damit verbundenen Arbeitsplätzen (inklusive IT–Ausstattung) zwischen den Bundesministerien führt im Allgemeinen aufgrund der organisatorischen, personellen und räumlichen Verschiebungen zu hohem Aufwand in der neu zuständigen IT–Abteilung, um die dazugekommene IT–Ausstattung der Arbeitsplätze, die IT–Fachanwendungen und die IT–Infrastruktur zu integrieren.

Da das Management und die Maßnahmen zur Umsetzung der IT–Sicherheit in hohem Maße ressortspezifisch geprägt waren, machte es die Verschiebung von Kompetenzen zwischen den Bundesministerien und den damit verbundenen Arbeitsplätzen (inklusive IT–Ausstattung) erforderlich, auf die zu übernehmenden IT–Systeme die IT–Sicherheitsstrategie und deren technische Methoden sowie Produkte des aufnehmenden Bundesministeriums anzuwenden. Dies konnte insbesondere in der Phase der Überleitung IT–Sicherheitsrisiken beinhalten, weil innerhalb eines Bundesministeriums parallel unterschiedliche Maßnahmen zur Gewährleistung der IT–Sicherheit anzuwenden sind. Vor diesem Hintergrund verwies der RH auf seine Kritik in TZ 3, wonach auch im September 2020 – neun Monate nach Verschiebung von Ressortkompetenzen in den hier überprüften Bundesministerien (BKA, BMKÖS und BMSGPK) – noch keine ressorteinheitliche IT–Zuständigkeit gegeben war.

Eine Kompetenz zur Koordination der IT–Sicherheit war im BMG nicht ausdrücklich festgelegt.

Vor dem Hintergrund einer kontinuierlichen Sicherstellung bei ressortübergreifender Kompetenzänderung empfahl der RH dem BKA und BMDW, eine Regierungsvorlage zu

erarbeiten, mit der im BMG eine Kompetenz zur Koordination der IT–Sicherheit klar und ausdrücklich festgelegt wird.

2.3 (1) Das BKA teilte dazu in seiner Stellungnahme mit, dass die interne IKT–Sicherheit von jedem Ressort selbstständig wahrzunehmen und diese Verantwortung im BKA laut Geschäftseinteilung der Abteilung I/8 zugeordnet sei. Die ressortübergreifende Koordination der Cybersicherheit sei nicht Gegenstand des Berichts und sei schon im Bundesministeriengesetz 1986 als Kompetenz des BKA enthalten.

(2) Das BMDW begrüßte in seiner Stellungnahme die Ausarbeitung einer Regierungsvorlage, mit der im BMG eine Zuständigkeit zur Koordination der IT–Sicherheit klar und ausdrücklich festgelegt werde. Eine diesbezügliche Zuständigkeit des BMDW sehe es jedoch nicht.

2.4 (1) Der RH entgegnete dem BKA, dass das BMG bisher lediglich die Zuständigkeit des BKA für die Angelegenheiten der strategischen Netz– und Informationssicherheit (gemäß NISG) festlegte. § 4 NISG konkretisierte diese weiter, enthielt jedoch keine ausdrückliche Kompetenz zur Koordination der IT–Sicherheit der Bundesministerien. Der RH hielt daher seine Empfehlung aufrecht.

(2) Dem BMDW entgegnete der RH, dass das BMDW aufgrund seiner Zuständigkeit für die Digitalisierung der Bundesverwaltung aufgerufen war, gemeinsam mit dem BKA einen Vorschlag zur Koordination der IT–Sicherheit zu entwickeln.

Zuständigkeit der IT–Abteilungen/Konsolidierung

3.1 (1) Im Jänner 2020 erfolgte gemäß BMG eine Verschiebung von Kompetenzen zwischen den Bundesministerien und den damit verbundenen Arbeitsplätzen (inklusive IT–Ausstattung). In den von dieser Gebarungsüberprüfung umfassten Bundesministerien betraf die Verschiebung beispielhaft die Agenden Familie und Jugend vom BKA zum damals neuen Bundesministerium für Arbeit, Familie und Jugend (**BMAFJ**), die Agenden Kunst/Kultur vom BKA zum BMKÖS, die Agenden Integration vom Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**) zum BKA, die Agenden Staatliche Verfassung vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz (**BMVRDJ**) zum BKA sowie die Agenden Arbeit vom Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz (**BMASGK**) zum damals neuen BMAFJ.

1. Im BMDW ergab sich im Jänner 2020 keine Änderung der Betreuungsverhältnisse; die IT–Ausstattung der Arbeitsplätze, die IT–Fachanwendungen, das Netz des BMDW und die IT–Sicherheitsvorkehrungen wurden einheitlich von der zugehörigen IT–Abteilung des BMDW (und ihres externen Dienstleisters) betreut.

2. Im BKA ergaben sich 2018 wesentliche Änderungen in der von der IT–Abteilung zu betreuenden Verwaltung durch die Kompetenzverschiebung der Sektionen öffentlicher Dienst in das Bundesministerium für öffentlichen Dienst und Sport (**BMöDS**) und Staatliche Verfassung in das damalige BMVRDJ. Dafür waren nunmehr die Sektionen Familie und Jugend sowie Frauen neu zu unterstützen.

3. 2020 wurden die Sektion Kunst und Kultur vom BKA in das nunmehrige BMKÖS (Nachfolger des BMöDS) und die Sektion Familie und Jugend in das BMAFJ verschoben, hingegen die Sektionen Integration vom BMEIA und Staatliche Verfassung vom Bundesministerium für Justiz (**BMJ**) in das BKA übertragen.

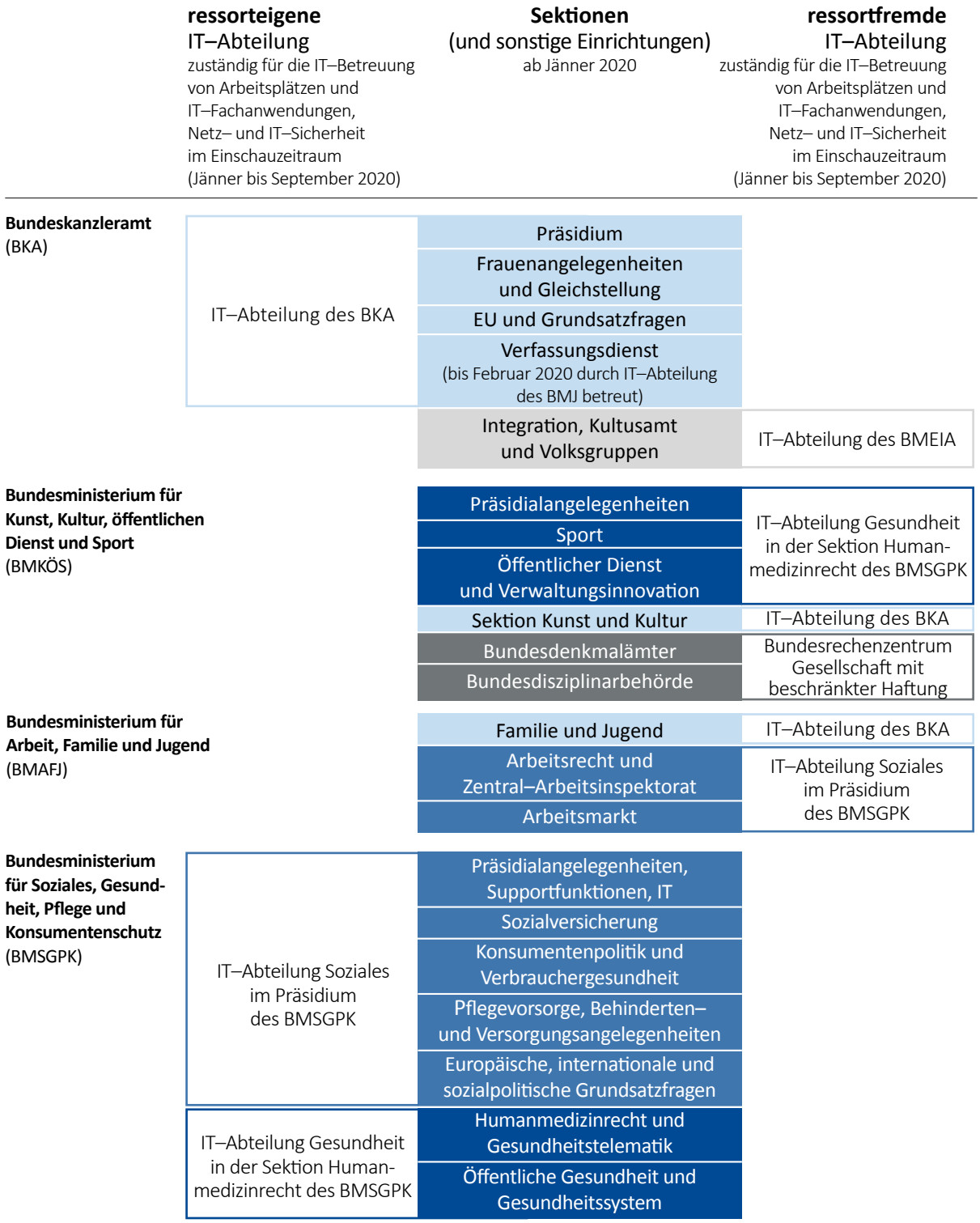
4. Das 2018 neu eingerichtete BMöDS hatte keine eigene IT–Abteilung; daher wurde vereinbart, dass die IT–Abteilung Gesundheit des BMASGK dieses Ressort parallel mitbetreut. Diese operative Betreuung wurde auch nach der Änderung der Kompetenzen 2020 (das BMöDS wurde nach Übernahme der Agenden Kunst und Kultur zum BMKÖS) beibehalten. In der Geschäftseinteilung des BMKÖS war nunmehr auch eine eigene für die IT und IT–Sicherheit zuständige Abteilung als Teil der Sektion I (Präsidium) ausgewiesen. Diese führte auch einzelne Personen der IT–Abteilung Gesundheit des nunmehrigen BMSGPK in der Geschäftseinteilung des BMKÖS an, womit diese Personen in der Geschäftseinteilung von zwei Ressorts vorkamen.

5. Die IT–Abteilung Gesundheitsinformationsmanagement und Gesundheitsinformatik (IT–Abteilung Gesundheit) des BMSGPK ging aus der IT–Abteilung des mit 1. Juli 2016 eingerichteten Bundesministeriums für Gesundheit und Frauen[4] (**BMGF**) hervor und wurde mit der Übertragung der Gesundheitsagenden 2018 in das BMASGK (ab 2020 BMSGPK) verschoben. Dort betreute sie ab 2018 nicht nur die IT–Ausstattung der Arbeitsplätze des Bereichs Gesundheit, sondern auch die zugehörigen sehr spezifischen IT–Fachanwendungen. Die IT–Abteilung Informationstechnologie und –management (in der Folge: **IT–Abteilung Soziales**) war 2018 im BMASGK (bzw. 2020 im BMSGPK) weiterhin für die IT der Agenden Arbeit, Soziales und Konsumentenschutz zuständig; 2020 gingen die Sektionen Arbeitsrecht und Arbeitsmarkt an das damals neue BMAFJ.

   Die Abbildung 1 stellt für das BKA, das BMAFJ, das BMKÖS und das BMSGPK für den Zeitraum Jänner bis September 2020 die Betreuung einzelner Sektionen durch verschiedene IT–Abteilungen dar. Die in den letzten Jahren mehrfachen Kompetenzänderungen und damit verbundenen Verschiebungen von Sektionen in ein anderes Ressort zeigten sich anhand der die Sektionen in diesem Zeitraum jeweils noch betreuenden IT–Abteilungen.

[4] bis 30. Juni 2016 Bundesministerium für Gesundheit; BGBl. I 49/2016

Abbildung 1: Zuständigkeiten der IT–Abteilungen betreffend BKA, BMAFJ, BMKÖS und BMSGPK (Jänner bis September 2020)



Quellen: BKA; BMKÖS; BMDW; BMSGPK; Darstellung: RH

Obwohl die Verschiebung von Kompetenzen zwischen den Bundesministerien und den damit verbundenen Arbeitsplätzen (inklusive IT–Ausstattung) in den Ressorts im Jänner 2020 erfolgte, waren im September 2020 in den Ressorts BKA, BMKÖS und BMSGPK noch unterschiedliche IT–Abteilungen in ein und derselben Zentralstelle tätig.

Darüber hinaus erfolgte die IT–Betreuung der im BMAFJ eingegliederten drei Sektionen (Familie und Jugend; Arbeitsrecht; Arbeitsmarkt) auch im September 2020 noch durch die IT–Abteilungen des BKA bzw. BMSGPK (im BMAFJ war zwar eine IT–Abteilung systemisiert, es waren im September 2020 laut Geschäftsverteilung jedoch erst zwei Arbeitsplätze eingerichtet). Die Bundesministeriengesetz–Novelle 2021 brachte eine neuerliche Verschiebung der Agenden Familie und Jugend in das BKA.

(2) Das IKT–Konsolidierungsgesetz[5] schuf 2012 die Grundlage für die Vereinheitlichung bestehender und neuer IKT–Lösungen des Bundes.[6] Das IKT–Konsolidierungsgesetz sah dazu vor, dass nähere Festlegungen durch eine Verordnung getroffen werden sollten. Diese Verordnung fehlte jedoch zur Zeit der Gebarungsüberprüfung; die Zuständigkeit hierfür oblag bis 2017 dem BKA, ab 2018 dem BMDW.

2018 hatte die Bundesregierung mit den Projekten der Konferenz der Generalsekretäre weitere Konsolidierungsmaßnahmen eingeleitet, welche die IT–Arbeitsplätze, die Arbeitsplatzsoftware, die zentrale Infrastruktur, die IT–Anwendungen und IT–Verfahren umfassen sollten. Der dazu im November 2019 vorgelegte Statusbericht zeigte die Heterogenität der IT–Ausstattung der Arbeitsplätze, Rechenzentren, IT–Verfahren und IT–Anwendungen im Bund auf und enthielt Vorschläge zur IT–Konsolidierung. Auch der zum Statusbericht gefasste Beschluss der Bundesregierung im November 2019 unterstützte die Umsetzung von Konsolidierungsmaßnahmen.

3.2 Der RH stellte kritisch fest, dass im September 2020 und damit neun Monate nach Verschiebung von Ressortkompetenzen in den Bundesministerien BKA, BMKÖS und BMSGPK noch keine ressorteinheitliche IT–Zuständigkeit gegeben war.

Weiters stellte er kritisch fest, dass die im IKT–Konsolidierungsgesetz von 2012 vorgesehene Verordnung zur Konsolidierung der Heterogenität der IT–Systeme im Jahr 2020 noch nicht vorlag.

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

[6] 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, die duale Zustellung, elektronische Signaturen, das Identity– und Accessmanagement (Rechte– und Rollenverwaltung), der ELAK, Softwarebausteine bzw. Softwarebibliotheken sowie Basiskomponenten (z.B. Scanning).

Der RH empfahl dem BMDW, im Einvernehmen mit dem BKA die im IKT–Konsolidierungsgesetz vorgesehene Verordnung zu erlassen.

Weiters empfahl der RH dem BKA, BMDW, BMSGPK und dem BMKÖS, jeweils in einem Projekt die Konsolidierung der IT–Ausstattung der Arbeitsplätze des Ressorts zu behandeln, um die Kosten der IT–Beschaffung und der Lizenzgebühren zu reduzieren, die Heterogenität der generellen Bürosoftwareausstattung zu verringern und die Betreuung der IT–Ausstattung der Arbeitsplätze zu bündeln. Die Verwendung einheitlicher Bürosoftware sowie die einheitliche und zeitgerechte Installierung der zugehörigen Sicherheits–Updates ermöglichen auch die Bündelung des für die IT–Sicherheit zuständigen Personals und können einen Beitrag zur Erhöhung der IT–Sicherheit leisten.

3.3 (1) Zu den im IKT–Konsolidierungsgesetz vorgesehenen Verordnungen teilte das BMDW in seiner Stellungnahme mit, dass die Notwendigkeit und die entsprechende Erarbeitung und Erlassung von Verordnungen im Programm IT–Konsolidierung pro Projekt gesondert bewertet und bei Bedarf empfohlen würden. Aktuell befinde sich die Verordnung zum Bundes–CMS (Content Management System) in Umsetzung.

Zur Konsolidierung der IT–Ausstattung der Arbeitsplätze sei das Projekt „Standardarbeitsplatz des Bundes (STAB)“ im Rahmen der IT–Konsolidierung initiiert worden. Ein entsprechendes Konzeptionsprojekt solle im 3. Quartal 2021 begonnen werden.

(2) Zur Konsolidierung der IT–Ausstattung der Arbeitsplätze der Ressorts teilte das BKA in seiner Stellungnahme mit, dass diese Empfehlungen bereits im Rahmen des Programms „IT–Konsolidierung“ bearbeitet würden.

(3) Das BMSGPK teilte in seiner Stellungnahme mit, dass es im Ressort die interministeriellen Vereinbarungen für den Bundesclient, die auch die wesentlichen Elemente der Bürosoftwareausstattung regeln, umgesetzt habe.

Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport

4.1 (1) Im Jänner 2018 (BGBl. I 164/2017) wurde das Bundesministerium für öffentlichen Dienst und Sport (BMöDS) gegründet. Es setzte sich aus Teilen der vormaligen Ressorts BKA (Sektion Öffentlicher Dienst und Verwaltungsinnovation), Bundesministerium für Landesverteidigung und Sport (Sektion Sport) und Bundesministerium für Gesundheit und Frauen (Präsidium) zusammen. Im Jänner 2020 (BGBl. I 8/2020) wurde das Bundesministerium um die Sektion Kunst und Kultur (vormals im BKA) erweitert und in Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport umbenannt. Die operative Betriebsführung der IT des BMöDS (nunmehr BMKÖS) oblag der IT–Abteilung Gesundheit des BMASGK (nunmehr BMSGPK) auf Grundlage eines Verwaltungsübereinkommens.

Laut Geschäftseinteilung des BMKÖS war die Abteilung I/3 Rechtskoordination, Informations–, Organisations– und Verwaltungsmanagement u.a. für die IT–Sicherheit, die IKT–Infrastruktur und den IKT–Betrieb zuständig. In der Geschäftseinteilung des BMKÖS war dazu vermerkt, dass diese Aufgaben durch den Leiter und weitere elf in der Geschäftseinteilung namentlich angeführte Bedienstete der IT–Abteilung Gesundheit des BMSGPK durchgeführt wurden. Damit war die IT–Abteilung Gesundheit einerseits für die IT–Sicherheit und den IKT–Betrieb im Bereich Gesundheit im BMSGPK zuständig und andererseits auch für den operativen Betrieb der IT des BMKÖS tätig.

(2) Die IT–Abteilung Gesundheit des BMSGPK war für die technisch–organisatorischen Angelegenheiten der Zusammenarbeit mit nationalen und internationalen Gesundheitsbehörden und –organisationen sowie für IKT–Angelegenheiten, –Infrastruktur, –Betrieb und –Beschaffung für den Bereich Gesundheit verantwortlich. Daher hatte sie wegen der COVID–19–Pandemie besondere technische, organisatorische und personelle Herausforderungen zu bewältigen. Infolge dieser konnte sie nach ihren Angaben während der Gebarungsüberprüfung keine Ausarbeitungen bzw. umfassenden Unterlagen und Daten zur IT–Sicherheit im BMKÖS zur Verfügung stellen. Die Beantwortung der vom RH übermittelten Fragebögen sowie die Erstellung weiterer für diese Gebarungsüberprüfung relevanter Ausarbeitungen für den Wirkungsbereich des BMKÖS waren ihr (faktisch) nicht möglich.

Im BMKÖS lagen auch im Oktober 2020 noch keine eigenen grundlegenden Dokumente betreffend das Management der IT–Sicherheit, etwa zu den Themen IT–Strategie, –Risikomanagement, –Berichtswesen und –Organisation, vor, obwohl dieses Bundesministerium im Wesentlichen im Jänner 2018 eingerichtet worden war. Diesbezüglich verwies das BMKÖS lediglich auf Schriftsätze und Konzepte der IT–Abteilung Gesundheit des BMSGPK, die allerdings den Bereich Gesundheit betrafen.

4.2 Der RH hielt kritisch fest, dass das BMKÖS keine eigenen grundlegenden Dokumente zum Management der IT–Sicherheit vorlegen konnte, sondern lediglich auf Schriftsätze und Konzepte der IT–Abteilung Gesundheit für den Bereich Gesundheit im BMSGPK verwies. Er kritisierte daher, dass das BMöDS es seit 2018 bzw. das BMKÖS es seit 2020 verabsäumt hatte, jene grundsätzlichen strategischen, organisatorischen und strukturellen Festlegungen zu treffen und zu dokumentieren, die für ein ordnungsgemäßes Management der IT–Sicherheit wesentlich waren.

Er wies in diesem Zusammenhang darauf hin, dass die Verantwortung für die IT–Sicherheit, die IKT–Infrastruktur und den IKT–Betrieb des BMöDS bzw. nunmehr BMKÖS trotz des mit dem BMASGK (nunmehr BMSGPK) geschlossenen Verwaltungsübereinkommens bei der Abteilung I/3 (Rechtskoordination, Informations–, Organisations– und Verwaltungsmanagement) des nunmehrigen BMKÖS lag.

Der RH wies auch darauf hin, dass der IT–Abteilung Gesundheit des BMSGPK aufgrund ihrer Aufgaben im Zusammenhang mit der Bewältigung der COVID–19–Pandemie die Beantwortung der vom RH übermittelten Fragebögen sowie die Erstellung weiterer für diese Gebarungsüberprüfung relevanter Ausarbeitungen und Unterlagen für den Wirkungsbereich des BMKÖS faktisch nicht möglich war.

Der RH nahm daher von einer Beurteilung der IT–Sicherheit im BMKÖS Abstand, wird aber im Rahmen einer Follow–up–Überprüfung diese Aspekte überprüfen. Der RH verkannte nicht die Vorteile der Nutzung von Verwaltungsübereinkommen für den ressortübergreifenden Betrieb der IT in der ersten Phase der Einrichtung eines neuen Bundesministeriums. Er beurteilte allerdings die nationalen und internationalen Aufgaben der IT–Abteilung Gesundheit – nicht nur zur Betreuung der IT–Systeme zur Erfassung und Dokumentation der COVID–19–Pandemie, sondern grundsätzlich – als sehr wichtig und ressourcenbindend. Die zusätzliche Betreuung des BMKÖS durch die IT–Abteilung Gesundheit war aufgrund der Doppelbelastung für beide Bundesministerien nachteilig und brachte das Risiko eines nicht ausreichenden Managements der IT–Sicherheit des BMKÖS mit sich.

Der RH empfahl dem BMKÖS daher, das Management der IT und deren Sicherheit so zu gestalten, dass die grundlegenden Aufgaben der IT–Sicherheit vom Ressort selbst wahrgenommen werden können.

Grundlagen der IT–Sicherheit

Technische Vorgaben

5.1 Im März 2013 beschloss die Bundesregierung die „Österreichische Strategie für Cyber Sicherheit“ (in der Folge: **Cybersicherheitsstrategie**) unter Federführung des BKA. Diese verfolgte u.a. das Ziel, durch einen „gesamtstaatlichen Ansatz der zuständigen Bundesministerien“ sicherzustellen, dass „die nationalen IKT–Infrastrukturen sicher und resilient gegen Gefährdungen“ sind. Dazu definierte sie unterschiedliche Handlungsfelder, welche auch die Festlegung von Mindestsicherheitsstandards für die IT enthielten. Diese wurden im Österreichischen Informationssicherheitshandbuch (in der Folge: **Informationssicherheitshandbuch**) zusammengefasst. Das Informationssicherheitshandbuch war online abrufbar und wurde laufend aktualisiert. Es enthielt Vorgaben, Standards und Leitlinien hinsichtlich strategischer Ansätze, Risikoanalysen, Organisation, Telearbeit, Verhalten von Mitarbeiterinnen und Mitarbeitern, Klassifikation von Informationen, Sicherheit von Datenträgern etc. Diese waren als Handlungsanleitung für Unternehmen und die öffentliche Verwaltung zur sicheren Gestaltung der IT zu verstehen. Das Informationssicherheitshandbuch setzte daher primär Standards im Sinne technischer und organisatorischer Sicherheitsmaßnahmen innerhalb eines spezifischen Rechtsträgers.

Das Regierungsprogramm 2020–2024 sah neben der Aktualisierung der Cybersicherheitsstrategie auch einheitliche Sicherheitsstandards für die IKT der öffentlichen Verwaltung vor. Das BKA teilte hierzu mit, dass die Aktualisierung der Cybersicherheitsstrategie voraussichtlich bis zum Ende des Jahres 2020 abgeschlossen sein werde.

5.2 Der RH stellte fest, dass eine Cybersicherheitsstrategie zwar bereits 2013 ausgearbeitet, jedoch zur Zeit der Gebarungsüberprüfung noch nicht aktualisiert war. Der RH hielt fest, dass mit dem auf der Cybersicherheitsstrategie beruhenden Informationssicherheitshandbuch Standards auch in Bezug auf die IT–Sicherheit festgelegt wurden. Nachdem die Cybersicherheitsstrategie von den einzelnen Mitgliedern der Bundesregierung beschlossen worden war, erachtete der RH auch die sich darauf gründenden Sicherheitsstandards des Informationssicherheitshandbuchs als für die einzelnen Bundesministerien von besonderer Relevanz. Aus Sicht des RH hatten daher auch die Mitglieder der Bundesregierung die Umsetzung dieser Sicherheitsstandards in ihrem jeweiligen Wirkungsbereich sicherzustellen. Ausgewählte Aspekte dieser Standards zog der RH im Rahmen der gegenständlichen Gebarungsüberprüfung daher als Maßstab für den Vergleich der in den Bundesministerien eingesetzten Maßnahmen des Managements der IT–Sicherheit heran.

Der RH empfahl dem BKA, in der geplanten neuen „Österreichischen Strategie für Cyber Sicherheit“ auch die Standards in Bezug auf die IT–Sicherheit festzulegen.

5.3 Das BKA teilte in seiner Stellungnahme dazu mit, dass die Festlegung der Standards bereits im Rahmen der Koordination zum Entwurf der geplanten neuen „Österreichischen Strategie für Cyber Sicherheit“ vorgesehen sei. Ebenso werde im Rahmen der Zusammenarbeit der Generalsekretärinnen und Generalsekretäre (der Bundesministerien) ein derartiges Projekt vorangetrieben, um „Cyber Sicherheit Leitlinien“ zu erstellen.

Rechtliche Vorgaben

6.1 Für die IT–Sicherheit in den überprüften Bundesministerien waren das Netz– und Informationssystemsicherheitsgesetz (**NISG**; BGBl. I 111/2018), die Datenschutz–Grundverordnung (**DSGVO**; ABl. L 2016/119, 1), das Informationssicherheitsgesetz (**InfoSiG**; BGBl. I 23/2002 i.d.g.F.) mit der Informationssicherheitsverordnung (**InfoSiV**; BGBl. II 548/2003 i.d.g.F.) und die Geheimschutzordnung des Bundes wesentlich:

(1) Das NISG trat am 29. Dezember 2018 in Umsetzung einer Richtlinie (EU 2016/1148 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz– und Informationssystemen in der Union, ABl. L 2016/194) der EU in Kraft. Mit diesem Bundesgesetz wurden Maßnahmen festgelegt, mit denen ein hohes Sicherheitsniveau von Netz– und Informationssystemen

- in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur,
- von Anbietern digitaler Dienste und
- wichtiger Dienste bei Einrichtungen der öffentlichen Verwaltung

erreicht werden soll.

Die Bundesministerien haben daher für die von ihnen betriebenen wichtigen Dienste geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein (§ 22 NISG) (TZ 8 und TZ 23).

(2) Gemäß der DSGVO ist bei der Verarbeitung personenbezogener Daten ein angemessenes Sicherheitsniveau durch geeignete technische und organisatorische Maßnahmen zu gewährleisten (Art. 5 Abs. 1 lit. f und Art. 32 DSGVO). Das BKA, das BMDW und das BMSGPK setzten diese Datensicherheitsvorgaben einerseits durch entsprechende organisatorische und personelle Maßnahmen, andererseits durch technische Sicherheitsmaßnahmen um. Organisatorisch richteten sie für die IT– und Datensicherheit verantwortliche Stellen (z.B. Betrauung von Datenschutzbeauftragten, Informationssicherheitsbeauftragten) bzw. Organisationseinheiten ein. Personelle

Maßnahmen betrafen z.B. Schulungen der Bediensteten. Technische Sicherheitsmaßnahmen dienten insbesondere dem Schutz der personenbezogene Daten verarbeitenden IT–Systeme.

(3) Das InfoSiG und die InfoSiV regelten den Umgang mit Informationen, die einer besonderen Geheimhaltung unterliegen (klassifizierte Informationen: „eingeschränkt", „vertraulich", „geheim" und „streng geheim") und die Österreich im Einklang mit völkerrechtlichen Regelungen erhält („internationaler Geheimschutz"). Nach dem InfoSiG war in jedem Bundesministerium ein Informationssicherheitsbeauftragter zu betrauen. Überdies war die Informationssicherheitskommission – unter dem Vorsitz des Informationssicherheitsbeauftragten des BKA – einzurichten, der die Informationssicherheitsbeauftragten aller Bundesministerien angehörten. Ihre Aufgabe war u.a., auf die „bundesweite Einheitlichkeit von Schutzmaßnahmen und deren Koordination im Bereich der Bundesverwaltung hinzuwirken" und regelmäßig an die Bundesregierung zu berichten (§ 8 Abs. 1 InfoSiG).

(4) Der Umgang mit klassifizierten Informationen außerhalb des Anwendungsbereichs des InfoSiG („nationaler Geheimschutz") war in der Geheimschutzordnung des Bundes geregelt. Diese war im Gegensatz zum InfoSiG und zur InfoSiV nicht im Bundesgesetzblatt kundgemacht, sondern war ein – nicht öffentlich zugänglicher – Beschluss des Ministerrats vom Jänner 2008.

Beide Regelungskomplexe – der internationale wie der nationale Geheimschutz – geben neben Klassifizierungsstufen auf Basis des Amtsgeheimnisses und des Schädigungsrisikos auch – teilweise unterschiedliche – Regelungen zur elektronischen Verarbeitung klassifizierter Informationen vor. So durften etwa Informationen ab der Klassifizierungsstufe „vertraulich" im Bereich des internationalen Geheimschutzes nur auf von der Informationssicherheitskommission akkreditierten IT–Systemen verarbeitet werden (§ 9 Abs. 2 InfoSiV). Im Bereich des nationalen Geheimschutzes war auf Grundlage der Geheimschutzordnung des Bundes eine solche Akkreditierung dagegen nicht vorgesehen.

Die Informationssicherheitskommission befasste sich in ihrem Bericht zur strategischen Neuausrichtung in der Informationssicherheit an die Bundesregierung im Juli 2020 mit den historisch gewachsenen Geheimschutzsystemen des InfoSiG und der Geheimschutzordnung des Bundes. Sie wies darauf hin, dass das InfoSiG nur für die Dienststellen des Bundes, jedoch nicht für jene der Länder galt und umfangreiche Ausnahmen von den Voraussetzungen für den Zugang zu klassifizierten Informationen vorsah. Außerdem hielt sie fest, dass die Geheimschutzordnung des Bundes lediglich für die Zentralstellen der Bundesministerien galt und als Beschluss des Ministerrats hinsichtlich ihrer rechtlichen Qualifikation „schwach abgesichert" war. Die Informationssicherheitskommission kam daher u.a. zu dem Schluss, dass die

Regelungen zum österreichischen Geheimschutzsystem lückenhaft und inkohärent seien, was wiederum ein systemimmanentes Sicherheitsrisiko nach sich ziehe.

6.2 Der RH verwies auf den Bericht der Informationssicherheitskommission zur strategischen Neuausrichtung in der Informationssicherheit und die darin enthaltenen Feststellungen zu den rechtlichen Grundlagen des internationalen und nationalen Geheimschutzes in Österreich. In diesem Zusammenhang erachtete der RH insbesondere die Harmonisierung der verschiedenen rechtlichen Grundlagen (InfoSiG und Geheimschutzordnung des Bundes) als wesentlich für eine strategische Neuausrichtung in der Informationssicherheit zur Reduzierung der von der Informationssicherheitskommission identifizierten Sicherheitsrisiken.

Der RH empfahl daher dem BKA, eine Regierungsvorlage zu erarbeiten, welche ein einheitliches Regelungssystem zur elektronischen Verarbeitung klassifizierter Informationen für den internationalen und nationalen Geheimschutz schafft.

6.3 Das BKA teilte in seiner Stellungnahme mit, dass ein einheitliches Regelungssystem zur elektronischen Verarbeitung klassifizierter Informationen für den internationalen und nationalen Geheimschutz im Zuge der bereits im Ministerrat angekündigten Geheimschutzreform (Ausarbeitung eines „InfoSiG neu“ im Rahmen der Informationssicherheitskommission) in Bearbeitung sei.

IT–Sicherheitsstrategien der überprüften Bundesministerien

7.1 (1) Die in der Cybersicherheitsstrategie und im Informationssicherheitshandbuch verankerte IT–Sicherheitsstrategie ist die Grundlage des IT–Sicherheitsmanagements und definiert u.a. dessen Ziele, Verantwortlichkeiten und Methoden. Eine solche Strategie soll allgemeine Festlegungen treffen, um den Schutz der IT–Systeme innerhalb einer Organisation zu gewährleisten. Sie soll außerdem die Verantwortlichkeiten in der IT–Sicherheitsorganisation eines Bundesministeriums und der Bediensteten festlegen und sicherstellen, dass die Ressortleitung das IT–Sicherheitsmanagement ausreichend unterstützt („Management Commitment“). Die IT–Sicherheitsstrategie ist transparent in Kraft zu setzen, damit auch das Personal entsprechende Kenntnis über deren – wichtigste – Inhalte erlangt.

Für eine IT–Sicherheitsstrategie waren daher die Festlegung klarer Ziele und Verantwortlichkeiten (Ressortleitung, Organisation, Personal) sowie ihre Nachvollziehbarkeit (insbesondere für die betroffenen Bediensteten) jedenfalls erfolgskritisch. Die

IT–Sicherheitsstrategien der überprüften Bundesministerien erfüllten diese Kriterien wie folgt:

Tabelle 3: IT–Sicherheitsstrategien

Thema	BKA	BMDW	BMSGPK
IT–Sicherheitsstrategie vorhanden	ja, aus 2020	ja, aus 2014, aktualisiert 2016	ja, aus 2017, aktualisiert 2018
Bezeichnung	„Leitlinie IKT–Sicherheit im Bundeskanzleramt“	„Grundsätze zur Informationssicherheitspolitik“	„Grundsätze zur umfassenden IT–Sicherheitspolitik“
Erfassung des nachgeordneten Bereichs	ja	teilweise	ja
unterzeichnet von	Generalsekretär	oberstem Organ	oberstem Organ
Kundmachung mit Rundschreiben	nein	ja	ja
wesentliche Ziele der IT–Sicherheitsstrategie	Vertraulichkeit, Integrität, Verfügbarkeit, Risikomanagement, Mängelerkennung und –behebung	Vertraulichkeit, Integrität und Verfügbarkeit, Risikomanagement, Legal Compliance, Schadensvermeidung, Mängelerkennung und –behebung, Ansehenswahrung, Mitarbeitersensibilisierung, Kontinuitätswahrung	Vertraulichkeit, Integrität und Verfügbarkeit, Legal Compliance, Ansehenswahrung, Sensibilisierung, Notfallvorsorge
Verantwortlichkeit oberstes Organ	nicht festgelegt	festgelegt	festgelegt
Berücksichtigung von Organisation und Personal	ja	ja	ja
Nachvollziehbarkeit der Maßnahmen	ja, z.B. risikoorientierte Sicherheitsmaßnahmen, Notfall– und Krisenmanagement, Schulung	ja, z.B. risikoorientierte Sicherheitsmaßnahmen, Notfall– und Krisenmanagement, Schulung	ja, z.B. risikoorientierte Sicherheitsmaßnahmen, Notfall– und Krisenmanagement, Schulung

IKT = Informations– und Kommunikationstechnologie

Quellen: BKA; BMDW; BMSGPK

(2) Zu den IT–Sicherheitsstrategien in den überprüften Bundesministerien war im Besonderen festzuhalten:

(a) Der Generalsekretär im BKA beauftragte im Mai 2020 – nach Beginn der gegenständlichen Gebarungsüberprüfung – das Projekt „Stärkung der Cyberabwehrfähigkeiten im BKA“. Ziel dieses Projekts war die Einrichtung eines umfassenden Informationssicherheitsmanagement–Systems für das BKA. Mit dem Projekt sollten u.a. ein System zur Bewältigung von Sicherheitsvorfällen und ein Risikomanagementsystem eingeführt sowie die Anforderungen nach dem NISG umgesetzt werden. Das Projektende war mit dem 2. Quartal 2022 festgelegt; der Großteil der Projektziele sollte im 1. Quartal 2021 erreicht werden, die Einführung des Risikomanagementsystems war bis zum Projektabschluss im 2. Quartal 2022 vorgesehen.

Eines der ersten Ergebnisse dieses Projekts war die strategische Leitlinie „IKT–Sicherheit im Bundeskanzleramt“ vom Juli 2020. Das BKA brachte diese Leitlinie nicht allen Bediensteten aktiv (etwa in Form eines Rundschreibens) zur Kenntnis, sondern stellte sie im Intranet zur Verfügung. Sie wurde außerdem den Führungskräften der für die Informationstechnologie zuständigen Gruppe (Gruppe I/C: IT–Personalmanagement; IKT–Sicherheit; IKT–Infrastruktur) als Weisung, alle künftigen Managemententscheidungen leitlinienkonform zu treffen, übermittelt. Das BKA beabsichtigte, die Leitlinie im Zuge des Projekts „Stärkung der Cyberabwehrfähigkeiten im BKA“ durch eine „Leitlinie Informationssicherheit“ zu ersetzen und diese zentral allen Bediensteten zur Verfügung zu stellen.

Die aktuelle Leitlinie legte neben der Verantwortung des IKT–Betriebs und der für Cybersicherheit zuständigen Abteilung zur Sicherung des „Management Commitments“ auch jene „der strategischen Führungsebene“ fest. Der Begriff der „strategischen Führungsebene“ war in der Leitlinie selbst jedoch nicht definiert. Das BKA teilte dazu mit, dass darunter der Generalsekretär im BKA zu verstehen sei und begründete dies mit seiner besonderen organisatorischen Stellung als einzigem Amtsträger im BKA, der (in allen Angelegenheiten) Vorgesetzter aller Bediensteten des Ressorts war.

(b) Im BMDW galten seit 2004 „Grundsätze zur Informationssicherheitspolitik“. Diese strategische Richtlinie wurde zuletzt 2016 (durch den damaligen Bundesminister für Wissenschaft, Forschung und Wirtschaft) aktualisiert. Sie bezog sich auf den Verwaltungsbereich Wirtschaft und dessen nachgeordneten Bereich; das waren die Bundeswettbewerbsbehörde, die Burghauptmannschaft Österreich, die Beschussämter (Wien und Ferlach) und die Bundesmobilienverwaltung, mit Ausnahme des Bundesamts für Eich– und Vermessungswesen.

Die 2018 gegründete Sektion I „Digitalisierung und E–Government“ im BMDW, der das Personal und die Kompetenzen vom BKA und Bundesministerium für Finanzen (**BMF**) übertragen waren, war daher nicht ausdrücklich vom Geltungsbereich der Richtlinie erfasst[7]. Das BMDW teilte im Rahmen der Gebarungsüberprüfung mit, dass nunmehr die „Grundsätze zur Informationssicherheitspolitik“ überarbeitet, den aktuellen organisatorischen Rahmenbedingungen angepasst und auch das Bundesamt für Eich– und Vermessungswesen miteinbezogen werde.

(c) Im BMSGPK galten seit 2017 eigene „Grundsätze zur umfassenden IT–Sicherheitspolitik“, die 2018 aktualisiert und von der damaligen Bundesministerin mittels Rundschreiben kundgemacht bzw. erlassen wurden. Sie galten auch für das Sozialministeriumservice und damit für den gesamten nachgeordneten Bereich.

[7] Laut Mitteilung des BMDW umfasste jedoch der „Verwaltungsbereich Wirtschaft“ jedenfalls die gesamte Zentralstelle des BMDW. In der Sektion I wurden außerdem mit einem „Handbuch zum Management der IT–/Informationssicherheit und des Datenschutzes“ organisatorische Rahmenbedingungen und Arbeitsanweisungen zur IT–Sicherheit festgelegt.

7.2 Der RH anerkannte grundsätzlich, dass das BKA, das BMDW und das BMSGPK über IT–Sicherheitsstrategien verfügten, diese Strategien die wesentlichen, für eine umfassende IT–Sicherheit relevanten Ziele verfolgten, die darin festgelegten Maßnahmen nachvollziehbar waren und organisatorische und personelle Aspekte berücksichtigten.

Der RH hielt jedoch fest, dass das BKA seine IT–Sicherheitsstrategie nicht allen Bediensteten aktiv – etwa in Form eines internen Rundschreibens – zur Kenntnis gebracht hatte und diese auch keine Ausführungen zur Verantwortung der obersten Führungsebene für die IT–Sicherheit enthielt. Aus Sicht des RH würden eine erhöhte Transparenz und ein erhöhtes „Management Commitment" einen Beitrag dazu leisten, die Akzeptanz und den Umsetzungserfolg der IT–Sicherheitsstrategie zu steigern.

Der RH empfahl daher dem BKA, in seiner IT–Sicherheitsstrategie auch die Verantwortung der obersten Führungsebene für die IT–Sicherheit zu definieren und die IT–Sicherheitsstrategie allen Bediensteten aktiv kundzumachen.

Der RH wies darauf hin, dass die IT–Sicherheitsstrategie des BMDW zuletzt 2016 aktualisiert wurde. Damit war die (erst 2018 gegründete) Sektion I „Digitalisierung und E–Government" nicht ausdrücklich und auch das Bundesamt für Eich– und Vermessungswesen nicht von deren Geltungsbereich erfasst.

Der RH empfahl dem BMDW, seine IT–Sicherheitsstrategie zu aktualisieren, ihren Geltungsbereich umfassend festzulegen und alle nachgeordneten Dienststellen miteinzubeziehen.

7.3 (1) Laut Stellungnahme des BKA befinde sich die Empfehlung im Rahmen des internen „Information Security Management System"–Projekts bereits in Umsetzung.

(2) Das BMDW teilte in seiner Stellungnahme mit, dass zum Zwecke der Aktualisierung der IT–Sicherheitsstrategie eine Reorganisation im Bereich der Informationssicherheit des BMDW in Umsetzung sei. Die Rolle des Chief Information Security Officers (CISO) mit der Aufgabe, das Informationssicherheitsmanagement–Team zu leiten, werde im BMDW eingerichtet. Diese Funktion werde in der in Überarbeitung befindlichen Informationssicherheitspolitik verankert, deren Geltungsbereich alle nachgeordneten Dienststellen umfassen solle. In der Konferenz der Generalsekretäre bzw. in der Runde der Chief Digital Officer sei das Dokument „Der CISO im Bundesministerium – Rollenbeschreibung, Anforderungen, Befugnisse" ausgearbeitet worden und befinde sich zur Zeit der Stellungnahme in finaler Abstimmung.

Management von IT–Sicherheitsrisiken

8.1 (1) Für das Management von IT–Sicherheitsrisiken stellt das Informationssicherheitshandbuch (Punkt 4) unterschiedliche Ansätze dar:

- Es wird für alle IT–Systeme eine detaillierte Risikoanalyse durchgeführt, die als Basis für konkrete Sicherheitsmaßnahmen dient. Dieser Ansatz führt zu effektiven und angemessenen Sicherheitsmaßnahmen, ist jedoch kosten– und zeitaufwendig.
- Der Grundschutzansatz geht unabhängig vom tatsächlichen Schutzbedarf von einer pauschalen Gefährdung für alle IT–Systeme aus. Als Sicherheitsmaßnahmen kommen dann (personelle, organisatorische und technische) Grundschutzmaßnahmen zum Einsatz. Dieser Ansatz ist grundsätzlich ressourcenschonend, allerdings besteht das Risiko, dass einzelne IT–Systeme zu wenig geschützt werden.
- Im kombinierten Ansatz wird in einem ersten Schritt der Schutzbedarf für die einzelnen IT–Systeme ermittelt. Jene Systeme mit einem niedrigen oder mittleren Schutzbedarf werden mit Grundschutzmaßnahmen abgesichert. Für jene mit einem hohen oder sehr hohen Schutzbedarf wird eine detaillierte Risikoanalyse durchgeführt, auf deren Basis individuelle – weitere – Schutzmaßnahmen getroffen werden. Damit können alle Systeme mit hohem Schutzbedarf wirksam und angemessen geschützt und Maßnahmen für die anderen Systeme mithilfe des Grundschutzes schnell implementiert werden.

  Das NISG (§ 22) verfolgt einen abgestuften Ansatz, wonach die Bundesministerien für wichtige Dienste risikoorientierte, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen haben. Die Identifizierung wichtiger Dienste setzt daher eine Analyse sämtlicher in einem Bundesministerium betriebener Dienste bzw. IT–Systeme voraus.

  Die IT–Sicherheitsstrategien des BKA, des BMDW und des BMSGPK legten für das Management von IT–Sicherheitsrisiken den kombinierten Ansatz fest.

Die weitere Systematik zum Management von IT–Sicherheitsrisiken in den überprüften Bundesministerien stellte sich wie folgt dar:

Tabelle 4: Systematik des Managements von IT–Sicherheitsrisiken

Thema	BKA	BMDW	BMSGPK
strategische Verankerung	ja	ja	ja
Ansatz	kombinierter Ansatz	kombinierter Ansatz	kombinierter Ansatz
Schutzbedarfs– und Risikoanalysen	teilweise	teilweise	ja
Definition wichtiger Dienste gemäß NISG	ja, 13 Dienste	ja, 14 Dienste	ja, 21 Dienste
Besonderheiten	IT–spezifisches Risikomanagementsystem in Erarbeitung	Informations– und Datenschutz–Risikoanalysen fortlaufend aktualisiert	allgemeine Risikostrategie behandelt auch IT–spezifische Risiken

NISG = Netz– und Informationssystemsicherheitsgesetz

Quellen: BKA; BMDW; BMSGPK

(2) Im BKA war – außer für die von der BRZ GmbH betriebenen IT–Verfahren bzw. –Systeme – kein Risikomanagementsystem festgelegt.

2018 führte das Compliance–Management des BKA eine allgemeine Risikobefragung im BKA durch und empfahl, ein IT–spezifisches Risikomanagementsystem einzuführen. Dieser Empfehlung sollte künftig mit dem aktuellen Projekt „Stärkung der Cyberabwehrfähigkeiten im BKA“, welches auch die Einführung eines IT–spezifischen Risikomanagementsystems vorsieht, entsprochen werden.

(3) Das BMDW erstellte bzw. aktualisierte die Analysen in einem fortlaufenden Prozess. Bei (Weiter–)Entwicklungen von IT–Verfahren bzw. –Systemen war eine Informations– und Datenschutz–Risikoanalyse durchzuführen, welche den Schutzbedarf und die jeweiligen Sicherheitsanforderungen definierte. Die darauf aufbauenden Maßnahmen waren in einem eigenen Sicherheitskonzept zu dokumentieren. Zur Zeit der Gebarungsüberprüfung war eine solche Analyse allerdings erst für die Hälfte der IT–Verfahren bzw. –Systeme des BMDW umgesetzt.

(4) Für die im BMSGPK Bereich „Soziales“ betriebenen IT–Verfahren und –Systeme wurden Schutzbedarfs– und Risikoanalysen – als Bestandteil des jeweiligen Vertrags mit der BRZ GmbH – durchgeführt. Der Schutzbedarf der IT–Verfahren und –Systeme des Bereichs „Gesundheit“ war generell festgelegt. Spezifische Schutzmaßnahmen waren anwendungsbezogen für das jeweilige IT–Verfahren bzw. –System definiert.

Daneben waren IT–spezifische Risiken auch in der allgemeinen Risikostrategie des BMSGPK thematisiert. Diese wurde im September 2018 beschlossen und im Laufe des Jahres 2019 umgesetzt. Sie behandelte die IT–spezifischen Risiken nicht auf Ebene der einzelnen IT–Systeme und –Verfahren, sondern umschrieb diese allge-

mein bezogen auf die von den Organisationseinheiten des BMSGPK verantworteten wesentlichen Geschäftsprozesse.

(5) Im Februar 2018 schlossen das BKA, das BMF und das BMDW ein Verwaltungsübereinkommen über gemeinsame Informationssicherheits– und Datenschutzstandards. Dieses Übereinkommen legte für bestimmte – gemeinsam genutzte und von der BRZ GmbH betriebene – IT–Verfahren bzw. –Systeme u.a. die Durchführung von Informationssicherheits–Risikoanalysen fest.

8.2 Der RH anerkannte, dass die IT–Sicherheitsstrategien des BKA, des BMDW und des BMSGPK auf dem kombinierten Ansatz zum Management von IT–Sicherheitsrisiken beruhten und das BKA und das BMDW (mit dem BMF) gemeinsame Informationssicherheits– und Datenschutzstandards für bestimmte – gemeinsam genutzte – IT–Verfahren bzw. –Systeme festlegten.

Der RH wies jedoch darauf hin, dass das Compliance–Management des BKA im Rahmen seiner Risikobefragung 2018 auf die Notwendigkeit eines IT–spezifischen Risikomanagementsystems hingewiesen hatte. Dieses war jedoch noch nicht implementiert und wurde erst zur Zeit der Gebarungsüberprüfung durch das Projekt „Stärkung der Cyberabwehrfähigkeiten im BKA“ erarbeitet.

Der RH empfahl daher dem BKA, ein IT–spezifisches Risikomanagementsystem einzuführen.

Der RH anerkannte, dass im BMDW ein System zum Management von IT–Sicherheitsrisiken implementiert war. Er wies das BMDW jedoch darauf hin, dass es erst für die Hälfte seiner IT–Verfahren und –Systeme die notwendigen Informationssicherheits– und Datenschutz–Risikoanalysen durchgeführt hatte.

Er empfahl daher dem BMDW, die noch offenen Informationssicherheits– und Datenschutz–Risikoanalysen durchzuführen.

Der RH anerkannte, dass das allgemeine Risikomanagementsystem des BMSGPK auch IT–spezifische Risiken behandelte.

8.3 (1) Laut Stellungnahme des BKA befinde sich die Empfehlung bereits im Rahmen des internen „Information Security Management System“–Projekts in Umsetzung.

(2) Das BMDW teilte in seiner Stellungnahme mit, dass die Informationssicherheits– und Datenschutzrisikoanalysen bereits begonnen und auch zu einem großen Teil bereits abgeschlossen worden seien. Die noch fehlenden Informationssicherheits– und Datenschutzrisikoanalysen würden so rasch wie möglich finalisiert.

Internes Berichtswesen

9.1 (1) Ein funktionierendes internes Berichtswesen zur IT–Sicherheit ist besonders relevant, weil es in der Verantwortung der Führungsebene liegt, einen systematischen IT–Sicherheitsmanagementprozess zu begründen, zu steuern und zu kontrollieren. Die Wahrnehmung dieser Verantwortung ist nur dann gesichert, wenn die Führungsebene stetig und nachweislich insbesondere mit den folgenden essenziellen Informationen versorgt wird:

- Sicherheitsanforderungen (etwa aufgrund gesetzlicher oder vertraglicher Verpflichtungen),
- aggregierte Daten im Sinne von Sicherheitskennzahlen,
- aktuelle Sicherheitsrisiken und
- aufgetretene Schwachstellen oder Sicherheitsvorfälle.

Das interne Berichtswesen sollte so strukturiert sein, dass einerseits konkrete Anlassfälle – z.B. Sicherheitsvorfälle, Notfälle – jedenfalls an die Führungsebene zu berichten sind. Andererseits sollte die Führungsebene anhand regelmäßiger Berichte – z.B. mit entsprechend aggregierten Daten – in die Lage versetzt werden, Fehler und Schwachstellen zu erkennen, abzuschätzen, zu beseitigen und folglich die IT–Sicherheitsstrategie sowie die darauf aufbauenden Konzepte, Maßnahmen, Vorgaben und Abläufe zu optimieren (vgl. Punkt 3.1. und Punkt 3.4. Informationssicherheitshandbuch).

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

Tabelle 5: Internes Berichtswesen zur IT–Sicherheit

Berichtswesen	BKA	BMDW	BMSGPK
strategische Verankerung	ja, grundsätzlich	ja, grundsätzlich	ja, grundsätzlich
Festlegung einer Struktur	nein	nein	nein
Festlegung von Berichtsweg und –empfänger	teilweise	nein	nein
Erstellung von regelmäßigen Berichten	nein, anlassfallbezogen	ja, monatlich über interne und externe IT–Sicherheit	ja, wöchentlich und halbjährlich
Berichtsempfänger	Generalsekretär, Kabinett des Bundeskanzlers	Generalsekretär, Kabinett der Bundesministerin	jeweils verantwortliche Sektionsleitung (halbjährlicher Bericht) CIO/IT–Leiter (wöchentlicher Bericht)

CIO = Chief Information Officer

Quellen: BKA; BMDW; BMSGPK

(2) Im BKA erfolgten Berichte an die Führungsebene anlassfallbezogen. Ein regelmäßiges Berichtswesen war in der IT–Sicherheitsstrategie des BKA nur grundsätzlich und hinsichtlich der Berichtsempfänger („Führungsebene") verankert, seine Struktur oder Inhalte waren jedoch nicht festgelegt. Das BKA teilte dazu mit, dass mit dem aktuellen Projekt „Stärkung der Cyberabwehrfähigkeiten im BKA" auch ein umfassendes und standardisiertes Berichtswesen eingeführt werden solle.

(3) Im BMDW wurde ab Jänner 2019 mindestens monatlich ein Bericht zur internen und externen Informationssicherheit erstellt und bei Bedarf durch den zuständigen Gruppenleiter an den Generalsekretär und das Kabinett der Bundesministerin weitergeleitet. Ab Juni 2019 wurde der Bericht monatlich erstellt, im Oktober 2019 erfolgte eine Aufteilung des Berichts in einen ressortinternen und einen externen Bericht. Das Berichtswesen war in der IT–Sicherheitsstrategie des BMDW nur grundsätzlich verankert, seine Struktur, Inhalte und insbesondere der konkrete Berichtsweg und die Berichtsempfänger waren hingegen nicht festgelegt.

(4) Im BMSGPK wurde halbjährlich ein „Sicherheits– und Betriebsbericht" an die Leitung der Sektion I (Präsidialangelegenheiten, Supportfunktionen, IT) erstellt. Dieser enthielt vorwiegend zentrale Kenndaten zu Verfügbarkeiten zentraler Systeme sowie zu Viren– und sonstigen Sicherheitsvorfällen für den Bereich „Soziales". Darüber hinaus erhielten der Chief Information Officer (**CIO**) und Leiter der IT–Abteilung Soziales einen wöchentlichen „Sicherheitsmanagement Report". Dieser enthielt detaillierte Aufstellungen und Daten über die für die IT–Sicherheit relevanten Bereiche, beispielsweise über Virenvorfälle, Angriffe, Spamaufkommen, Sicherheitslücken in Software und Hardware oder externe Zugriffe auf das Netzwerk.

Im Bereich „Gesundheit" wurde ebenso ein halbjährlicher „Sicherheits– und Betriebsbericht" mit entsprechenden zentralen Kenndaten an die Leitung der Sektion VI (Humanmedizinrecht und Gesundheitstelematik) erstellt.

Die Koordination dieser beiden Bereiche (Soziales und Gesundheit) erfolgte über die Sitzungen des IT–Sicherheitsmanagement–Teams, ein über beide Bereiche konsolidierter „Sicherheits– und Betriebsbericht" wurde nicht erstellt.

Das Berichtswesen war in der IT– Sicherheitsstrategie des BMSGPK nur grundsätzlich verankert, seine Struktur, Inhalte und insbesondere der konkrete Berichtsweg und die Berichtsempfänger waren hingegen nicht festgelegt.

9.2 Der RH anerkannte, dass die IT–Sicherheitsstrategien des BKA, des BMDW und des BMSGPK ein internes Berichtswesen zur IT–Sicherheit grundsätzlich festlegten. Er wies jedoch kritisch darauf hin, dass im BKA die Führungsebene lediglich anlassfallbezogene Berichte erhielt und ihr somit darüber hinausgehende relevante Informationen für die Steuerung des IT–Sicherheitsmanagementsystems fehlten.

Er empfahl daher dem BKA, rasch das geplante umfassende und standardisierte Berichtswesen zur IT–Sicherheit einzuführen und dabei auch die Struktur des internen Berichtswesens, insbesondere den konkreten Berichtsweg, und die notwendigen Inhalte festzulegen.

Der RH anerkannte, dass im BMDW und im BMSGPK die verantwortliche Führungsebene regelmäßige Berichte zur IT–Sicherheit erhielt. Er wies jedoch darauf hin, dass die Struktur des Berichtswesens und insbesondere der konkrete Berichtsweg und die Berichtsempfänger nicht ausdrücklich festgelegt waren. Gegenüber dem BMSGPK wies er außerdem darauf hin, dass die „Sicherheits– und Betriebsberichte" der Bereiche „Soziales" und „Gesundheit" nicht konsolidiert wurden.

Der RH empfahl daher dem BMDW und dem BMSGPK, die Struktur des internen Berichtswesens zur IT–Sicherheit und insbesondere den konkreten Berichtsweg und die Berichtsempfänger festzulegen.

Er empfahl dem BMSGPK außerdem, die für die Bereiche „Soziales" und „Gesundheit" getrennten „Sicherheits– und Betriebsberichte" im Sinne der Beschreibung der Sicherheitslage des gesamten Bundesministeriums zusammenzuführen.

9.3 (1) Laut Stellungnahme des BKA befinde sich die Empfehlung bereits im Rahmen des internen „Information Security Management System"–Projekts in Umsetzung.

(2) Das BMDW teilte in seiner Stellungnahme mit, dass in der neu zu überarbeitenden IT–Sicherheitsstrategie des BMDW neben der Verankerung der Rechte und Pflichten des Chief Information Security Officers (CISO) und des Informationssicherheitsmanagement–Teams auch die Definition eines konkreten Berichtswesens im Bereich IT–Sicherheit vorgesehen sei.

(3) Das BMSGPK werde sich laut seiner Stellungnahme mit der Frage einer neuen Berichtsstruktur auseinandersetzen, sobald die pandemiebedingte Belastung dies zulasse.

IT–Sicherheitsorganisation

Aufbau der IT–Sicherheitsorganisation in der Zentralstelle

10.1 Für die konkrete Umsetzung der IT–Sicherheitsstrategie des jeweiligen Bundesministeriums ist eine entsprechende IT–Sicherheitsorganisation aufzubauen und den einzelnen Organisationseinheiten die Verantwortung für die verschiedenen Teilbereiche der IT–Sicherheit, z.B. IT–Betrieb, Fachanwendungen, zuzuteilen.

Die Abbildung 2 zeigt für die überprüften Bundesministerien einen Überblick über die für die Umsetzung der IT–Sicherheit zuständigen Organisationseinheiten sowie deren Einordnung in die Gesamtorganisation:

Abbildung 2: Organisationsebenen der IT–Sicherheit

■ Leitung für gesamte IT
□ IT–Agenden

Bundeskanzleramt (BKA)		Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS)	Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW)		Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)	
Generalsekretär		Generalsekretärin	Generalsekretär		**Generalsekretärin**	
Sektion I (Präsidium)		Sektion I (Präsidium)	**Sektion I (Fachsektion)**		Sektion I (Präsidium)	Sektion VI (Fachsektion)
Gruppe I/C		Gruppe I/A	Gruppe A	Gruppe B	Gruppe I/B	Gruppe VI/B
Abt. I/7 IT–Personal-management	Auftrag-geber Betrieb	**Abt. I/A/3 Rechtskoordination, Informations–, Organisations– und Verwaltungsmanagement**	Abt. I/A/1 Digitale Strate-gien und Innova-tion; IT–Planung und Controlling, IKT–Manage-ment, Support	Abt. I/B/7 IKT BMDW–Zentralleitung	Abt. I/B/8 Informations-technologie und –manage-ment	Abt. VI/B/7 Gesundheits-informations-management und Gesund-heitsinformatik
Abt. I/8 Cyber Security	Strategie – BKA Sonder-aufgaben					
Abt. I/9 IKT–Infra-struktur	Betrieb – BKA	Auftraggeber Betrieb; wird durch BMSGPK–Gesundheit mitbetreut	Strategie – BMDW Sonder-aufgaben	Betrieb – BMDW	Strategie – BMSGPK Betrieb – Soziales	Betrieb – Gesundheit Betrieb – BMKÖS
Abt. I/10 Büro der ISK	Sonderaufgabe					

Abt. = Abteilung
IKT = Informations– und Kommunikationstechnologie
ISK = Informationssicherheitskommission

Quellen: BKA; BMKÖS; BMDW; BMSGPK; Darstellung: RH

- Im BKA lag die unmittelbare Leitung für die gesamte IT auf Gruppenebene; zur IT gehörten die Abteilungen für das IT–Personalmanagement, für die Koordination der Cybersicherheit, für den IT–Betrieb und das Büro der Informationssicherheitskommission.
- Im BMKÖS lag die unmittelbare Leitung für die IT auf Abteilungsebene; diese setzte als Auftraggeber im Rahmen eines Verwaltungsübereinkommens wiederum operativ eine andere IT–Abteilung, die IT–Abteilung Gesundheit des BMSGPK, als Dienstleister ein.
- Im BMDW, dem für Digitalisierung zuständigen Ministerium, lag die unmittelbare Leitung für die gesamte IT auf Sektionsebene; zur IT gehörten die Gruppe für den Betrieb der IT des BMDW und die Gruppe für die Digitalen Strategien und Innovation des Bundes.
- Im BMSGPK lag die unmittelbare Leitung für die gesamte IT erst auf Ebene der Generalsekretärin. Die Abteilung I/B/8 Informationstechnologie und –management (IT–Abteilung Soziales) der Präsidialsektion war für den IT–Betrieb des Präsidiums und des Bereichs „Soziales“ – das betraf die Sektionen für die Bereiche Soziales, Pflege und Konsumentenschutz – zuständig. In der Sektion VI (Humanmedizinrecht und Gesundheitstelematik) war eine eigenständige IT–Abteilung VI/B/7 Gesundheitsinformationsmanagement und Gesundheitsinformatik (IT–Abteilung Gesundheit) für den IT–Betrieb des aus zwei Sektionen bestehenden Bereichs „Gesundheit“ eingerichtet. Diese Abteilung hatte außerdem weitere Koordinationsaufgaben hinsichtlich Cyber Security im Gesundheits– und Veterinärwesen. Die Leitung für die gesamte IT des BMSGPK war daher erst in der Funktion der Generalsekretärin organisatorisch zusammengeführt.

10.2 Der RH wies kritisch darauf hin, dass im BMSGPK die unmittelbare Leitung für die gesamte IT des Ressorts organisatorisch erst bei der Funktion der Generalsekretärin zusammengeführt war. Durch die vom BMSGPK gewählte organisatorische Aufteilung des IT–Betriebs auf zwei (operative) IT–Abteilungen – eine für den Bereich „Soziales“ und eine für den Bereich „Gesundheit“ – in zwei getrennten Sektionen (Präsidialsektion und Sektion VI) entstand das Risiko einer uneinheitlichen Umsetzung der IT–Sicherheitsstrategie. Der RH hielt außerdem fest, dass es nicht die typische Aufgabe der Funktion der Generalsekretärin war, die laufende Tätigkeit von zwei operativen IT–Abteilungen zu koordinieren.

Der RH empfahl daher dem BMSGPK, die Agenden für die Steuerung der IT und der IT–Sicherheit des Ressorts zusammenzufassen und unter eine einheitliche Führung zu stellen.

10.3 Das BMSGPK teilte in seiner Stellungnahme mit, dass die Abteilung Informationstechnologie und –management (IT–Abteilung Soziales) und die Abteilung für Gesundheitsinformationsmanagement und Gesundheitsinformatik (IT–Abteilung Gesundheit) völlig unterschiedliche Aufgabenschwerpunkte hätten. Der IT–Abtei-

lung Soziales obliege die strategische Steuerung der IT im BMSGPK inklusive der Ressort–IT–Sicherheitsstrategie. Der IT–Abteilung Gesundheit komme die Koordination der Cybersicherheit im föderalen Gesundheitssystem sowie im internationalen Gesundheitssektor zu. Dies betreffe etwa den Vorsitz des strategischen Steuerungsgremiums „Cybersicherheitsausschuss für eHealth", die Errichtung des HealthCERT[8] sowie die Vertretung des Gesundheitssektors in der „Cyber Sicherheit Plattform", im CERT–Verbund und weiteren informationssicherheitsrelevanten Gremien samt der Mitwirkung im Gesundheitsbereich der EU–Agenturen und der ENISA[9].

Weiters berücksichtige die Aufbauorganisation des BMSGPK die Vorteile einer engen Einbindung der für Gesundheitsdienste und –applikationen zuständigen IT–Abteilung Gesundheit in dem Gesundheitsministeriumsbereich der Zentralstelle. Die Schnittstellen zwischen den Fachabteilungen im Gesundheitsbereich und der IT–Abteilung Gesundheit seien mannigfaltig und intensiv und bedürften häufiger und kurzfristiger Abstimmungen. Die IT–Abteilung Gesundheit aus diesem Verbund herauszunehmen und in das Präsidium zu transferieren, wäre dieser intensiven Zusammenarbeit nicht förderlich.

Durch die Geschäftseinteilung des BMSGPK sei die IT–Abteilung Soziales für die IT–Strategie einschließlich der IT–Sicherheitsstrategie für das gesamte Ressort zuständig. In Wahrnehmung dieser Kompetenz seien entsprechende Strategien und Maßnahmen erarbeitet worden, wobei auch die IT–Abteilung Gesundheit aktiv beteiligt gewesen sei.

Die IT–Aufgaben in einem heterogenen, sich zwangsläufig eher an Systemen der Länder und der Sozialversicherung orientierenden Gesundheitsbereich seien mit den Aufgaben der Bundesverwaltungs–IT nur bedingt vergleichbar. Die etablierte Steuerung der IT–Sicherheit unter Federführung der Sektion I hinsichtlich der internen IT bei gleichzeitiger Ermöglichung der Steuerungsaufgaben der IT– Sicherheit im föderalen Gesundheitssystem durch die Fachsektion habe sich bewährt.

Daher würden die Vorteile der Integration der IT–Abteilung Gesundheit in den Gesundheitsbereich des BMSGPK überwiegen.

10.4 Der RH stellte gegenüber dem BMSGPK klar, dass die Intention seiner Empfehlung nicht die Herauslösung der gesamten Abteilung für Gesundheitsinformationsmanagement und Gesundheitsinformatik (IT–Abteilung Gesundheit) aus dem Bereich Gesundheit war, sondern die Zusammenfassung der Steuerung der IT und IT–Sicherheit des Ressorts unter einer einheitlichen Führung. Dies würde in allen Bereichen eine einheitliche Umsetzung der IT–Sicherheitsstrategie, einheitliche Sicherheits-

[8] CERT = Computer Emergency Response Team

[9] ENISA = Agentur der Europäischen Union für Cybersicherheit

standards und ein aufeinander abgestimmtes IT–Notfallmanagement sicherstellen sowie zeitgerechte vergleichbare IT–Sicherheitsüberprüfungen gewährleisten.

In der Aufbauorganisation zur Zeit der Gebarungsüberprüfung lag die Gesamtverantwortung nicht nur in strategischen Angelegenheiten, sondern auch für den IT–Betrieb und die IT–Sicherheit des Ressorts bei der Generalsekretärin. Der RH hielt daher erneut fest, dass es nicht die typische Aufgabe der Funktion der Generalsekretärin war, die laufende Tätigkeit von zwei operativen IT–Abteilungen und deren IT–Sicherheit zu koordinieren.

Funktionen und Rollen in der IT–Sicherheitsorganisation

11.1 (1) Für die effiziente Wahrnehmung der operativen Aufgaben der IT–Sicherheit ist die Festlegung von Rollen und klaren Verantwortlichkeiten notwendig. Dafür haben sich national und international Standardfunktionen (Rollen, Tätigkeiten) etabliert, denen entsprechende Aufgaben zugeordnet sind:

1. Die im internationalen Kontext geläufige Funktionsbezeichnung für alle Fragen der Informations– und IT–Sicherheit ist der Chief Information Security Officer (**CISO**), der zentral für Informations– und IT–Sicherheit verantwortlich ist.

2. Dem CISO entspricht auf nationaler Ebene der IT–Sicherheitsbeauftragte gemäß Informationssicherheitshandbuch. Er agiert als zentrale Ansprechperson für alle Fragen der Informations– und IT–Sicherheit und trägt die fachliche Verantwortung für diesen Bereich. Er ist gesamtverantwortlich für die Realisierung der Sicherheitsmaßnahmen, plant und koordiniert Schulungs– und Sensibilisierungsveranstaltungen und verwaltet die für die Informationssicherheit zur Verfügung stehenden Ressourcen.

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

4. Der Informationssicherheitsbeauftragte ist gemäß InfoSiG in jedem Bundesministerium einzurichten und überwacht primär die Einhaltung der Bestimmungen dieses Bundesgesetzes.

5. Der Chief Digital Officer (**CDO**) eines Bundesministeriums ist für die Digitalisierungsstrategie und Digitalisierungsmaßnahmen des jeweiligen Bundesministeriums gesamtverantwortlich.

In den überprüften Bundesministerien waren nachfolgende für die IT–Sicherheit relevante Funktionen (Rollen) eingerichtet:

Tabelle 6: Funktionen der IT–Sicherheitsorganisation

Inhaber der Funktionen (Rollen)			
Funktion	BKA	BMDW	BMSGPK[1]
Chief Information Security Officer (CISO) verantwortlich für die Informationssicherheit (somit auch für die IT–Sicherheit) im Bundesministerium	AL (I/C/8)	–	–
IT–Sicherheitsbeauftragter zentrale Ansprechperson für die IT–Sicherheit des Bundesministeriums (gemäß Ressortdefinition)	Ref (I/C/8)	Ref (I/B/7)	Soziales: Ref (I/B/8) Gesundheit: Ref (VI/B/7)
Leiter der IT–Abteilung (CIO) verantwortlich für die IT–Infrastruktur des Bundesministeriums	AL (I/C/9)	AL (I/B/7)	Soziales: AL (I/B/8) Gesundheit: AL (VI/B/7)
Informationssicherheitsbeauftragter gemäß InfoSiG Überwachung der Einhaltung des InfoSIG	AL (I/C/10)	AL (Pr 6)	Soziales: Ref (I/B/11) Gesundheit: AL (VI/B/7)
Chief Digital Officer (CDO) Entwicklung und Umsetzung einer grundlegenden Digitalisierungsstrategie im Bundesministerium	GL (I/C)	GL (I/A)	–

AL = Abteilungsleitung
GL = Gruppenleitung
InfoSiG = Informationssicherheitsgesetz
Ref = Referentin bzw. Referent (Abteilungsbezeichnung)

Quellen: BKA; BMDW; BMSGPK

[1] Im BMSGPK waren alle Funktionen doppelt besetzt; jeweils eine Person aus dem Bereich Soziales und eine andere aus dem Bereich Gesundheit.

(2) An Besonderheiten waren festzustellen:

- Lediglich im BKA war ein für die Informations– und IT–Sicherheit gesamtverantwortlicher Chief Information Security Officer (CISO) auf Ebene einer Abteilungsleitung eingerichtet. Das BMDW teilte dazu im Rahmen der Gebarungsüberprüfung mit, dass im Zuge der Überarbeitung der „Grundsätze zur Informationssicherheitspolitik“ auch ein gesamtverantwortlicher CISO etabliert werden solle.
- Im BMDW und BMSGPK waren Funktionen mit der Bezeichnung „IT–Sicherheitsbeauftragter“ eingerichtet. Diese waren jedoch ausschließlich für Agenden der IT–Sicherheit – und damit nicht im umfassenden Sinne für Informationssicherheit – verantwortlich und auf Referentenebene angesiedelt. Das BMDW teilte dazu mit, dass – wie oben angeführt – ein gesamtverantwortlicher CISO etabliert werden solle.
- Die Funktion eines für die Digitalisierungsstrategie des gesamten Bundesministeriums verantwortlichen Chief Digital Officers (CDO) war im BMSGPK nicht besetzt.

11.2 Der RH wies kritisch darauf hin, dass im BMDW und im BMSGPK zwar Funktionen mit der Bezeichnung „IT–Sicherheitsbeauftragter“ eingerichtet und besetzt waren, diesen aber nicht jene umfassende Verantwortung und Umsetzungsbefugnisse zukamen, die für diese Funktion im Sinne des Informationssicherheitshandbuchs vorgesehen waren; ein CISO war in diesen beiden Ressorts nicht eingerichtet.

Der RH empfahl daher dem BMDW und dem BMSGPK, einen für die gesamte Informations– und IT–Sicherheit verantwortlichen fachkundigen Chief Information Security Officer (CISO) einzurichten.

Der RH wies gegenüber dem BKA darauf hin, dass die im Informationssicherheitshandbuch verwendete Benennung der für Informations– und IT–Sicherheit gesamtverantwortlichen Funktion als „IT–Sicherheitsbeauftragter“ missverständlich war, da diese Bezeichnung einen lediglich auf die IT–Sicherheit eingeschränkten Aufgabenbereich indizierte.

Der RH empfahl daher dem BKA, im Rahmen der Überarbeitung der Cybersicherheitsstrategie darauf hinzuwirken, auch im darauf beruhenden Informationssicherheitshandbuch die Aufgaben des IT–Sicherheitsbeauftragten derart anzupassen, dass dieser für die Agenden der IT–Sicherheit zuständig ist. Weiters wäre die Funktion des CISO als Verantwortlicher für die gesamte Informations– und IT–Sicherheit als gemeinsamer Standard für alle Bundesministerien zu verankern und von der Funktion des Chief Information Officers (CIO) zu trennen.

Der RH wies darauf hin, dass im BMSGPK die Funktionen „IT–Sicherheitsbeauftragter“, „Chief Information Officer“ und „Informationssicherheitsbeauftragter“ jeweils zweimal, einmal für den Bereich Soziales und die IT–Abteilung Soziales, und einmal für den Bereich Gesundheit und die IT–Abteilung Gesundheit besetzt waren. Damit bestand wiederum das Risiko einer uneinheitlichen Umsetzung der IT–Sicherheitsstrategie.

Der RH wiederholte daher seine Empfehlung aus TZ 10 an das BMSGPK, die Agenden für die Steuerung der IT und der IT–Sicherheit des Ressorts zusammenzufassen und unter eine einheitliche Führung zu stellen.

Der RH hielt kritisch fest, dass im BMSGPK kein Chief Digital Officer (CDO) betraut war. Er verwies dazu auf seinen Bericht „Digitalisierungsstrategie des Bundes“ (Reihe Bund 2020/11), in dem er die Einrichtung von Chief Digital Officers in den Bundesministerien zur Umsetzung einer Digitalisierungsstrategie grundsätzlich als sinnvoll erachtete.

Der RH empfahl daher dem BMSGPK, die Funktion des Chief Digital Officers (CDO) rasch zu besetzen.

11.3 (1) Laut Stellungnahme des BKA habe es die Empfehlung zur Anpassung des Informationssicherheitshandbuchs bereits – unabhängig von der Cybersicherheitsstrategie – dem Dienstleister zur Umsetzung in Auftrag gegeben.

(2) Das BMDW teilte in seiner Stellungnahme mit, dass im Zuge einer Reorganisation im Bereich der Informationssicherheit des BMDW die Funktion des Chief Information Security Officers (CISO) in der in Überarbeitung befindlichen Informationssicherheitspolitik verankert werde.

(3) Wie das BMSGPK in seiner Stellungnahme mitteilte, habe es am 21. April 2021 die Funktion Chief Digital Officer (CDO) besetzt. Ferner beabsichtige es, nach Maßgabe der personellen Möglichkeiten einen für die gesamte Informations– und IT–Sicherheit verantwortlichen Chief Information Security Officer (CISO) einzurichten.

Informationssicherheitsmanagement–Team

12.1 (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 Funktionsträger und ausgewählte Vertretungen der Anwenderinnen und Anwender umfassen. Bei Bedarf können auch weitere Expertisen beispielsweise zum Risikomanagement sowie die nachgeordneten Dienststellen eingebunden werden. In größeren Organisationen ist es daher, wie im Informationssicherheitshandbuch dargestellt, zweckmäßig, ein Informationssicherheitsmanagement–Team (**ISMT**) aufzubauen, das die Verantwortlichen unterstützt, die übergreifenden Belange der IT–Sicherheit koordiniert sowie Pläne, Vorgaben und Richtlinien (z.B. Schutzmaßnahmen, Klassifizierung und Kennzeichnung von Informationen) erarbeitet.

Die internen Koordinationsstrukturen stellten sich im BKA, BMDW und BMSGPK wie folgt dar:

Tabelle 7: Informationssicherheitsmanagement–Team

Informationssicherheitsmanagement–Team in den überprüften Bundesministerien			
	BKA	BMDW	BMSGPK
Informationssicherheitsmanagement–Team eingerichtet	nein, aber geplant[1]	ja, gemäß Informationssicherheitspolitik	ja[2], gemäß IT–Sicherheitspolitik
Aufgaben des Informationssicherheitsmanagement–Teams	–	Entwicklung und regelmäßige Revision der Informationssicherheitspolitik, Erarbeitung von Plänen, Vorgaben und Richtlinien	Beratung der Ressortleitung, Behandlung von IT–Sicherheitsvorfällen, Ausarbeitung von IT–Sicherheitsmaßnahmen
Vorsitz durch	–	Informationssicherheitsbeauftragten	Leitung der Sektion I
vorgesehene Sitzungsfrequenz	–	regelmäßig	halbjährlich bzw. im Anlassfall
Einbindung der für die IT–Sicherheit verantwortlichen Funktionsträger	–	ja	ja[2]
Einbindung nachgeordnete Dienststellen	–	ja	bei Bedarf
Einbindung der Anwenderinnen und Anwender	–	Personalabteilung, Personalvertretung	bei Bedarf: interne Expertinnen und Experten
Einbindung Externer	–	nicht explizit vorgesehen	bei Bedarf: externe Expertinnen und Experten

[1] Laut Mitteilung des BKA vom 13. Jänner 2021 sei ein Informationssicherheitsmanagement–Team seit 16. Dezember 2020 eingerichtet.
[2] Im BMSGPK waren die Funktionen im Informationssicherheitsmanagement–Team doppelt besetzt; jeweils eine Person aus dem Bereich Soziales, eine andere aus dem Bereich Gesundheit.

Quellen: BKA; BMDW; BMSGPK

(2) Im BKA erfolgten die Aufgabenwahrnehmung und Koordinierung der IT–Sicherheit entsprechend der Linienorganisation. In einer Gruppe der Präsidialsektion waren die vier Fachabteilungen „IT–Personalmanagement“, „Cyber Security“, „IKT–Infrastruktur“ und „Büro der Informationssicherheitskommission“ für Einzelmaßnahmen bezüglich der IT–Sicherheit zuständig. Ein Informationssicherheitsmanagement–Team war zur Zeit der Gebarungsüberprüfung nicht eingerichtet. Hierzu teilte das BKA mit, dass ein solches mit dem Projekt „Stärkung der Cyberabwehrfähigkeiten im BKA“ (TZ 7) eingerichtet werden solle (laut Mitteilung des BKA vom 13. Jänner 2021 sei ein Informationssicherheitsmanagement–Team seit 16. Dezember 2020 eingerichtet).

(3) Im BMDW war ein Informationssicherheitsmanagement–Team eingerichtet, das grundlegende Beschlüsse betreffend IT– und Informationssicherheit zu treffen und diesbezügliche Empfehlungen, Richtlinien oder Erlässe zu erarbeiten hatte. Den Vorsitz führte der Informationssicherheitsbeauftragte. Das Informationssicherheitsmanagement–Team beschloss 2020 im Umlaufwege die Neufassung der IKT–

Nutzungsrichtlinie des BMDW. Von 2018 bis 2020 fand keine Sitzung des Informationssicherheitsmanagement–Teams statt, obwohl die Informationssicherheitspolitik regelmäßige Sitzungen vorsah.

(4) Im BMSGPK war ein Informationssicherheitsmanagement–Team als Gremium aus Führungskräften und Expertinnen und Experten eingerichtet, welches die Entscheidungsträger des Bundesministeriums in allen Belangen der IT–Sicherheit beriet. Bei Bedarf konnten auch externe Expertinnen bzw. Experten hinzugezogen werden.

12.2 Der RH stellte fest, dass im BKA die Etablierung eines Informationssicherheitsmanagement–Teams zwar geplant, aber zur Zeit der Gebarungsüberprüfung noch nicht umgesetzt war.

Er empfahl dem BKA, das geplante Informationssicherheitsmanagement–Team einzurichten und dabei auf eine zweckentsprechende Einbindung der Anwenderinnen und Anwender sowie der nachgeordneten Dienststellen zu achten.

Der RH hielt die Informationssicherheitsmanagement–Teams des BMDW und BMSGPK für grundsätzlich geeignet, die entsprechenden Aufgaben zu erfüllen. Er wies jedoch darauf hin, dass im BMDW der vorsitzführende Informationssicherheitsbeauftragte lediglich für die Einhaltung des InfoSiG verantwortlich war (siehe TZ 11) und ihm keine umfassende Verantwortung für die Informations– und IT–Sicherheit zukam. Er erachtete die Vorsitzführung des Informationssicherheitsmanagement–Teams durch einen Chief Information Security Officer (CISO) bzw. durch eine Sektionsleitung als zweckmäßiger.

Er wies außerdem kritisch darauf hin, dass – obwohl die Informationssicherheitspolitik im BMDW regelmäßige Treffen des Informationssicherheitsmanagement–Teams vorsah – dieses von 2018 bis 2020 nicht zusammengetreten und damit wirkungslos war.

Der RH empfahl daher dem BMDW, den Vorsitz des Informationssicherheitsmanagement–Teams beim neu einzurichtenden, für die gesamte Informations– und IT–Sicherheit verantwortlichen Chief Information Security Officer (CISO) anzusiedeln, eine Mindestsitzungsfrequenz für das Informationssicherheitsmanagement–Team festzulegen und diese auch einzuhalten.

12.3 (1) Das BKA teilte in seiner Stellungnahme mit, dass sich die Empfehlung im Rahmen des internen „Information Security Management System"–Projekts bereits in Umsetzung befinde.

(2) Laut Stellungnahme des BMDW werde es den neu etablierten Chief Information Security Officer (CISO) mit der Leitung des Informationssicherheitsmanagement–Teams beauftragen. Die Festlegung einer Mindestfrequenz an Sitzungen sei geplant.

IT–Arbeitsplätze und Telearbeit/Homeoffice

IT–Arbeitsplätze

13.1 (1) Zur Vereinheitlichung bestehender und neu zu schaffender IKT–Lösungen und IT–Verfahren des Bundes wurde der standardisierte IT–Büroarbeitsplatz in der Bundesverwaltung – die sogenannte „Bundesclient–Architektur" – auf Grundlage der §§ 2 und 3 IKT–Konsolidierungsgesetz eingeführt. Diese legte eine Standard–Softwarebüroausstattung einschließlich eines Betriebssystems fest und gewährleistete somit die Kompatibilität für die zentralen Anwendungen des Bundes (ELAK, Personalverwaltung, Haushaltsverrechnung).

Aufbauend auf der Bundesclient–Architektur installierten die Bundesministerien jeweils auch ressortspezifische Anwendungen (einschließlich unterschiedlicher Produkte zur Gewährleistung der IT–Sicherheit) und dafür unterschiedliche Systemeinstellungen auf den IT–Arbeitsplätzen; ebenso lag in den Ressorts eine unterschiedliche Hardwareausstattung vor. Damit waren die IT–Arbeitsplätze der Bundesministerien nicht einheitlich und folglich auch nicht austauschbar.

(2) IT–Arbeitsplätze konnten anhand ihrer Funktionsweise in vollwertige IT–Arbeitsplätze (z.B. PC oder Laptops) und in Thin–Clients unterschieden werden:

- Vollwertige IT–Arbeitsplätze sind hinsichtlich Speicher– und Rechenleistung vollwertig ausgestattete stationäre bzw. mobile Arbeitsplätze. Die Benutzerdaten können lokal oder über das Netzwerk abgespeichert werden; nicht nur die Dateneingabe und –ausgabe sondern auch die Datenverarbeitung – z.B. mit Bürosoftware – können lokal erfolgen. Damit ist der Einsatz dieser Geräte auch ohne permanente Verbindung zum Server (offline) grundsätzlich möglich.
- Im Vergleich dazu verfügt ein Thin–Client über sehr geringe Speicher– und Rechenleistung und keinen eigenen Festspeicher für die permanente Speicherung von Daten. Die Anwendungen werden am zentralen Server (Applikationsserver) ausgeführt, auch die Datenspeicherung erfolgt nur zentral.

Wie in nachfolgender Tabelle dargestellt, setzten das BKA, das BMDW und das BMSGPK im Bereich Soziales Standard–PC bzw. Laptops ein, das BMSGPK im Bereich Gesundheit hingegen Thin–Clients:

Tabelle 8: Ausstattung der IT–Arbeitsplätze

Arbeitsplatzausstattung	BKA	BMDW	BMSGPK Bereich Soziales	BMSGPK Bereich Gesundheit
Standard–Arbeitsplatz	vollwertiger IT–Arbeitsplatz	vollwertiger IT–Arbeitsplatz	vollwertiger IT–Arbeitsplatz	Thin–Client
Arbeitsplatz–Standardsoftware	Bundesclient	Bundesclient	Bundesclient	entspricht Bundesclient am Server
zusätzliche Software	ressortspezifische Fachsoftware bei Bedarf	ressortspezifische Fachsoftware bei Bedarf	ressortspezifische Fachsoftware bei Bedarf	ressortspezifische Fachsoftware bei Bedarf
VPN–Client	ja	ja	ja	nicht notwendig

VPN = Virtual Private Network

Quellen: BKA; BMDW; BMSGPK

(3) Im Einzelnen war zu den Bundesministerien Folgendes auszuführen:

- Im BKA, BMDW und BMSGPK Bereich Soziales bestand ein IT–Arbeitsplatz aus einem stationären (PC) oder einem mobilen (Laptop) Arbeitsplatzrechner. Auf diesen war die Software der Bundesclient–Architektur installiert, bedarfsentsprechend konnte zusätzliche Fachsoftware installiert werden. Um einen gesicherten Zugriff auf das Netzwerk des jeweiligen Bundesministeriums von externen Arbeitsplätzen zu ermöglichen, war auf den mobilen Arbeitsplatzrechnern ein VPN–Client installiert. Im BKA und BMSGPK Bereich Soziales erfolgte ab 2020 die Neuausstattung nur mehr mit mobilen Arbeitsplatzrechnern.
- Im BMSGPK Bereich Gesundheit bestand ein Standardarbeitsplatz aus einem Thin–Client mit Monitor, Tastatur und Maus. Die IT–Systeme waren so ausgelegt, dass die Daten ausschließlich auf der zentralen Infrastruktur gespeichert wurden. Die Softwarekonfiguration der zentralen Anwendungsserver entsprach dem Bundesclient. Zusatzsoftware konnte bei Bedarf von den zentralen Anwendungsservern zur Verfügung gestellt werden (der externe Zugriff erfolgte mittels Zwei–Faktor–Authentifizierung).

13.2 Der RH anerkannte, dass das BKA, das BMDW und das BMSGPK die Bundesclient–Architektur für die Standard–Softwarebüroausstattung verwendeten; dennoch verursachte, wie in TZ 3 beschrieben, eine ressortübergreifende Verschiebung von IT–Arbeitsplätzen einen hohen Aufwand für die betroffenen IT–Abteilungen.

Der RH wiederholte daher seine Empfehlung aus TZ 3, in einem Projekt die Konsolidierung der IT–Ausstattung der Arbeitsplätze des Ressorts zu behandeln.

Anforderungen an die IT–Sicherheit bei Telearbeit

14.1 (1) Zusätzlich zu den Risiken eines IT–Arbeitsplatzes an der Dienststelle ergaben sich im Zusammenhang mit Telearbeit weitere spezifische Risiken. Zu diesen zählten u.a. der Verlust der Ausstattung des mobilen IT–Arbeitsplatzes (z.B. durch Diebstahl), das Ausspähen von Zugangsdaten oder eine allfällige, gegenüber dem IT–Arbeitsplatz an der Dienststelle infrastrukturell bedingt herabgesetzte IT–Sicherheit.

Das telearbeitsspezifische Risiko konnte durch geeignete, dem Stand der Technik entsprechende Maßnahmen reduziert werden, etwa durch

- eine Zwei–Faktor–Authentifizierung für Zugriffe von außen auf das Netz des Bundesministeriums,
- eine Verschlüsselung der Daten auf den Festplatten der Arbeitsplatzrechner,
- eine Endpoint–Protection für die mobilen Arbeitsplätze (siehe TZ 23),
- die Sperre des Startens (Bootens) des externen Arbeitsplatzes von externen Datenträgern,
- eine Datenspeicherung am zentralen Server,
- einen verschlüsselten Datenaustausch zwischen den externen Arbeitsplätzen und dem Netz des Bundesministeriums mit Hilfe einer VPN–Verbindung und
- einen Virenschutz, um die mobilen Arbeitsplatzrechner vor Schadsoftware zu schützen.

Da bei Thin–Clients die Daten zentral am Server gespeichert und bearbeitet wurden, fielen einzelne Risiken systembedingt weg, z.B. Datenverlust bei Verlust des mobilen Arbeitsplatzes.

Die folgende Tabelle beschreibt die im BKA, BMDW und BMSGPK eingesetzten Maßnahmen zur telearbeitsspezifischen IT–Sicherheit:

Tabelle 9: Maßnahmen zur Reduktion telearbeitsspezifischer IT–Sicherheitsrisiken

Maßnahme am IT–Arbeitsplatz	BKA	BMDW	BMSGPK Bereich Soziales	BMSGPK Bereich Gesundheit
Zwei–Faktor–Authentifizierung	teilweise	ja, Einrichtung noch nicht abgeschlossen	ja	ja
Festplatten–Verschlüsselung	eingerichtet	eingerichtet	eingerichtet	nein, da keine Daten am Thin–Client
Unterbinden des Startens (Booten) von externen Datenträgern	eingerichtet	eingerichtet	eingerichtet	nein, da Thin–Client
Datenspeicherung am zentralen Server, Back–up	ja	ja	ja	ja
verschlüsselter Datenaustausch	ja (VPN)	ja (VPN)	ja (VPN)	verschlüsselte Übertragung von Tastatur–, Maus– und Bildschirminformationen
Schutz vor Schadsoftware am mobilen Arbeitsplatz	ja	ja	ja	nein, da Thin–Client[1]

VPN = Virtual Private Network

Quellen: BKA; BMDW; BMSGPK

[1] Bei Thin–Clients erfolgt keine Datenverarbeitung am lokalen Arbeitsplatz, sondern auf den Anwendungsservern; daher sind dort die entsprechenden Sicherheitsmaßnahmen eingerichtet.

(2) Im Einzelnen waren zu den überprüften Ressorts folgende Besonderheiten zur Telearbeit anzuführen:

- Das BKA setzte mobile Arbeitsplatzrechner mit mobilem Internetzugang des Dienstgebers ein; die Zwei–Faktor–Authentifizierung betraf allerdings nur den Zugang zum Portal (sowie die im Homeoffice teilweise eingesetzten Thin–Clients), nicht aber die mobilen Arbeitsplätze. Die Umsetzung einer Zwei–Faktor–Authentifizierung auch für mobile Arbeitsplätze war zur Zeit der Gebarungsüberprüfung vorgesehen.
- Das BMDW setzte mobile Arbeitsplatzrechner mit mobilem Internetzugang des Dienstgebers ein; Bedienstete nutzten allerdings auch ihren privaten Internetzugang. Die Einführung einer Zwei–Faktor–Authentifizierung für die Arbeitsplatzrechner befand sich in Umsetzung.
- Das BMSGPK setzte im Bereich Soziales mobile Arbeitsplatzrechner mit mobilem Internetzugang des Dienstgebers ein. Im Bereich Gesundheit setzte das BMSGPK auch für die Telearbeit Thin–Clients ein, die Speicherung der Daten erfolgte zentral.

14.2 Der RH stellte im Zusammenhang mit dem Homeoffice kritisch fest, dass das BKA auf den mobilen Arbeitsplätzen noch keine Zwei–Faktor–Authentifizierung einsetzte und das BMDW sein Vorhaben einer Zwei–Faktor–Authentifizierung für die Arbeitsplatzrechner des Ressorts noch nicht abgeschlossen hatte. Damit bestanden IT–Sicherheitsrisiken.

Er empfahl dem BKA und BMDW, die Zwei–Faktor–Authentifizierung für die Arbeitsplatzrechner flächendeckend zum Einsatz zu bringen.

14.3 (1) Laut Stellungnahme des BKA werde die Empfehlung bereits im Rahmen des Programms IT–Konsolidierung bearbeitet.

(2) Das BMDW teilte in seiner Stellungnahme mit, dass die Zwei–Faktor–Authentifizierung am IT–Arbeitsplatz auf Basis des bundeseinheitlichen Dienstausweises mittlerweile flächendeckend zum Einsatz komme.

Nutzung von Videokonferenzen bei Telearbeit/Homeoffice

15.1 Grundsätzlich gab es im Bund ein einheitliches Produkt für Videokonferenzanlagen; dieses wurde von der BRZ GmbH betreut und beispielsweise auch vom BKA und BMDW im Wege ihrer Videokonferenzräume eingesetzt.

Zum Informationsaustausch im Rahmen von Telearbeit bzw. Homeoffice boten sich grundsätzlich Videokonferenzen am IT–Arbeitsplatz an. Der RH erhob bei den überprüften Ressorts, ob diese Möglichkeit genutzt wurde und welche der am Markt verfügbaren Produkte für die IT–Arbeitsplätze verwendet wurden: Im BKA, BMDW und BMSGPK kamen vier unterschiedliche Produkte für die Anwendung am IT–Arbeitsplatz zum Einsatz.

15.2 Der RH stellte kritisch fest, dass im BKA, BMDW und BMSGPK vier unterschiedliche, innerhalb eines Bundesministeriums (BMDW) zum Teil mehrere Videokonferenz–Softwareprodukte auf den IT–Arbeitsplätzen zur Anwendung kamen. Er kritisierte, dass damit die Durchführung von Videokonferenzen[10] zwischen Bediensteten unterschiedlicher Bundesministerien, und selbst zwischen Bediensteten innerhalb eines Bundesministeriums, erschwert war und der Einsatz einer Vielzahl von Softwareprodukten einen erhöhten Betreuungsaufwand bedeutete. Vom BKA und der BRZ GmbH war auch im März 2021, somit ein Jahr nach Beginn des Homeoffice, noch keine einheitliche Softwarelösung hierfür präsentiert worden.

[10] Die bestehende bundeseinheitliche Videosoftware bezog sich auf Videokonferenzanlagen.

Der RH empfahl daher dem BKA und dem BMDW, eine ressortintern einheitliche Softwarelösung für Videokonferenzen vorzusehen. Darüber hinaus empfahl er dem BKA und dem BMDW, gemeinsam einerseits Standards für Videokonferenz–Softwareprodukte zu erstellen, die eine gegenseitige Kommunikation in der Bundesverwaltung sicherstellen und IT–Sicherheitsaspekte besonders berücksichtigen. Andererseits wäre zu evaluieren, ob es eine für alle Ressorts der Bundesverwaltung geeignete Videokonferenz–Software gibt und diese in den Bundesclient–Standard integriert werden kann.

15.3 (1) Das BKA teilte in seiner Stellungnahme mit, dass sowohl die Empfehlung zu einer ressortintern einheitlichen Softwarelösung für Videokonferenzen als auch jene zu Standards für Videokonferenz–Softwareprodukte sowie deren mögliche Integration in den Bundesclient–Standard bereits im Rahmen des Programms IT–Konsolidierung bearbeitet würden.

(2) Das BMDW verwies in seiner Stellungnahme auf das im Rahmen der IT–Konsolidierung initiierte Projekt „einheitliche Videokonferenzlösung im Bund (VIKO)“. Damit solle auch eine bundesweit einheitliche Lösung etabliert werden.

15.4 Der RH hielt gegenüber dem BKA und BMDW kritisch fest, dass seit dem mit März 2020 pandemiebedingten Bedarf einer flächendeckenden einheitlichen Videokonferenzlösung bis Juni 2021 (Übermittlung der Stellungnahmen) mehr als 15 Monate vergangen waren, ohne dass dafür eine Lösung erzielt worden war.

Homeoffice im Rahmen der COVID–19–Pandemie

16.1 (1) Telearbeit liegt vor, wenn Bedienstete des Bundes (Beamtinnen und Beamte bzw. Vertragsbedienstete) bestimmte dienstliche Aufgaben außerhalb ihrer Dienststelle an einer von ihnen selbst gewählten Örtlichkeit, beispielsweise in ihrer Wohnung, verrichten und die erforderliche Informations– und Kommunikationstechnik einsetzen. Dabei dürfen dienstliche oder sonstige öffentliche Interessen (etwa der Schutz personenbezogener Daten) nicht entgegenstehen. Wesentliche gesetzliche Voraussetzungen für die Zulässigkeit von Telearbeit sind, dass sich die Bediensteten bis dahin bewährt haben, ihr Arbeitserfolg auch bei Telearbeit kontrolliert werden kann und sie den Datenschutz gewährleisten können. Festzulegen ist neben dem Ausmaß der Telearbeit insbesondere, wie und wann die Bediensteten erreichbar sein müssen.

Dienstrechtlich wird Telearbeit bei Beamtinnen und Beamten (öffentlich–rechtliches Dienstverhältnis) mit deren Zustimmung angeordnet und bei Vertragsbediensteten (vertragliches Dienstverhältnis) mit diesen vereinbart. Die Bediensteten haben keinen Rechtsanspruch auf Telearbeit.

(2) Das Homeoffice während der COVID–19–Pandemie im Frühjahr 2020 unterschied sich von der gesetzlich festgelegten Telearbeit. In Umsetzung eines Ministerratsbeschlusses zum Gesundheitsschutz ordneten die Bundesministerinnen und Bundesminister jeweils für ihren Wirkungsbereich generell mit Rundschreiben an, dass alle Bediensteten mit Ausnahme des unverzichtbaren Schlüsselpersonals ihre Dienstleistung ab 16. März 2020 zu Hause zu erbringen hatten. Im BMSGPK war zusätzlich eine Vereinbarung der Bediensteten mit ihren Vorgesetzten sowie den Dienstbehörden bzw. Personalstellen vorgesehen. Das angeordnete Homeoffice umfasste nicht nur Telearbeit im herkömmlichen Sinn mit den entsprechenden technischen Hilfsmitteln, sondern auch sonstige Aufgabenerfüllung unabhängig von speziellen technischen Hilfsmitteln und unabhängig von den für die Telearbeit im Gesetz festgelegten Voraussetzungen. Am 6. Juli 2020 endete diese besondere Art des Homeoffice mit der durch Ministerratsbeschluss abgestimmten Aufnahme des regulären Dienstbetriebs.

(3) Nachfolgende Hard– und Software beschafften die überprüften Ressorts für das Homeoffice aufgrund der COVID–19–Pandemie, um einen Dienstbetrieb auch einem Teil jener Bediensteten zu ermöglichen, die bis dahin über keine mobile Arbeitsplatzausstattung verfügten:

Tabelle 10: IKT–Beschaffungen aufgrund der COVID–19–Pandemie

IKT–Beschaffungen März bis Juni 2020				
	BKA[1]	BMKÖS	BMDW	BMSGPK (Bereich Soziales)
Hardware	419.925 EUR	29.335 EUR	173.793 EUR	258.261 EUR
u.a. Laptops	240 Stück	29 Stück	140 Stück	131 Stück
u.a. Mobiltelefone	57 Stück	nicht ausgewiesen[2]	35 Stück	60 Stück
Software	67.744 EUR	keine Software beschafft	63.698 EUR	59.516 EUR

IKT = Informations– und Kommunikationstechnologie Quellen: BKA; BMKÖS; BMDW; BMSGPK

[1] inklusive Familie und Jugend, Kunst und Kultur
[2] Im BMKÖS wurden aufgrund von COVID–19 beschaffte Mobiltelefone nicht eigens ausgewiesen.

16.2 Der RH merkte an, dass die COVID–19–Pandemie zusätzliche IKT–Beschaffungen notwendig machte, um den Regelbetrieb aufrechtzuerhalten. Diese beliefen sich in den genannten Ressorts für den Zeitraum März bis Juni 2020 in Summe auf rd. 1,07 Mio. EUR.

IT–Arbeitsplätze bei Telearbeit/Homeoffice

17.1 (1) Der Bund als Dienstgeber hat den Bediensteten die erforderliche technische Ausstattung für die Telearbeit zur Verfügung zu stellen. In den überprüften Bundesministerien erhielten die Bediensteten dafür Laptops, die teilweise mit einer Docking–Station auch stationär am Arbeitsplatz im Ministerium (BKA, BMDW, BMSGPK) verwendet wurden. Daneben verfügten die Bediensteten teilweise auch über dienstliche Smartphones oder Tablets.

(2) Die folgende Tabelle gibt jeweils für die Stichtage 29. Februar 2020 (vor der COVID–19–Pandemie) und 30. April 2020 (während der COVID–19–Pandemie) einen Überblick, wie viele Bedienstete in der Zentralstelle der überprüften Ministerien beschäftigt waren, wie viele davon Telearbeit (im Sinne der gesetzlichen Definition) verrichten durften, wie viele über eine für Telearbeit geeignete dienstliche IT–Ausstattung verfügten und wie viele die Möglichkeit hatten, ihre private IT–Ausstattung für dienstliche Zwecke zu nutzen:

Tabelle 11: Anteil der Bediensteten mit Telearbeitsanordnung bzw. –vereinbarung

Bedienstete	am 29. Februar 2020 (reguläre Telearbeit)			am 30. April 2020 (Telearbeit bzw. Homeoffice während COVID–19–Pandemie)		
	BKA	BMDW	BMSGPK	BKA	BMDW	BMSGPK
Bedienstete	Anzahl					
Zentralstelle gesamt	690	746	760	702	752	761
davon						
mit Telearbeitsanordnung bzw. –vereinbarung	*38*	*162*	*83*	*40*	*162*	*84*
mit dienstlicher, für Telearbeit[1] geeigneter IT–Ausstattung	*330*	*378*	*264*	*530*	*513*	*365*
mit Möglichkeit der Nutzung privater[2] IT–Ausstattung für Telearbeit	*0*	*112*	*90*	*50*	*272*	*314*

[1] sowie auch generell für die Dienstleistung außerhalb der Dienststelle (beispielsweise für Dienstreisen) geeigneter IT–Ausstattung
[2] Die Möglichkeit der Nutzung privater IT–Ausstattung bestand zum Teil auch für Bedienstete mit dienstlicher, für die Dienstleistung außerhalb der Dienststelle geeigneter IT–Ausstattung.

Quellen: BKA; BMDW; BMSGPK

Ende Februar 2020 betrug der Anteil der Bediensteten mit Telearbeitsanordnung oder –vereinbarung zwischen 5,5 % im BKA und 21,7 % im BMDW. Dieser Anteil veränderte sich in den ersten beiden Monaten der COVID–19–Pandemie (März und April 2020) nahezu nicht. Von Ende Februar bis Ende April 2020 ergab sich jedoch – im Zusammenhang mit der COVID–19–Pandemie und dem angeordneten Homeoffice – ein beachtlicher Anstieg des Anteils jener Bediensteten, denen die Ressorts eine dienstliche, für Telearbeit geeignete IT–Ausstattung (z.B. Laptop) zur Verfügung stellten (BKA um 57,9 %, BMDW um 34,6 %, BMSGPK um 38,1 %).

(3) Wie aus Tabelle 11 ersichtlich ist, bestand im BMDW und im BMSGPK auch die Möglichkeit, private Endgeräte für die Dienstverrichtung zu nutzen. Vor der COVID–19–Pandemie verfügte das BMDW über 112 solcher gesicherter Zugänge zu den Systemen des Ressorts; das BMSGPK gab an, dass 90 Bedienstete ihren Dienst auch mit privaten Endgeräten verrichten konnten, was jedoch einer Freigabe durch die IT–Abteilung bedurfte.

Während der COVID–19–Pandemie erhöhte sich diese Anzahl (bis Ende April 2020) auf 272 im BMDW bzw. 314 im BMSGPK. Im BKA bestand die Möglichkeit der Nutzung privater Endgeräte erst im Rahmen des Homeoffice während der COVID–19–Pandemie (50 Bedienstete Ende April 2020).

17.2 Der RH stellte fest, dass im Rahmen des zeitlich begrenzten Homeoffice während der COVID–19–Pandemie die verstärkte Nutzung der privaten IT–Ausstattung durch die Bediensteten des BKA, des BMDW und des BMSGPK als Maßnahme zur Aufrechterhaltung des Dienstbetriebs diente.

Er wies darauf hin, dass für den regulären Dienstbetrieb die Nutzung privater IT–Ausstattung (Endgeräte) für Telearbeit

- gesetzlich nicht vorgesehen war, da der Dienstgeber gemäß § 36a BDG bzw. § 5c VBG die erforderliche IT–Ausstattung für die Telearbeit zur Verfügung zu stellen hatte, und
- Risiken beinhalten könnte. Diese umfassen beispielsweise die parallele dienstliche und private Nutzung dieser privaten Endgeräte und damit das Risiko, dass dienstliche Daten auf privaten Endgeräten gespeichert bleiben. Auch sind auf den privaten Endgeräten die IT–Sicherheitsvorkehrungen gegenüber Schadsoftware im Vergleich mit den IT–Sicherheitsmaßnahmen des Bundesministeriums typischerweise geringer.

Für den regulären Dienstbetrieb sollte der Einsatz privater IT–Ausstattung für Telearbeit daher nicht standardmäßig vorgesehen werden.

Der RH empfahl dem BKA, dem BMDW und dem BMSGPK, die Telearbeit im regulären Dienstbetrieb nur dann vorzusehen, wenn eine geeignete dienstliche IT–Ausstattung zur Verfügung steht und die technischen Sicherheitsvorkehrungen erfüllt sind, um die IT–Sicherheit zu gewährleisten.

Weiters empfahl er, auch im Hinblick auf mögliche weitere Phasen von krisenbedingtem Homeoffice die IT–Ausstattung der Arbeitsplätze künftig so einzurichten, dass in dem zur Aufrechterhaltung des Dienstbetriebs erforderlichen Umfang eine Dienstverrichtung außerhalb der Dienststelle mit dienstlichen Geräten möglich ist.

17.3 (1) Das BKA teilte in seiner Stellungnahme mit, dass die Dienstverrichtung außerhalb der Dienststelle mit dienstlichen Geräten bereits möglich sei, da die Vollausstattung

der Bediensteten mit dienstlichen Geräten zum mobilen Arbeiten mittlerweile aufgrund der Ausstattungsmaßnahmen im Zuge der Corona–Epidemie gewährleistet sei.

(2) Das BMDW führte in seiner Stellungnahme an, entsprechend der Telearbeits–Richtlinie den Bediensteten für die Telearbeit die dienstliche Ausstattung (Laptop, VPN–Zugang, Mobil–Telefon) zur Verfügung gestellt zu haben. Der Einsatz privater IT–Ausstattung sei nicht für eine Dienstverrichtung in Telearbeit vorgesehen gewesen, sondern nur als punktuelle, anlassbezogene Einstiegsmöglichkeit. In der COVID–19–Krise habe zur Aufrechterhaltung des Dienstbetriebs zunächst auf die Verwendung privater Geräte – mit entsprechenden Sicherheitsvorkehrungen (Remote–Desktop–Verbindung) – zurückgegriffen werden müssen. In weiterer Folge seien sämtliche Mitarbeiterinnen und Mitarbeiter mit aktuellen Laptops ausgerüstet worden.

(3) Das BMSGPK wies in seiner Stellungnahme darauf hin, dass die teilweise Verwendung privater IT–Ausstattung durch die kurzfristig pandemiebedingt aufgetretene Notwendigkeit des Homeoffice erforderlich gewesen sei. Dabei sei sichergestellt gewesen, dass dienstliche Daten nicht auf privaten Endgeräten gespeichert würden und es zu keiner Gefährdung dieser Daten komme. Der Empfehlung des RH werde zwischenzeitlich bereits weitgehend – im Sozialbereich sogar zur Gänze – entsprochen.

Regelungen zur Gewährleistung der IT–Sicherheit bei Telearbeit/Homeoffice

18.1 Für die Telearbeit bzw. für die mobile IT–Ausstattung der Bediensteten galten im BKA, BMDW und BMSGPK spezielle Regelungen zur Gewährleistung der IT–Sicherheit (Telearbeits–Rahmenvereinbarungen oder –Richtlinien, technische Anweisungen zum Einsatz mobiler Endgeräte). Zusätzlich waren die allgemeinen Regelungen für die Nutzung der Informations– und Kommunikationstechnologie (IKT–Nutzungsverordnung, IT–Nutzungsrichtlinien) unabhängig davon anwendbar, an welchem Ort die Bediensteten ihre Dienstleistung erbrachten.

Diese Vorschriften enthielten auch sicherheitsrelevante Vorgaben für die Bediensteten in Telearbeit, beispielsweise zur sicheren Verwahrung der Arbeitsgeräte, zum Datenschutz, zur Verwendung von Kennwörtern, zum Schutz der dienstlichen Software, zu Datenaustausch und Datenspeicherung. Diese sicherheitsrelevanten Vorgaben galten grundsätzlich auch für die Zeit des Homeoffice während der COVID–19–Pandemie, da sie sich hauptsächlich aus den für alle Bediensteten verbindlichen Regelungen (IKT–Nutzungsverordnung der Bundesregierung, gesetzliche Bestimmungen zum Datenschutz, Regelungen zur Verwendung der zur Verfügung gestellten mobilen IT–Ausstattung) ergaben.

Wie in TZ 17, Tabelle 11, angeführt, hatte vor der COVID–19–Pandemie nur ein geringer Teil der Bediensteten des BKA (5,5 %), des BMDW (21,7 %) und des BMSGPK (10,9 %) Telearbeitsanordnungen bzw. –vereinbarungen und daher Erfahrungen mit der Dienstverrichtung auf IT–Arbeitsplätzen außerhalb der Dienststelle sowie den dafür notwendigen IT–Sicherheitsvorkehrungen. Weiters fehlten Vorschriften einschließlich sicherheitsrelevanter Vorgaben (z.B. Schutz vor Schadsoftware, gesicherte Verbindung, Löschung dienstlicher Daten vom privaten Endgerät) für jene Bediensteten, die im Homeoffice ihre private IT–Ausstattung nutzten.

Darüber hinaus war nicht ausreichend festgelegt, welche dienstlichen Aufgaben aus Sicherheitsgründen an der Dienststelle zu verrichten bzw. welche für Homeoffice geeignet sind.

18.2 Der RH hielt kritisch fest, dass für die Nutzung privater IT–Ausstattung während des Homeoffice ausdrückliche Vorgaben zur IT–Sicherheit und zu deren spezifischen Risiken fehlten. Er hielt weiters fest, dass die für die Telearbeit angeordneten Sicherheitsvorkehrungen nur einem geringen Teil der Bediensteten im Rahmen ihrer Telearbeitsanordnungen bzw. –vereinbarungen nachweislich zur Kenntnis gebracht waren.

Der RH empfahl dem BKA, BMDW und BMSGPK, insbesondere im Hinblick auf einen allfällig neuerlich notwendigen Übergang des Dienstbetriebs auf Homeoffice,

1. ausdrückliche organisatorische und technische Vorgaben betreffend die allfällig notwendige Nutzung privater IT–Ausstattung im Netz des Bundesministeriums zu erstellen,
2. den Bediensteten die in den verschiedenen Regelungen vorgesehenen IT–Sicherheitsmaßnahmen für eine Dienstverrichtung auf IT–Arbeitsplätzen außerhalb der Dienststelle nachweislich zur Kenntnis zu bringen und
3. konkret festzulegen, ob bestimmte dienstliche Aufgaben jedenfalls aus Sicherheitsgründen an der Dienststelle zu verrichten sind.

18.3 (1) Das BKA verwies in seiner Stellungnahme auf die klare Vorgabe, dass keine private IKT zu nutzen sei. Nur im Einzelfall bzw. aufgrund der Corona–Ausnahmesituation seien mit konkreter Zustimmung des Dienstgebers und nach Freischaltung durch die IKT–Abteilung private Geräte in einer sicheren und durch das BKA gemanagten Software–Umgebung genutzt worden. Zur Zeit der Stellungnahme sei die Nutzung privater IKT–Ausstattung nicht mehr erforderlich, da alle Bediensteten mit einem mobilen Arbeitsplatzrechner ausgestattet seien.

Darüber hinaus befinde sich die Empfehlung aus TZ 20 für eine Richtlinie zur Nutzung mobiler Endgeräte sowie eine zusammenfassende Richtlinie zur Telearbeit im

Rahmen des internen „Information Security Management System"–Projekts bereits in Umsetzung.

(2) Das BMDW sagte in seiner Stellungnahme zu, die Empfehlungen des RH aufzugreifen. Dazu sei vorgesehen, dass das Informationssicherheitsmanagement–Team erforderliche Ergänzungen der bestehenden internen Richtlinien aufzeige und vorschlage.

(3) Laut Stellungnahme des BMSGPK hätten die bestehenden Regelungen sicherheitstechnischer Natur auch die Nutzung privater IT und somit die Erfordernisse der Homeoffice–Phase abgedeckt und seien den Bediensteten bekannt. Es hätte daher keiner darüber hinausgehenden Regelung bedurft. Das BMSGPK sicherte jedoch zu, im Zuge der regelmäßigen Aktualisierung der Regelungen auf die Empfehlung des RH Rücksicht und explizit auf die Situation im Homeoffice Bezug zu nehmen.

18.4 Der RH betonte gegenüber dem BKA, dem BMDW und dem BMSGPK, dass den Bediensteten die angeordneten Sicherheitsvorkehrungen regelmäßig in aktueller Form zur Kenntnis zu bringen sind.

IT–Sicherheit Personal

Zugriffsberechtigungen

19 Durch die Benutzerverwaltung und die Zugriffskontrolle sollte sichergestellt werden, dass nur befugte Personen Zugriff zu den entsprechenden Daten, IT–Systemen und IT–Diensten erhielten. Benutzerverwaltung und Zugriffskontrolle waren daher zentrale Bestandteile der IT–Sicherheit. Dazu konnten verschiedene Maßnahmen, wie Berechtigungskonzepte, Authentifizierungsverfahren, technische Umsetzung von Passwortvorgaben oder regelmäßige Überprüfungen der Benutzerkonten und Berechtigungen, eingesetzt werden.

Tabelle 12: Maßnahmen zur Zugriffskontrolle

Maßnahme	BKA	BMDW	BMSGPK
Berechtigungskonzept	ja	ja	ja
Authentifizierungsverfahren	Username/Passwort; von außen Zwei–Faktor–Authentifizierung	Username/Passwort; von außen sowie in sensiblen Bereichen Zwei–Faktor–Authentifizierung	Zwei–Faktor–Authentifizierung
Umsetzung von Passwortvorgaben	ja, wird technisch erzwungen	ja, wird technisch erzwungen	ja, wird technisch erzwungen
regelmäßige Überprüfung der Benutzerkonten und Berechtigungen	ja	ja	Stichproben

Quellen: BKA; BMDW; BMSGPK

In den überprüften Bundesministerien kamen automatisierte Standardprozesse für die Vergabe von Zugriffsberechtigungen zur Anwendung, auch wurden die Berechtigungen der Benutzerkonten regelmäßig (im BMSGPK in Stichproben) auf ihre Aktualität überprüft. Weiters galten Richtlinien für Einrichtung und Änderung von Passwörtern der Benutzerinnen und Benutzer, deren Einhaltung mit Hilfe einer technischen Maßnahme erzwungen wurde. Die Benutzerauthentifizierung im Netz des BKA und des BMDW erfolgte mit User–ID und Passwort; im BMSGPK, in sensiblen Bereichen des BMDW sowie für alle externen Zugriffe auf diese Bundesministerien war eine Zwei–Faktor–Authentifizierung eingerichtet.

Regelungen

20.1 (1) Der RH überprüfte das Management der IT–Sicherheit im Bereich Personal in den Bundesministerien anhand von drei Themenbereichen:

(a) wesentliche Regelungen,

(b) Maßnahmen vor, während und nach Beendigung eines Dienstverhältnisses (TZ 21) sowie

(c) Personal externer Dienstleister (TZ 22).

Er orientierte sich dabei am Informationssicherheitshandbuch.

(2) Das BKA, BMDW und BMSGPK trafen Regelungen zur personellen IT–Sicherheit in unterschiedlichem Ausmaß:

Tabelle 13: Wesentliche Regelungen zur personellen IT–Sicherheit

wesentliche Regelungen	BKA	BMDW	BMSGPK
Dienstrecht (BDG 1979, VBG)	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	in Überarbeitung	vorhanden	vorhanden
dokumentierte Passwortrichtlinie	vorhanden	vorhanden	vorhanden
Richtlinie zu mobilen Endgeräten	in Ausarbeitung	vorhanden	vorhanden
Erläuterungen zum Datenschutz	vorhanden	vorhanden	vorhanden
Richtlinie zur Telearbeit	keine zusammenfassende Regelung vorhanden, aber diverse Vorgaben in mehreren Regelungen	vorhanden	vorhanden
Regelungen zur elektronischen Kommunikation	vorhanden	vorhanden	vorhanden
Regelungen zur Privatnutzung	IKT–Nutzungsverordnung, Rundschreiben Diensthandy	IKT–Nutzungsverordnung, IKT–Nutzungsrichtlinie des BMDW	IKT–Nutzungsverordnung, IT–Benutzungsrichtlinie des BMSGPK
klassifizierte Informationen	Geheimschutzordnung; Informationssicherheitsgesetz und –verordnung; Erlass der Informationssicherheitskommission; elektronischer Prozess und E–Learning–Tool	Geheimschutzordnung; Informationssicherheitsgesetz und –verordnung; IKT–Nutzungsrichtlinie	Geheimschutzordnung; Informationssicherheitsgesetz und –verordnung

BDG = Beamten–Dienstrechtsgesetz
IKT = Informations– und Kommunikationstechnologie
VBG = Vertragsbedienstetengesetz

Quellen: BKA; BMDW; BMSGPK

Im BKA lagen einzelne Regelungen zur personellen IT–Sicherheit (z.B. zur Nutzung der IKT oder zur elektronischen Kommunikation) oder einzelne Vorgaben in mehreren regulativen Dokumenten (z.B. zur Telearbeit) vor. Andere Aspekte der personellen IT–Sicherheit waren allerdings erst in Ausarbeitung bzw. fehlten:

- eine Richtlinie zur Nutzung mobiler Endgeräte war in Ausarbeitung und
- eine zusammenfassende Richtlinie zur Regelung der Telearbeit lag noch nicht vor.

20.2 Der RH hielt kritisch fest, dass im BKA Richtlinien zur sicheren Nutzung mobiler Endgeräte sowie eine zusammenfassende Richtlinie zur Telearbeit noch nicht vorlagen.

Er empfahl daher dem BKA, Richtlinien zur Nutzung mobiler Endgeräte sowie eine zusammenfassende Richtlinie zur Telearbeit zu erstellen und in Kraft zu setzen.

20.3 Das BKA gab in seiner Stellungnahme an, dass sich die Empfehlung im Rahmen des internen „Information Security Management System"–Projekts bereits in Umsetzung befinde.

Maßnahmen vor, während und nach Dienstverhältnissen

21.1 (1) Die folgende Tabelle gibt die Maßnahmen des BKA, BMDW und BMSGPK hinsichtlich der personellen IT–Sicherheit **vor Beginn des Dienstverhältnisses** wieder:

Tabelle 14: Maßnahmen zur personellen IT–Sicherheit vor Beginn des Dienstverhältnisses

Maßnahmen vor Beginn des Dienstverhältnisses	BKA	BMDW	BMSGPK
Überprüfung der Qualifikation der Bediensteten im Aufnahmeverfahren	vorgesehen	vorgesehen	vorgesehen
Arbeitsplatzbeschreibungen mit IT–sicherheitsrelevanten Aufgaben[1] (z.B. IT–Sicherheitsbeauftragter)	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
Verpflichtungserklärungen hinsichtlich IKT–Nutzung	vorgesehen	vorgesehen	vorgesehen

IKT = Informations– und Kommunikationstechnologie Quellen: BKA; BMDW; BMSGPK

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

(2) Nachfolgende Tabelle führt die vom BKA, BMDW und BMSGPK gesetzten Maßnahmen zur personellen IT–Sicherheit **während des Dienstverhältnisses** an:

Tabelle 15: Maßnahmen zur personellen IT–Sicherheit während des aufrechten Dienstverhältnisses

Maßnahmen während des Dienstverhältnisses	BKA	BMDW	BMSGPK
Awareness–Schulungen	regelmäßiges Angebot, auch online; Teilnahme freiwillig	Angebot 2019, keines 2020; Teilnahme freiwillig	Angebot 2019 und 2020; Teilnahme freiwillig; verpflichtend im Rahmen der Grundschulung
Weiterbildung IT–Personal	nach Bedarf; verpflichtende Grundschulung inklusive IT–Sicherheit	nach Bedarf; keine verpflichtende Grundschulung über IT–Sicherheit	nach Bedarf; verpflichtende Grundschulung inklusive IT–Sicherheit
Informationen zu Support, Anforderungs– und Meldewege	im Intranet	in Nutzungs–Richtlinie	in Benutzungs–Richtlinie
Informationen zu aktuellen Nutzungsregelungen	vorgesehen	vorgesehen	vorgesehen
Vertretungsregelungen	generell in Geschäftsordnung; bei Schlüsselpersonal auch anlassbezogen	in Geschäfts– und Personaleinteilung für IT–Schlüsselpersonal	laut Arbeitsplatzbeschreibung, Intranet
Informationen über Sicherheitsvorfälle	im Anlassfall Sicherheitsempfehlungen für Endnutzerinnen und Endnutzer	bei wichtigen, für die Endnutzerinnen und Endnutzer relevanten Vorfällen	bei wichtigen, für die Endnutzerinnen und Endnutzer relevanten Vorfällen

Quellen: BKA; BMDW; BMSGPK

(a) Im BKA

- fanden die laufenden Awareness–Schulungen zur IT–Sicherheit auf freiwilliger Basis statt,
- war die IT–Sicherheit nicht nur Bestandteil von freiwilligen Weiterbildungsmaßnahmen (speziell für IT–Personal), sondern auch einer verpflichtenden Grundschulung für neu eintretende Bedienstete,
- fanden sich Vertretungsregelungen zwar grundsätzlich in der Geschäftsordnung, für das IT–Schlüsselpersonal erfolgte aber eine anlassbezogene Vertretungsfestlegung.

(b) Im BMDW

- fanden Awareness–Schulungen zur IT–Sicherheit zuletzt im Jahr 2019 auf freiwilliger Basis statt,
- gab es keine verpflichtenden IT–Sicherheitsgrundschulungen.

(c) Im BMSGPK

- fanden Awareness–Schulungen zur IT–Sicherheit auf freiwilliger Basis statt, im Rahmen der Grundschulung waren sie verpflichtend,
- war die IT–Sicherheit nicht nur Bestandteil von freiwilligen Weiterbildungsmaßnahmen (nach Bedarf speziell für IT–Personal), sondern auch einer verpflichtenden Grundschulung für neu eintretende Bedienstete,
- fanden sich Vertretungsregelungen in den Arbeitsplatzbeschreibungen und im Intranet.

(3) Der nachfolgenden Tabelle sind die Maßnahmen zur personellen IT–Sicherheit im BKA, BMDW und BMSGPK **nach Ende des Dienstverhältnisses** zu entnehmen:

Tabelle 16: Maßnahmen zur personellen IT–Sicherheit nach Ende des Dienstverhältnisses

Maßnahmen nach Ende des Dienstverhältnisses	BKA	BMDW	BMSGPK
Personalprozess	definiert	definiert	definiert
Prozessablauf	automatisiert (ELAK)	nach Aufgabenliste	nach Aufgabenliste
Sicherstellung von Daten und Ausstattung	vorgesehen	vorgesehen	vorgesehen
Entzug von Zugangs– und Zugriffsberechtigungen	vorgesehen	vorgesehen	vorgesehen

ELAK = elektronisches Aktenverwaltungssystem Quellen: BKA; BMDW; BMSGPK

Das BKA, das BMDW und das BMSGPK hatten einen strukturierten Prozess bei Beendigung des Dienstverhältnisses definiert, der die IT–sicherheitsrelevanten Maßnahmen zur Sicherstellung von Daten und Ausstattung sowie den Entzug von Zugangs– und Zugriffsberechtigungen berücksichtigte.

21.2 Der RH betonte, dass laufende Awareness–Schulungen zur IT–Sicherheit auf einer verpflichtenden Basis für alle Bediensteten sowie unter Zuhilfenahme von zeitgemäßen Wissensvermittlungsformen wie E–Learning–Plattformen mit Online–Kursen einen wichtigen Beitrag zur IT–Sicherheit leisten können. Er hielt fest, dass im BKA laufend sowie im BMSGPK 2019 und 2020 freiwillige Awareness–Schulungen stattfanden; allerdings hielt er eine verpflichtende Teilnahme für zweckmäßiger. Der RH stellte kritisch fest, dass das BMDW die letzte (freiwillige) Awareness–Schulung 2019 abhielt.

Der RH empfahl daher dem BKA, dem BMDW und dem BMSGPK, regelmäßig verpflichtende Awareness–Schulungen zur IT–Sicherheit durchzuführen, die eine nachweisliche Wissensvermittlung, etwa in Form von E–Learning–Kursen mit einer anschließenden Wissensabfrage, sicherstellen sollen.

Weiters stellte der RH kritisch fest, dass im BKA Vertretungsregelungen von IT–Schlüsselpersonal auch anlassbezogen festgelegt wurden. Er sah insbesondere in auftretenden Krisensituationen und Notfällen eine im Vorhinein klar festgelegte organisatorische Struktur als wesentlichen Faktor für deren erfolgreiche Bewältigung an.

Der RH empfahl daher dem BKA, für das IT–Schlüsselpersonal entsprechende Vertretungsregelungen festzulegen und zu dokumentieren, um auch in Krisensituationen und Notfällen einen reibungslosen Ablauf der Geschäftsprozesse sicherzustellen.

21.3 (1) Laut Stellungnahme des BKA plane es, die E–Learning–Kurse in Zukunft verpflichtend vorzugeben. Weiters sei die Festlegung von Vertretungsregelungen von IT–Schlüsselpersonal bereits in Umsetzung.

(2) Das BMDW hielt in seiner Stellungnahme fest, für seine Bediensteten zur Stärkung von Awareness und Wissen bezüglich IT–Sicherheit und Datenschutz eine Reihe von Seminaren angeboten zu haben. Zusätzlich zu diesen Angeboten stünden allen Bediensteten am Serviceportal des Bundes die E–Learning–Module „Datenschutz–Grundverordnung“ und „Umgang mit klassifizierten Informationen“ zur Verfügung. Als zusätzliche Ergänzung sei bereits 2020 die Planung weiterer Schulungsmodule zum Thema Homeoffice gestartet worden, welche auch das Thema Awareness umfasse. Die Modulreihe sei in finaler Ausarbeitung und würde noch bis Ende 2021 von bis zu 100 Teilnehmerinnen und Teilnehmern absolviert werden können.

(3) Das BMSGPK wies in seiner Stellungnahme darauf hin, dass bereits bisher Awareness–Schulungen und E–Learning–Kurse angeboten worden seien und es beabsichtige, das Angebot zu erweitern sowie der Empfehlung des RH entsprechend auch eine Wissensabfrage sowie eine Verpflichtung zur Teilnahme einzuführen.

21.4 Der RH anerkannte die Planungen des BMDW für zusätzliche Schulungsmodule zum Thema Homeoffice inklusive Awareness mit Beginn im Jahr 2021. Er wies jedoch erneut auf seine Empfehlung hin, Awareness–Schulungen zur IT–Sicherheit regelmäßig verpflichtend mit einer nachweislichen Wissensvermittlung, etwa in Form von E–Learning–Kursen und einer anschließenden Wissensabfrage, durchzuführen.

Externes Personal

22.1 (1) Das BKA, BMDW und BMSGPK bezogen IT–Dienstleistungen von externen Unternehmen in unterschiedlichem Ausmaß. Die zugehörigen Maßnahmen zur Erhöhung der IT–Sicherheit bei Einsatz externen Personals zeigt nachfolgende Tabelle:

Tabelle 17: Maßnahmen zur personellen IT–Sicherheit bei Einsatz externen Personals

Maßnahmen für externes Personal	BKA	BMDW	BMSGPK
IT–Sicherheitsanforderungen Vertragsbestandteil	ja	ja	ja
Qualifikationen des externen Personals	vertraglich festgelegt	vertraglich festgelegt	vertraglich festgelegt
Geheimhaltungspflichten	§ 17 BRZ GmbH Gesetz[1]; sonst vertraglich festgelegt	§ 17 BRZ GmbH Gesetz[1]; sonst vertraglich festgelegt	§ 17 BRZ GmbH Gesetz[1]; sonst vertraglich festgelegt
Pflichten hinsichtlich Datenschutz	vertraglich festgelegt	vertraglich festgelegt	vertraglich festgelegt
Überprüfung der Vertrauenswürdigkeit	Sicherheitsüberprüfung nach Informationssicherheitsgesetz	Sicherheitsüberprüfung nach Informationssicherheitsgesetz (teilweise im EU–Ausland)	Sicherheitsüberprüfung nach Informationssicherheitsgesetz
Einhaltung der IT–Sicherheitsvorgaben des Ressorts	Verpflichtungserklärung nach Kenntnisnahme der IT–sicherheitsrelevanten Informationen; Einbindung in die laufenden Informationsflüsse	Überbindung der wesentlichen Regelungen an den Auftragnehmer	Verpflichtungserklärung nach Sicherheitsunterweisung
Informationssicherheitsmanagement–System beim Auftragnehmer	ja	ja	ja

BRZ GmbH = Bundesrechenzentrum Gesellschaft mit beschränkter Haftung Quellen: BKA; BMDW; BMSGPK

[1] Bundesgesetz über die Bundesrechenzentrum GmbH (BRZ GmbH), BGBl. 757/1996 i.d.g.F.

(2) Das BKA zog externes Personal der BRZ GmbH zur Bewältigung der Aufgaben der IT vor Ort bei. Zur Sicherstellung der personellen IT–Sicherheit hinsichtlich dieses externen Personals fanden sich Regelungen zu Anforderungen, Qualifikationen, Geheimhaltungspflichten und Datenschutz in den geltenden Verträgen. Darüber hinaus band § 17 BRZ GmbH Gesetz Mitarbeiterinnen und Mitarbeiter der BRZ GmbH an Verschwiegenheitspflichten mit Verweis auf Regelungen im Beamten–Dienstrechtsgesetz sowie auf die Geheimhaltungspflicht in der Bundesabgabenordnung. Das BKA band das externe Personal auch in die IT–sicherheitsrelevanten Informationsflüsse ein (z.B. durch E–Mail, ELAK, Intranet oder Awareness–Schulungen). Die BRZ GmbH verfügte über ein eigenes Informationssicherheitsmanagement–System.

(3) Das BMDW setzte für den Betrieb der IT auch Personal eines privaten IT–Dienstleisters, das seinen Arbeitsort im EU–Ausland hatte, ein. Zu den Anforderungen, zur Qualifikation, zur Geheimhaltung, zum Datenschutz und zur Einhaltung interner IT–Sicherheitsvorgaben wurden mit diesem Dienstleister eigene vertragliche Regelungen getroffen. Sicherheitsüberprüfungen des externen IT–Personals, das im Second–Level–Support der IT–Systeme des BMDW tätig war, erfolgten – aufgrund des Standorts des privaten IT–Dienstleisters im EU–Ausland – mithilfe der dortigen Behörden.

Darüber hinaus bezog das BMDW auch IT–Dienstleistungen von der BRZ GmbH.

(4) Im BMSGPK war externes Personal der BRZ GmbH vor Ort tätig. Durch Vertragsregelungen (Rahmenvertrag und zusätzliche Regelungen in Einzelverträgen bei den jeweiligen Fachanwendungen bzw. Supportvereinbarungen) sowie durch gesetzliche Bestimmungen waren die wichtigsten Aspekte der personellen IT–Sicherheit (Anforderungen und Qualifikation des Personals, Geheimhaltung, Datenschutz, Vertrauenswürdigkeit, Kenntnisnahme der internen IT–Sicherheitsvorgaben) umgesetzt.

22.2 Der RH stellte fest, dass das BMDW im Wege seines externen Dienstleisters auch Personal – mit Zugriff im Second–Level–Support auf die IT–Systeme des BMDW – einsetzte, das seinen Arbeitsort im EU–Ausland hatte. Die notwendigen Sicherheitsüberprüfungen des Personals erfolgten im EU–Ausland mit Hilfe sicherheitspolizeilicher Unterstützung der lokalen Behörden vor Ort. Da das externe IT–Personal mit Arbeitsort im EU–Ausland auch Zugriff auf wichtige Dienste des BMDW hatte, lag darin nach Ansicht des RH auch ein Risiko hinsichtlich der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der vom BMDW verarbeiteten Daten. Durch den genannten Arbeitsort war eine unmittelbare Aufsicht bzw. Kontrolle des externen Personals weder für den externen Dienstleister noch für den Auftraggeber BMDW direkt möglich.

Der RH empfahl dem BMDW, beim künftigen Einsatz von externem IT–Personal mit Zugriff auf wichtige Dienste des BMDW die Risiken hinsichtlich der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der vom BMDW verarbeiteten Daten derart zu berücksichtigen, dass der Dienstleister und damit auch der Auftraggeber BMDW unmittelbar Kontrolle und Überprüfungsmöglichkeiten über das externe IT–Personal hat. Diese unmittelbare Kontrolle und Überprüfungsmöglichkeit können bei einem Dienstort Österreich möglicherweise effektiver sichergestellt werden als bei einem Arbeitsort im EU–Ausland.

22.3 Das BMDW hielt in seiner Stellungnahme fest, dass der Vertrag mit dem Dienstleister des BMDW am 30. April 2022 ende. Bei der anstehenden Neuvergabe der IT–Leistungen würde die Empfehlung berücksichtigt.

IT–Sicherheit der Infrastruktur

Technische Maßnahmen zur Erhöhung der IT–Sicherheit

23.1 (1) Im Rahmen einer Risikoanalyse waren die Risiken für die IT–Sicherheit des Betriebs und der Daten zu identifizieren. Diese Risiken sollten durch technische und organisatorische Maßnahmen verringert werden, um die Sicherheit der IT–Anwendungen zu erhöhen. Dabei sollten solche Maßnahmen gesetzt werden, die unter Berücksichtigung von Kosten–Nutzen–Erwägungen die Erreichung eines möglichst hohen Sicherheitsniveaus erwarten ließen.

Das BKA, das BMDW und das BMSGPK hatten eine Reihe von wesentlichen technischen Maßnahmen zur Erhöhung der Sicherheit ihrer IT–Anwendungen ergriffen, die der RH seiner Beurteilung als Best–Practice–Maßstab zugrunde legte. Im Einzelnen waren dies folgende technische Maßnahmen:

- ein netzwerkbasiertes Intrusion Detection System (**IDS**)/Intrusion Prevention System (**IPS**) zur Erkennung/Verhinderung von Angriffen,
- ein Security Information and Event Management System (**SIEM**) zur strukturierten Analyse der verfügbaren Daten, um Angriffe bzw. ungewöhnliches Verhalten im Netz zu erkennen und gegebenenfalls Gegenmaßnahmen ergreifen zu können; dieses System klassifiziert und protokolliert teilweise automatisiert sicherheitskritische Vorfälle,
- Firewalls, um unerwünschte Netzwerkverbindungen vom Internet in das lokale Netz des Bundesministeriums zu unterbinden,
- Spamfilter zur Unterdrückung unerwünschter E–Mails, insbesondere von Werbung (Spam),
- Schutz vor Schadsoftware (Viren, Trojaner, Ransomware, Spyware etc.) für IT–Arbeitsplätze und Server,
- ein Applikations–Whitelisting, wodurch lediglich explizit erlaubte Anwendungen auf den IT–Arbeitsplätzen gestartet werden konnten,
- ein DDoS–Schutz (Schutz gegen gebündelte Angriffe auf den Server, deren Ziel es ist, diesen funktionsunfähig zu machen),
- die Verschlüsselung der Daten auf den Festplatten der IT–Arbeitsplätze,
- ein Endpoint–Protection–System zur umfassenden Sicherung von IT–Arbeitsplätzen,
- die Verhinderung des Startens eines Betriebssystems (Booten) von externen Datenträgern auf den IT–Arbeitsplätzen sowie
- ein Security Operation Center (**SOC**), das in der Regel auf Grundlage der Ergebnisse des Security Information and Event Management Systems laufend alle sicherheitsrelevanten Systeme (Netzwerke, Server, Clients, Webservices etc.) überwacht und analysiert.

Tabelle 18 enthält eine Übersicht über die genannten technischen Maßnahmen und ihren Einsatz in den überprüften Ressorts BKA, BMDW und BMSGPK:

Tabelle 18: Technische Maßnahmen zur Erhöhung der IT–Sicherheit

Maßnahme	BKA	BMDW	BMSGPK
Intrusion Detection System/Intrusion Prevention System	eingerichtet	eingerichtet	eingerichtet
Security Information and Event Management System (SIEM)	eingerichtet	eingerichtet	Bereich Soziales: nicht eingerichtet; Bereich Gesundheit: eingerichtet
Firewall	eingerichtet	eingerichtet	eingerichtet
Spamfilter	eingerichtet	eingerichtet	eingerichtet
Schutz vor Schadsoftware für IT–Arbeitsplätze und Server	eingerichtet	eingerichtet	eingerichtet
Applikations–Whitelisting	eingerichtet	eingerichtet	eingerichtet (Bereich Soziales[1])
Verschlüsselung der Daten auf Festplatten der IT–Arbeitsplätze	eingerichtet	eingerichtet	eingerichtet (Bereich Soziales[1])
DDoS–Schutz	eingerichtet	eingerichtet	eingerichtet
Endpoint–Protection–System	eingerichtet	eingerichtet	teilweise eingerichtet[2]
Unterbinden des Startens eines Betriebssystems von externen Datenträgern auf den IT–Arbeitsplätzen	eingerichtet	eingerichtet	eingerichtet (Bereich Soziales[1])
Security Operation Center (SOC)	eingerichtet	eingerichtet	nicht eingerichtet

[1] Bei den Thin–Clients im Bereich Gesundheit erfolgt keine Datenverarbeitung am lokalen Arbeitsplatz, sondern auf den Anwendungsservern; daher sind die entsprechenden Sicherheitsmaßnahmen dort eingerichtet.
[2] Einzelne Komponenten einer Endpoint–Protection waren gemäß BMSGPK eingerichtet (z.B. Virenschutz, Verschlüsselung der Festplatte, Intrusion Detection im Netz).

Quellen: BKA; BMDW; BMSGPK

(2) Zu den einzelnen Bundesministerien war Folgendes auszuführen:

(a) Das BKA

- führte ein Endpoint–Protection–System im Jahr 2020 ein,
- richtete sämtliche weitere in Tabelle 18 genannten technische Maßnahmen zur Erhöhung der IT–Sicherheit ein (diese wurden regelmäßig gewartet und aktualisiert) und
- setzte zum Schutz vor Schadsoftware Produkte unterschiedlicher Hersteller ein.

(b) Im BMDW waren

- sämtliche in Tabelle 18 aufgezählten Maßnahmen im Einsatz (diese wurden regelmäßig gewartet und aktualisiert) und
- zum Schutz vor Schadsoftware Produkte unterschiedlicher Hersteller eingesetzt. Das BMDW teilte dazu mit, eine Konsolidierung der Produkte zum Schutz vor Schadsoftware zu planen.

(c) Das BMSGPK

- richtete wesentliche der in Tabelle 18 genannten technischen Maßnahmen zur Erhöhung der IT–Sicherheit ein (diese wurden regelmäßig gewartet und aktualisiert),
- setzte zum Schutz vor Schadsoftware Produkte unterschiedlicher Hersteller ein und
- setzte ein Security Information and Event Management System (SIEM) nur im Bereich Gesundheit ein; im Bereich Soziales wurde kein derartiges System verwendet.

Komponenten im Sinne einer Endpoint–Protection für die mobilen Arbeitsplatzrechner waren gemäß Mitteilung des BMSGPK eingerichtet (z.B. Virenschutz, Verschlüsselung der Festplatte, Intrusion Detection im Netz); damit deckten die Sicherheitssysteme nach Auskunft des BMSGPK (Bereich Soziales) sämtliche Aspekte der Endpoint–Protection ab. Nach Ansicht des RH kann ein Endpoint–Protection–System[11] auch[12] umfassender (z.B. Intrusion Detection System am Client, lokale Firewall bei den Clients, Analyse des Prozessverhaltens, Analyse der Kommunikation, Einbinden der Log–Files in das SIEM) gesehen werden.

Ein Security Operation Center (SOC) zur laufenden Überwachung aller sicherheitsrelevanten Systeme – dieses benötigt in der Regel die Ergebnisse eines Security Information and Event Management Systems (SIEM) – war nicht eingerichtet.

23.2 Der RH erachtete die vom BKA, vom BMDW und vom BMSGPK getroffenen technischen Maßnahmen zur Erhöhung der IT–Sicherheit grundsätzlich für zweckmäßig.

Er stellte fest, dass die IT–Sicherheitssysteme des BMSGPK eine Reihe von Aspekten eines Endpoint–Protection–Systems abdeckten. Nach Ansicht des RH kann ein umfassender zu sehendes Endpoint–Protection–System weitere Systemmerkmale beinhalten (z.B. Intrusion Detection System am Client, lokale Firewall bei den Clients, Analyse des Prozessverhaltens, Analyse der Kommunikation, Einbinden der Log–Files in das SIEM).

Der RH empfahl dem BMSGPK, den Einsatz eines umfassenden Endpoint–Protection–Systems als Beitrag zur IT–Sicherheit der IT–Arbeitsplätze zu prüfen und erforderlichenfalls ein solches System einzusetzen.

[11] Ein Endpoint–Protection–System soll die verschiedenen Endgeräte (PCs, Tablets, Laptops, Smartphones etc.) im Netz vor Gefahren schützen, da auf diesen Geräten sensible Daten gespeichert werden können. Hierbei handelt es sich um eine integrierte Lösung, welche aus mehreren Komponenten besteht (z.B. Schutz vor Schadsoftware, Schutz vor Phishing, Firewall, Intrusion Detection System, Intrusion Prevention System, Datenträgerverschlüsselung, Applikation Whitelisting, Einbindung in ein SIEM). Dadurch soll gewährleistet werden, dass ein aktiver Schutz für sämtliche Endgeräte gegeben ist, um Cyberbedrohungen direkt am Endgerät effektiv zu identifizieren, einzudämmen und zu eliminieren.

[12] Signaturbasierte Antiviren–Produkte weisen grundlegende Probleme auf, weil die Anzahl der erkannten Bedrohungen exponenziell wächst. Für Antiviren–Produkte ist es praktisch unmöglich, verdächtige Dateien mit allen vorhandenen Signaturen zu vergleichen.

Er empfahl dem BMDW, zu evaluieren, ob der Einsatz eines umfassenden Endpoint–Protection–Systems in die Bundesclient–Architektur vorgesehen werden soll, um dadurch einen neuen IT–Sicherheitsstandard für alle Ressorts zu etablieren.

Der RH stellte weiters fest, dass das Security Information and Event Management System im BMSGPK nicht ressortweit, sondern lediglich im Bereich Gesundheit eingeführt war.

Er empfahl dem BMSGPK, zu prüfen, ob ein Security Information and Event Management System für den Bereich Soziales einen effektiven Beitrag zur Verbesserung der IT–Sicherheit der IT–Arbeitsplätze mit sich bringen würde, und erforderlichenfalls ein derartiges System einzuführen.

Der RH bewertete die Einrichtung einer zentralen IT–Überwachung (Security Operation Center) als zweckmäßig.

Er empfahl daher dem BMSGPK, zu evaluieren, ob die Einrichtung einer vergleichbaren zentralen Überwachung (Security Operation Center) zum Schutz der IT–Infrastruktur sinnvoll wäre oder ob die laufende Kontrolle der IT–Sicherheit durch andere Einrichtungen sichergestellt ist.

Weiters stellte der RH fest, dass das BKA, das BMDW und das BMSGPK zum Schutz vor Schadsoftware Produkte unterschiedlicher Hersteller einsetzten. Nach Ansicht des RH kann nur im Einzelfall beurteilt werden, ob die möglichen Vorteile einer breiteren Abdeckung gegenüber Schadsoftware durch den Einsatz mehrerer Produkte den Aufwand für das Management dafür überwiegen.

Der RH empfahl daher dem BKA, dem BMDW und dem BMSGPK, jeweils innerhalb des Ressorts zu prüfen, ob die unterschiedlichen Produkte zum Schutz vor Schadsoftware betreffend die Server und Clients zur Erhöhung der IT–Sicherheit optimiert oder vereinheitlicht werden sollen.

23.3 (1) Laut Stellungnahme des BKA sei die Empfehlung, unterschiedliche Produkte zum Schutz vor Schadsoftware zu optimieren oder zu vereinheitlichen, fachlich nicht nachvollziehbar, da es gerade im Bereich des Virenschutzes sinnvoll sei, unterschiedliche Produkte einzusetzen, um unterschiedliche Entwicklungen und Kenntnisstände der Hersteller zu nutzen.

(2) Das BMDW teilte in seiner Stellungnahme mit, dass im Projekt „Standardarbeitsplatz und sichere Basisdienste“ als Teil des Programms „IT–Konsolidierung“ eine umfassende Endpoint–Protection vorgesehen sei.

Zur Empfehlung, unterschiedliche Produkte zum Schutz vor Schadsoftware zu optimieren oder zu vereinheitlichen, sei eine Prüfung eingeplant.

(3) Wie das BMSGPK in seiner Stellungnahme mitteilte, würden seine IT–Systeme sämtliche Punkte eines Endpoint–Protection–Systems adressieren und durch Sicherheitsaudits geprüft. Im Rahmen der IT–Konsolidierung des Bundes werde sich das BMSGPK aktiv beteiligen und die Empfehlung bei der Erarbeitung von IT–Standardarbeitsplätzen des Bundes einbringen.

Die Empfehlung bezüglich eines Security Information and Event Management Systems (SIEM) für den Bereich Soziales werde das BMSGPK prüfen und das Thema auch im Rahmen der IT–Konsolidierung einbringen.

Weiters sagte das BMSGPK zu, die Empfehlung zur Einrichtung einer zentralen Überwachung zum Schutz der IT–Infrastruktur (Security Operation Center, SOC) zu evaluieren.

Der Einsatz unterschiedlicher Produkte zum Schutz von Schadsoftware auch auf unterschiedlichen Ebenen sei ein Ergebnis konkreter IT–Sicherheitsüberlegungen des BMSGPK gewesen. Im Zuge der Mitwirkung bei der Erarbeitung von IT–Standardarbeitsplätzen des Bundes werde das BMSGPK diese Frage einbringen und neuerlich beurteilen.

23.4 Der RH hielt gegenüber dem BKA fest, dass er eine Prüfung dahingehend empfohlen hatte, ob die vorliegenden unterschiedlichen Produkte zum Schutz vor Schadsoftware optimiert oder vereinheitlicht werden können; dies unter Abwägung ressortspezifischer Vor– und Nachteile, z.B. einer möglicherweise erhöhten Sicherheit im Vergleich zu einem erhöhten Betreuungsaufwand. Darüber hinaus hielt der RH fest, dass der gleichzeitige Einsatz verschiedener Softwareprodukte zum Schutz vor Schadsoftware in einem System allerdings auch zu unvorhersehbaren Wechselwirkungen führen kann.

Dem BMSGPK entgegnete der RH, dass aktuelle Endpoint–Protection–Systeme eine integrierte Lösung aus mehreren Komponenten darstellen. Dadurch soll gewährleistet werden, dass ein aktiver Schutz für sämtliche Endgeräte gegeben ist, um Sicherheitsbedrohungen direkt am Endgerät effektiv zu identifizieren, einzudämmen und zu eliminieren. Der RH nahm von der Stellungnahme des BMSGPK, wonach dessen IT–Sicherheitsvorkehrungen alle wesentlichen Komponenten einer umfassenden Endpoint–Protection abdecken, Kenntnis. Er hielt aber gegenüber dem BMSGPK die Notwendigkeit fest, die zugesagten Sicherheitsfunktionen im Rahmen spezieller IT–Sicherheitsüberprüfungen regelmäßig zu testen.

IT–Sicherheitsüberprüfungen

24.1 (1) Die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen zur IT–Sicherheit kann erst durch spezifische IT–Sicherheitsüberprüfungen (Audits) beurteilt werden. Diese – auf einer umfangreichen Risikoanalyse beruhenden – Überprüfungen konnten entweder durch die jeweilige Organisation selbst oder von externen Spezialisten – zum Teil automatisiert – durchgeführt werden. Entsprechend der Vielfalt der möglichen technischen und organisatorischen Sicherheitsmaßnahmen konnte auch eine Vielzahl von IT–Sicherheitsüberprüfungen vorgenommen werden. Diese sollten nicht nur die Wirksamkeit der getroffenen Maßnahmen, sondern auch das Fehlen von Schutzvorkehrungen aufzeigen. Dem Stand der Technik und dem Best Practice der überprüften Bundesministerien entsprachen insbesondere folgende spezifische IT–Sicherheitsüberprüfungen:

- Prozess–Audits zur Betrachtung einzelner Prozesse,
- System–Audits zur Betrachtung des IT–Managementsystems,
- Netzwerk–Audits zur Analyse von Netzwerk, IT und Infrastruktur,
- Social Engineering–Audits zur Überprüfung von Verhaltensregeln von Mitarbeiterinnen und Mitarbeitern,
- Datenschutz–Audits, z.B. zur Überprüfung der Erfüllung der Anforderungen der Datenschutz–Grundverordnung,
- Vulnerability Scannings zur Analyse und Identifizierung von Schwachstellen,
- Penetration Testing und Ethical Hacking zur Überprüfung von Systemen aus der Sicht eines möglichen Angreifers,
- Compliance–Audits zur Überprüfung der Einhaltung von gesetzlichen Vorschriften und Richtlinien im IT–Bereich,
- technische Audits zur Betrachtung technischer Systeme,
- Produkt–Audits zur Betrachtung eines Produkts anhand der Kundenerwartungen und
- Projekt–Audits zur Betrachtung der Einhaltung der Projektvorgaben.

IT–Sicherheitsüberprüfungen sollten regelmäßig durchgeführt werden, um auch aktuelle Bedrohungen im innovativen Bereich der IT–Sicherheit innerhalb eines dem Risiko–Level angemessenen Zeitraums berücksichtigen zu können. Die Standards für IT–Sicherheitsüberprüfungen, die als Maßstab dienten, waren in verschiedenen Regelwerken festgelegt, z.B. in der internationalen Norm ISO/IEC 27001[13], im Informationssicherheitshandbuch oder in den vom deutschen Bundesamt für Sicherheit in der Informationstechnik (**BSI**) entwickelten IT–Grundschutzkatalogen; diese beschrieben u.a. die Vorgehensweise zum Identifizieren und Umsetzen von Sicher-

[13] Die Norm ISO/IEC 27001 spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagement–Systems (**ISMS**).

heitsmaßnahmen der IT mit dem Ziel, ein mittleres, angemessenes und ausreichendes Schutzniveau für IT–Systeme zu erreichen.

Die überprüften Bundesministerien gaben an, betreffend die im jeweiligen Bundesministerium betriebenen IT–Systeme IT–Sicherheitsüberprüfungen durchgeführt zu haben bzw. in einzelnen Bereichen regelmäßig durchzuführen. Einen Überblick über die im BKA, im BMDW und im BMSGPK durchgeführten Sicherheitsüberprüfungen enthält nachstehende Tabelle:

Tabelle 19: Durchgeführte IT–Sicherheitsüberprüfungen

Art der IT–Sicherheitsüberprüfung	BKA	BMDW	BMSGPK
Prozess–Audits	ja	keine Angabe	ja
System–Audits	ja	keine Angabe	ja
Netzwerk–Audits	ja	ja	ja
Social Engineering–Audits	ja	ja	nein[1]
Datenschutz–Audits	ja	keine Angabe	nein[1]
Vulnerability Scannings	ja	ja	ja
Penetration Testing und Ethical Hacking	ja	ja	ja (Bereich Gesundheit); nein (Bereich Soziales)
Compliance–Audits	ja	keine Angabe	nein[2]
technische Audits	ja	ja	ja
Produkt–Audits	ja	ja	ja
Projekt–Audits	ja	nein	keine Angabe

[1] Keine Audits, aber bei der Ausbildung bzw. Grundausbildung berücksichtigt; darüber hinaus war das DSGVO–Grundlearning–Tool von allen Bediensteten anhand einer Onlinetestung zu absolvieren.
[2] Neben der Grundausbildung wurde zwischenzeitlich den Bediensteten das E–Learning–Programm „Umgang mit klassifizierten Informationen“ mit der Möglichkeit der Selbstzertifizierung zur Verfügung gestellt.

Quellen: BKA; BMDW; BMSGPK

(2) Im Einzelnen war zu den Ressorts Folgendes auszuführen:

(a) Das BKA hatte die in Tabelle 19 angeführten Arten von IT–Sicherheitsüberprüfungen – bzw. Sicherheitsüberprüfungen, die diese Aspekte berücksichtigen – durchgeführt, beispielsweise ein Produkt–Audit im Jahr 2018, ein Vulnerability–Scan im Jahr 2019 und jährliche Penetration Tests. Nach Auskunft des BKA wurden die aus den Überprüfungen ableitbaren Ergebnisse bzw. Empfehlungen abgearbeitet und umgesetzt. Weiters setzte das BKA besonders im Bereich des Social Engineering Maßnahmen, um das Risiko von Angriffen in diesem Bereich zu reduzieren.

(b) Das BMDW führte sechs der in Tabelle 19 angeführten Arten der IT–Sicherheitsüberprüfungen durch. Einige Überprüfungen fanden monatlich statt, Produkt–Audits nur vereinzelt. Die Social Engineering–Audits erfolgten im Rahmen von externen IT–Sicherheitsüberprüfungen; diese wurden in größeren Abständen durchgeführt. Laut Auskunft des BMDW war geplant, diese externen IT–Sicherheitsüberprüfungen ab 2020 jährlich vorzunehmen.

Die Ergebnisse und Empfehlungen der IT–Sicherheitsüberprüfungen fanden sich in den Berichten über die monatlichen Vulnerability–Scans sowie über die externen IT–Sicherheitsüberprüfungen. Erstere wurden zeitnah, letztere nur mittel– bis langfristig – im Rahmen der IT–Security Roadmap des BMDW – umgesetzt.

Projekt–Audits wurden im BMDW nicht durchgeführt, zu Datenschutz–Audits machte es keine Angabe. Der IKT–Abteilung des BMDW war nicht bekannt, ob Prozess–, System– und Compliance–IT–Sicherheitsüberprüfungen von anderen Abteilungen des BMDW durchgeführt wurden.

(c) Laut Auskunft des BMSGPK beauftragte der zentrale Dienstleister BRZ GmbH externe Spezialisten, regelmäßig IT–Sicherheitsüberprüfungen bezüglich bestimmter IT–Komponenten im Bereich Soziales durchzuführen; diese umfassten auch System–, Netzwerk–, technische und Vulnerability–Audits. Im Bereich Gesundheit wurden die gesundheits– und veterinärbehördlichen Informationssysteme laufend internen und gegebenenfalls externen IT–Sicherheitsüberprüfungen und Penetration Tests unterzogen. Weitere Unterlagen zur Art der IT–Sicherheitsüberprüfungen konnte die IT–Abteilung Gesundheit nicht zur Verfügung stellen.

24.2 Der RH anerkannte die im BKA durchgeführten IT–Sicherheitsüberprüfungen.

Er bewertete die im BMDW durchgeführten IT–Sicherheitsüberprüfungen sowie das Ziel, jährliche externe IT–Sicherheitsüberprüfungen vorzunehmen, positiv. Er kritisierte jedoch, dass für die IT–Sicherheit wichtige Überprüfungen (Datenschutz–, Projekt–, Prozess–, System– und Compliance–IT–Sicherheitsüberprüfungen) nicht stattgefunden hatten.

Der RH stellte fest, dass die vom BMSGPK durchgeführten Sicherheitsüberprüfungen wichtige Bereiche der möglichen Audits abdeckten; um die Wirksamkeit der im Bundesministerium getroffenen technischen (Sicherheits–)Maßnahmen zu beurteilen, wären Sicherheitsüberprüfungen in allen Bereichen, beispielsweise auch hinsichtlich der vorliegenden Endpoint–Protection–Lösung, regelmäßig durchzuführen.

Der RH empfahl dem BMDW und dem BMSGPK, den Bedarf an IT–Sicherheitsüberprüfungen in den verschiedenen Bereichen festzustellen und auf dieser Grundlage ein mittelfristiges Konzept zu entwickeln und umzusetzen.

Der RH stellte kritisch fest, dass das BMDW keinen ressortweiten konsolidierten Überblick zu IT–Sicherheitsüberprüfungen hatte.

Daher empfahl er dem BMDW, Informationen zu allen im Ressort stattfindenden IT–Sicherheitsüberprüfungen zentral in einer einzigen Organisationseinheit zusammenzuführen.

24.3 (1) Laut Stellungnahme des BMDW seien Bedarf und konkrete Ausgestaltung von IT–Sicherheitsüberprüfungen im sogenannten Sicherheitskonzept, das auf den Ergebnissen der Informationssicherheits– und Datenschutzrisikoanalyse basiere, pro IT–Verfahren vor Projektbeginn festzulegen. Die Einhaltung und Durchführung der dort definierten IT–Sicherheitsüberprüfungen verantworte der zuständige Betriebsmanager in der jeweiligen Fachabteilung. Vorlagen zur Informationssicherheits– und Datenschutzrisikoanalyse sowie zum Sicherheitskonzept würden Passagen zu IT–Sicherheitsüberprüfungen beinhalten. Die zentrale Vorgabe besage daher, dass sich Projekt– und Betriebsmanager verpflichtend dieses Themas annehmen müssten. Zentrale und einheitliche Vorgaben zur Ausgestaltung von IT–Sicherheitsüberprüfung seien aufgrund der Diversität der IT–Verfahren nicht zielführend.

Zur Zusammenführung von Informationen zu allen im Ressort stattfindenden IT–Sicherheitsüberprüfungen teilte das BMDW mit, dass die Notwendigkeit von IT–Sicherheitsüberprüfungen pro IT–Verfahren auf Basis der für das IT–Verfahren geltenden Betriebserträge bewertet würde. Für die Einhaltung der IT–Sicherheit sowie der Durchführung von IT–Sicherheitsüberprüfungen seien die jeweiligen Betriebsmanager in den Fachabteilungen der Sektion I „Digitalisierung und E–Government“ zuständig. Die formelle Einbindung des Chief Information Security Officers (CISO) in laufende und geplante IT–Sicherheitsüberprüfungen werde evaluiert.

(2) Das BMSGPK teilte in seiner Stellungnahme mit, dass es – wie auch vom RH festgestellt – regelmäßig Sicherheitsaudits durchführe. Es sei beabsichtigt, unter Berücksichtigung der vorhandenen Ressourcen diese Aktivitäten zu verstärken und den Empfehlungen entsprechend mittelfristig ein diesbezügliches Konzept zu entwickeln und umzusetzen.

24.4 Der RH entgegnete dem BMDW, dass zur Gewährleistung der IT–Sicherheit auch solche IT–Sicherheitsüberprüfungen durchzuführen sind, welche nicht direkt einem IT–Verfahren oder einem Projekt zuzuordnen sind, z.B. Social Engineering–Audits oder Datenschutz–Audits. Weiters wies der RH darauf hin, dass eine Festlegung des Bedarfs sowie die konkrete Ausgestaltung von IT–Sicherheitsüberprüfungen pro IT–Verfahren vor Projektbeginn das Risiko aktueller Bedrohungen mitunter nicht abdecken; vielmehr ist eine regelmäßige Analyse notwendig, um auch aktuelle Entwicklungen und Risiken abdecken zu können. Ergänzend hielt der RH fest, dass das BMDW bezüglich einiger Arten von IT–Sicherheitsüberprüfungen keine Angaben machen konnte.

Der RH stellte nochmals fest, dass die Informationen zu allen im BMDW stattfindenden IT–Sicherheitsüberprüfungen zur Zeit der Gebarungsüberprüfung nicht zentral zusammengeführt wurden. Er hielt daher die Einbindung des Chief Information Security Officers (CISO) in laufende und geplante IT–Sicherheitsüberprüfungen für zweckmäßig.

IT–Notfallmanagement

Szenarien und Organisation

25.1 (1) Der RH überprüfte das Notfallmanagement der in den überprüften Bundesministerien betriebenen IT–Systeme und IT–Dienste anhand der Notfallszenarien und Notfallorganisation, der kritischen IT–Systeme, IT–Verfahren bzw. IT–Dienste und Notfallprozesse (TZ 26) und der Überprüfung des Notfallmanagements (TZ 27) und orientierte sich hierbei an den Inhalten des Informationssicherheitshandbuches bzw. des BSI–Standards (100–4) zum Notfallmanagement.

Die nachfolgende Tabelle stellt dar, welche Notfallszenarien zur Sicherstellung der Kontinuität des IT–Betriebs die Bundesministerien für die intern betriebenen IT–Systeme und IT–Dienste definierten und welche Notfallorganisation sie dafür eingerichtet hatten (die in der BRZ GmbH betriebenen IT–Verfahren, –Systeme und –Dienste waren nicht Gegenstand der Gebarungsüberprüfung):

Tabelle 20: Notfallszenarien, Notfallorganisation für die in den überprüften Bundesministerien betriebenen IT–Systeme und IT–Dienste

	BKA	BMDW	BMSGPK
IT–Notfallhandbuch	nicht vorhanden	nicht vorhanden	vorhanden
IT–Notfallszenarien/IT–Notfallpläne	teilweise vorhanden (für zwei konkrete Szenarien: DDoS, Komplettausfall Rechenzentrum)	nicht vorhanden	vorhanden (für die definierten wichtigen IT–Systeme bzw. –Dienste)
Definition der Kriterien für den Eintritt eines IT–Notfalls	nicht klar definiert	nicht vorhanden	vorhanden
Definition einer IT–Notfallorganisation (Festlegung zuständiger Organisationseinheiten)	teilweise vorhanden (hinsichtlich Meldeverpflichtungen im Falle von Cyberbedrohungen sowie gemäß NISG, DSGVO und InfoSiG; nur in Ausnahmefällen anlassbezogene Einsatzstäbe mit Schlüsselpersonal)	nicht vorhanden	vorhanden

BRZ GmbH = Bundesrechenzentrum Gesellschaft mit beschränkter Haftung
DDoS = Distributed Denial of Service
DSGVO = Datenschutz–Grundverordnung
InfoSiG = Informationssicherheitsgesetz
NISG = Netz– und Informationssystemsicherheitsgesetz

Quellen: BKA; BMDW; BMSGPK

(2) Das BKA hatte für intern betriebene IT–Systeme bzw. IT–Dienste

- kein IT–Notfallhandbuch bzw. ein ähnliches Konzept in Kraft,
- zur Zeit der Gebarungsüberprüfung zwei definierte IT–Notfallpläne bzw. IT–Notfallszenarien (DDoS–Attacken, Rechenzentrumsausfall) ausgewiesen,
- die Kriterien für den Eintritt eines IT–Notfalls nicht klar definiert und
- die IT–Notfallorganisation nicht eigens festgelegt, sondern diese auf die Meldeverpflichtungen gemäß NISG, DSGVO und InfoSiG beschränkt; nur in sogenannten „Ausnahmefällen“ wurde eine eigene IT–Notfallorganisation anlassbezogen mit Schlüsselpersonal eingerichtet (z.B. während der COVID–19–Pandemie).

(3) Das BMDW hatte für die intern betriebenen IT–Systeme und IT–Dienste

- kein IT–Notfallhandbuch bzw. ein ähnliches Konzept in Kraft,
- keine IT–Notfallpläne bzw. IT–Notfallszenarien für die eigenen IT–Systeme definiert,
- die Kriterien für den Eintritt eines IT–Notfalls nicht definiert und
- die IT–Notfallorganisation dafür nicht festgelegt.

(4) Das BMSGPK hatte ein IT–Notfallhandbuch mit IT–Notfallplänen für wichtige IT–Systeme und IT–Dienste in Kraft. Darin waren Kriterien für den Eintritt eines IT–Notfalls, ein Maßnahmenplan und eine IT–Notfallorganisation festgelegt.

Allerdings wies das IT–Notfallhandbuch einzelne formale Mängel auf, etwa eine falsche Bezeichnung der Szenarien für das Gesundheitsberuferegister oder eine nicht aktuelle Liste von Ansprechpartnern.

25.2 Der RH stellte kritisch fest, dass das BKA die Notfallszenarien für intern betriebene IT–Systeme bzw. IT–Dienste nicht ausreichend festgelegt hatte (kein IT–Notfallhandbuch, nur zwei IT–Notfallszenarien, keine klaren Kriterien für den Eintritt von IT–Notfällen, keine eigene IT–Notfallorganisation).

Er kritisierte, dass im BMDW Notfallkonzepte, etwa IT–Notfallhandbücher, IT–Notfallszenarien oder IT–Notfallpläne für die intern betriebenen IT–Systeme bzw. IT–Dienste nicht vorhanden waren.

Der RH empfahl dem BKA und dem BMDW, für die intern betriebenen IT–Systeme und IT–Dienste ein IT–Notfallhandbuch mit allen wichtigen IT–Notfallszenarien zu erstellen und darin klare Kriterien für den Eintritt von IT–Notfällen und eine eigene IT–Notfallorganisation festzulegen.

Der RH merkte an, dass das vorhandene IT–Notfallhandbuch des BMSGPK einzelne formale Mängel hinsichtlich der Aktualität aufwies.

Er empfahl dem BMSGPK, das IT–Notfallhandbuch zu aktualisieren.

25.3 (1) Das BKA gab in seiner Stellungnahme an, dass sich die Empfehlung im Rahmen des internen „Information Security Management System"–Projekts bereits in Umsetzung befinde.

(2) Das BMDW hielt in seiner Stellungnahme fest, dass die Entwicklung eines IT–Notfallhandbuchs als Aufgabe des Informationssicherheitsmanagement–Teams eingeplant werde.

(3) Das BMSGPK sagte die Umsetzung im Rahmen der Aktualisierung des IT– Notfallhandbuchs zu.

Kritische IT–Systeme, IT–Verfahren, IT–Dienste und Notfallprozesse

26.1 (1) Die Bundesministerien definierten die für die Gewährleistung der IT–Sicherheit kritischen IT–Verfahren, IT–Dienste und IT–Systeme. Darauf aufbauend sollte eine Risikobewertung anhand der definierten Notfallszenarien erfolgen. Diese sollte Grundlage der festzulegenden IT–Notfallprozesse und Maßnahmen sein.

Der nachfolgenden Tabelle ist zu entnehmen, ob die überprüften Bundesministerien intern betriebene kritische IT–Systeme und IT–Dienste definiert hatten und welche Maßnahmen und Prozesse im Notfall dafür vorgesehen waren:

Tabelle 21: Kritische Systeme und Notfallprozesse für intern betriebene IT–Systeme und IT–Dienste

	BKA	BMDW	BMSGPK
Definition der kritischen IT–Systeme bzw. –Dienste	durchgeführt	durchgeführt	durchgeführt
Definition der IT–Notfallprozesse	teilweise vorhanden (nur hinsichtlich Meldeverpflichtungen bei Cyberbedrohungen und gemäß NISG, DSGVO und InfoSiG, nicht hinsichtlich anderer Notfälle)	nicht vorhanden	vorhanden (inklusive Verantwortlichkeiten und Kommunikationswegen)
Wiederherstellungsverfahren	grundsätzlich definiert für Daten; umfassende Konzepte noch nicht vorhanden (z.B. Desaster Recovery Konzept, Datensicherungskonzept)	definiert	definiert
Systeme zur laufenden Überwachung sowie Dokumentation durch Berichtswesen	vorhanden (für alle kritischen IT–Systeme)	vorhanden (für alle kritischen IT–Systeme)	vorhanden (für alle kritischen IT–Systeme)

DSGVO = Datenschutz–Grundverordnung
InfoSiG = Informationssicherheitsgesetz
NISG = Netz– und Informationssystemsicherheitsgesetz

Quellen: BKA; BMDW; BMSGPK

(2) Notfallprozesse der drei Bundesministerien:

(a) Das BKA hatte für intern betriebene IT–Systeme bzw. IT–Dienste

- IT–Meldeprozesse für IT–Notfälle – abgesehen von Meldeverpflichtungen aus den im NISG, InfoSiG und in der DSGVO genannten Gründen – noch nicht vorgesehen,
- einzelne Wiederherstellungsverfahren (z.B. für die Verlegung des IT–Betriebs von einem Rechenzentrumstandort auf einen anderen) definiert, allerdings umfassende bzw. weitergehende Konzepte (Business Continuity Management Konzept, Desaster Recovery Konzept, Datensicherungskonzept) der IT–Sicherheit noch nicht formuliert.

(b) Das BMDW erstellte für die internen IT–Systeme und IT–Dienste sowie für die interne IT–Infrastruktur ein Ausfallskonzept mit entsprechenden Ausfallsmechanismen im Rahmen des Störungsmanagements, stellte jedoch keine Verknüpfung bzw. Erweiterung zu IT–Notfallszenarien bzw. IT–Notfällen her.

(c) Das IT–Notfallhandbuch des BMSGPK beinhaltete für die wichtigen IT–Systeme bzw. IT–Dienste alle wesentlichen Kriterien, Maßnahmen und organisatorischen Aspekte für die jeweiligen IT–Notfallszenarien.

26.2 Der RH beanstandete, dass im BKA für intern betriebene IT–Systeme bzw. IT–Dienste generelle Meldeprozesse für IT–Notfälle fehlten, die über den Umfang anderer spezieller Meldeprozesse (NISG, DSGVO bzw. InfoSiG) hinausgingen, und dass umfassende Konzepte zur Wiederherstellung eines geregelten Normalbetriebs fehlten (z.B. Datensicherungskonzept, Desaster Recovery Konzept).

Er empfahl daher dem BKA, die generellen Meldeprozesse für IT–Notfälle (neben den bereits bestehenden Meldeprozessen nach NISG, DSGVO bzw. InfoSiG) zu erweitern und die im Einzelfall (Business Continuity Management Konzept, Desaster Recovery Konzept, Datensicherungskonzept) fehlenden Konzepte zur IT–Sicherheit bzw. zur Wiederherstellung eines geregelten IT–Normalbetriebs zu erstellen.

Der RH wies kritisch darauf hin, dass das BMDW zwar für die intern betriebenen IT–Systeme, IT–Dienste und IT–Infrastruktur umfangreiche Ausfallskonzepte hatte, allerdings aufgrund fehlender Notfallszenarien und Notfallpläne keine Verknüpfung zum Notfallmanagement herstellte.

Er wiederholte daher seine Empfehlung aus TZ 25 an das BMDW, für die intern betriebenen IT–Systeme und IT–Dienste ein IT–Notfallhandbuch mit allen wichtigen IT–Notfallszenarien zu erstellen und darin klare Kriterien für den Eintritt von IT–Notfällen und eine eigene IT–Notfallorganisation festzulegen.

26.3 (1) Laut Stellungnahme des BKA befinde sich diese Empfehlung im Rahmen des internen „Information Security Management System"–Projekts bereits in Umsetzung.

(2) Das BMDW hielt in seiner Stellungnahme fest, dass die Entwicklung eines IT–Notfallhandbuchs als Aufgabe des Informationssicherheitsmanagement–Teams eingeplant werde.

Überprüfung des IT–Notfallmanagements

27.1 (1) Die nachfolgende Tabelle gibt einen Überblick, ob regelmäßige Testungen und Überprüfungen des IT–Notfallmanagements in den Bundesministerien durchgeführt wurden:

Tabelle 22: Überprüfung Notfallmanagement für die intern betriebenen IT–Systeme und IT–Dienste

	BKA	BMDW	BMSGPK
Testung Notfallszenarien	regelmäßige Standort-abschaltungen im Zuge von Wartungsarbeiten	mit privatem IT–Dienstleister vereinbarte Notfalltestung zuletzt 2015	keine Notfalltestungen bei eigenen IT–Services
Überprüfungen (Audits hinsichtlich Notfallmanagement)	nicht hinsichtlich des eigenen Notfallmanagements; regelmäßig hinsichtlich des IT–Notfallmanagements der externen IT–Dienstleister[1]		

[1] z.B. vorgesehen durch die ISO/IEC 27001–Rezertifizierungen

Quellen: BKA; BMDW; BMSGPK

(2) (a) Das BKA überprüfte im Zuge von Wartungsarbeiten das Notfallszenario eines IT–Rechenzentrumstandortwechsels. Darüber hinaus fanden aufgrund fehlender Notfallszenarien keine Tests bzw. Übungen statt.

Das BKA beauftragte in regelmäßigen Abständen IT–Sicherheitsaudits durch externe Unternehmen.

(b) Die letzte IT–Notfalltestung im Betrieb des BMDW fand im Jahr 2015 statt, obwohl im Vertrag mit dem betriebsverantwortlichen IT–Dienstleister drei IT–Notfalltestungen innerhalb von fünf Jahren vorgesehen waren.

Auch das BMDW ließ in regelmäßigen Abständen IT–Sicherheitsaudits durch externe Unternehmen durchführen.

(c) Beim BMSGPK erfolgte noch keine Testung bzw. Überprüfung der vorhandenen IT–Notfallpläne.

Das BMSGPK ließ lediglich im Bereich Gesundheit externe Audits zur IT–Sicherheit durchführen. Allerdings bezogen sich diese Audits nicht explizit auf das IT–Notfallmanagement.

(3) Die von den überprüften Bundesministerien beauftragten IT–Dienstleister führten im Rahmen ihrer Zertifizierung zur Informationssicherheit (ISO/IEC 27001) auch Auditierungen des eigenen IT–Notfallmanagements durch.

27.2 Der RH stellte kritisch fest, dass

- das BKA aufgrund fehlender Notfallszenarien das Notfallmanagement nicht ausreichend testete,
- das BMDW die mit dem IT–Dienstleister vertraglich vereinbarten Testungen nicht regelmäßig durchführen ließ und
- das BMSGPK bisher noch keine Testungen bzw. Überprüfungen der definierten Notfallszenarien durchführte.

Er empfahl daher dem BKA, dem BMDW und dem BMSGPK, die IT–Notfallszenarien regelmäßig mit IT–Notfallübungen auf ihre Wirksamkeit zu überprüfen.

Der RH stellte kritisch fest, dass das IT–Notfallmanagement des BKA, des BMDW und des BMSGPK in den extern beauftragten IT–Audits nie Bestandteil der Überprüfungen war.

Er empfahl daher dem BKA, dem BMDW und dem BMSGPK, das IT–Notfallmanagement künftig auch in externen IT–Audits zu berücksichtigen.

27.3 (1) Laut Stellungnahme des BKA werde eine Umsetzungsstrategie zu den Empfehlungen ausgearbeitet.

(2) Das BMDW führte in seiner Stellungnahme aus, dass die Einrichtung regelmäßiger IT–Notfallübungen als Aufgabe des Informationssicherheitsmanagement–Teams eingeplant werde. Eine Notfallübung (Disaster Recovery Test) hätte im BMDW zuletzt im Februar 2021 stattgefunden. Das Notfallmanagement in externen IT–Audits werde das BMDW berücksichtigen und auch hinsichtlich seiner Effizienz evaluieren. Eine Notfallübung, welche das Krisenhandbuch und die darin definierten Rollen im Bereich IT–Sicherheit teste, sei bereits in Ausarbeitung.

(3) Das BMSGPK hielt in seiner Stellungnahme fest, dass den Empfehlungen unter Berücksichtigung der vorhandenen Ressourcen entsprochen werde.

Eine von der EU–Agentur für Cybersicherheit (ENISA) für 2020 anberaumte, grenzüberschreitende Cybersicherheitsübung für den Gesundheitssektor sei aufgrund der Auslastung durch die Pandemiebekämpfung einstweilen auf 2022 verschoben worden. An dieser Übung hätten für Österreich neben dem BMSGPK auch drei Bundesländer, Krankenhausbetreiber sowie Arzneimittel– und Medizingerätehersteller teilnehmen sollen, um die gemeinsame Abwehr von Cyberangriffen auf Supply Chains im Gesundheitssektor zu trainieren.

IT–Sicherheit ausgewählter Einzelsysteme

28 Der RH überprüfte stichprobenartig das Management der IT–Sicherheit an jeweils zwei Einzelsystemen des BKA, des BMDW und des BMSGPK. Die ausgewählten Einzelsysteme wurden entweder als IT–Verfahren bzw. IT–Dienst für die Zentralstelle des Bundesministeriums vom Dienstleister BRZ GmbH bezogen oder vom jeweiligen Bundesministerium selbst betrieben.

Daher waren das Management der IT–Sicherheit in den Dienstleistern (etwa der BRZ GmbH oder der Statistik Austria) der drei Bundesministerien sowie die von diesen Dienstleistern allgemein betriebenen Verfahren – wie beispielsweise das Unternehmensserviceportal, das Ergänzungsregister für sonstige Betroffene oder das Portal Österreich.gv.at (mit den u.a. vorgesehenen Anwendungen Beantragung Wahlkarte, Änderung im Melderegister, Änderung im Kraftfahrzeugregister, Beantragung einer Staatsbürgerschaft, Beantragung eines Reisepasses) – nicht Thema dieser Gebarungsüberprüfung.

Grundlage der Überprüfung der Einzelsysteme in den drei Bundesministerien war ein Fragenkonzept zu den Themenbereichen der IT–Sicherheit, wie sie im Informationssicherheitshandbuch sowie im ISO/IEC 27001–Standard „Informationssicherheitsmanagement“ dargestellt waren. Dies betraf etwa die Themen Zugriffskontrolle, Schutz vor Schadsoftware, personelle IT–Sicherheit, Netzwerk, Störungsmanagement oder Notfallmanagement. Die folgende Tabelle beschreibt für diese Überprüfung ausgewählte wesentliche Themenbereiche der IT–Sicherheit:

Tabelle 23: Ausgewählte Aspekte der IT–Sicherheit

Nr.	Themenbereich	Kurzbeschreibung
1	Management von Vermögenswerten	Systemkomponenten (Inventar) sollen bekannt und Verantwortlichkeiten dazu geregelt sein.
2	technisches Schwachstellen-management des Systems/ Verfahrens (z.B. wenn System aus vielen Komponenten Hardware/Software besteht)	Auf Grundlage der Systemkomponenten sollen mögliche Schwachstellen erkannt werden.
3	Informationsklassifizierung	Beschreibung, welche Informationen auf dem System verarbeitet werden, um den Schutzbedarf des Systems selbst festlegen zu können
4	Funktionstrennung und personelle Sicherheit	Eine Funktionstrennung soll die Unvereinbarkeit von Funktionen in einer Person (z.B. Buchung und Freigabe der Buchung) vermeiden. Die Regelungen zur personellen Sicherheit legen die Rahmenbedingungen für die sichere Arbeit der Bediensteten mit der IT fest.
5	Anforderungen in Bezug auf die Zugriffskontrolle	IT–sicherheitsrelevante Aspekte der Benutzer– und Berechtigungsverwaltung (geregelter Vergabeprozess, Identifizierung am System und Kontrolle)
6	Malwareschutz	Schutz vor Schadsoftware
7	Kryptografie – Verschlüsse-lungsverfahren	Verschlüsselung soll zum Schutz des IT–Systems in Abhängigkeit vom Schutzbedarf eingesetzt werden.
8	Trennung der Entwicklungs–, Test– und Betriebsumgebung	Eine Trennung der Entwicklungs–, Test– und Betriebsumgebung soll das Risiko von unautorisierten Zugriffen verringern.
9	Zugriffskontrolle auf Quelltexte	Zugriffe auf den Quelltext sollen in einer kontrollierten und sicheren Umgebung stattfinden.
10	Betriebsverfahren und Zuständigkeiten	Die Systemadministration und –betreuung sollen klar geregelt sein und einer Kontrolle unterliegen.
11	Ressourcenmanagement	Management von Ressourcen wie Verfügbarkeit, Auslastung oder Effizienz von Systemen inklusive Kontrollmechanismen
12	Back–up	Konzeption und Einsatz von Sicherungsmechanismen für Daten und Systeme
13	Logging und Monitoring	automatisierte Protokollierung und Überwachung von Systemen und Zugriffen sowie systematische Auswertungen (etwa nach Abweichungen, Fehlermeldungen)
14	Betriebssoftwarekontrolle	Überwachung und Kontrolle von Änderungen auf Ebene der Betriebssysteme sowie eingesetzte Sicherheitsmechanismen
15	Sicherheitsmanagement in der Kommunikation (Einbettung des Systems/Verfahrens im Netzwerk)	Maßnahmen der IT–Sicherheit im Netzwerk bezogen auf das IT–System
16	Sicherheit in Entwicklung, Betrieb und Wartung eines IT–Systems	Berücksichtigung der IT–Sicherheitsanforderungen von Erwerb bzw. Entwicklung bis zur Wartung und deren vertragliche Festlegung
17	Schutz der Datenübertragung von Anwendungen und Diensten	Sicherheitsmechanismen bei Datenübertragungen im IT–Verbund (z.B. elektronische Signaturen, Authentifizierung, sichere Verbindungen)
18	Richtlinie zur sicheren Entwicklung	Vorgaben unter Berücksichtigung von IT–sicherheitsrelevanten Aspekten in der Entwicklung von Systemen (z.B. Entwicklungsrichtlinien)
19	Softwareänderungskontrolle	definierter Prozess zur Kontrolle für sichere Softwareänderungen und deren Dokumentation
20	Richtlinien zur sicheren Systemerstellung	Vorgaben, wie die IT–Sicherheit bei Erstellung bzw. Implementierung aufgebaut sein soll

Nr.	Themenbereich	Kurzbeschreibung
21	sichere Entwicklungs-umgebung	Vorgaben an die eingesetzte Entwicklungsumgebung, um die IT–Sicherheit auch bei den eingesetzten Entwicklungswerkzeugen ausreichend zu berücksichtigen
22	Outsourcing der Entwicklung	Berücksichtigung von IT–sicherheitsrelevanten Aspekten in den vertraglichen Regelungen (z.B. Lizenzvereinbarungen) bei der Auslagerung von Entwicklungs-tätigkeiten
23	Systemabnahmetests	Vorgaben für IT–sicherheitsrelevante Maßnahmen bei Testung und Abnahme vor Produktivsetzung
24	Testdaten	Vorgaben zur Beschaffenheit von und zum Umgang mit Testdaten auf Nicht–Produktivsystemen (z.B. Pflicht zur Anonymisierung, eigens erstellte Testdatensätze, Löschung)
25	Regelungen von IT–sicher-heitsrelevanten Aspekten mit dem Lieferanten (Informati-onsschutz, Verfügbarkeiten, Kontrollmechanismen, Risiko, Änderungsmanagement)	Regelungen der Lieferantenbeziehungen insbesondere im Hinblick auf IT–sicherheitsrelevante Pflichten und Leistungsvereinbarungen während der gesamten Zusammenarbeitsphase (Umgang mit Informationen, Lieferungen und Leistungen, Risikovereinbarungen, Leistungsabweichungen etc.)
26	Störungsmanagement	Vorgaben zu Verfahren und Prozessen im Störungsbetrieb, die eine ausreichende IT–Sicherheit des IT–Systems gewährleisten sollen
27	IT–Sicherheit im betrieblichen Kontinuitätsmanagement	Pläne, Reaktions– bzw. Wiederherstellungsverfahren bei schädigenden Ereignissen (z.B. IT–Notfälle)
28	Compliance	Berücksichtigung aller gesetzlichen, vertraglichen bzw. sonstigen IT–sicherheits-relevanten Vorgaben
29	Überprüfung der Einhaltung technischer Vorgaben	regelmäßige Kontrolle und Dokumentation der IT–sicherheitsrelevanten technischen Vorgaben

Quelle: Informationssicherheitshandbuch

Der RH überprüfte im BKA die Systeme „SAP Smart Data Hana Plattform“ und „Medienakkreditierung“, im BMDW die Systeme „ELAK“ und „Baukostenindex“ und im BMSGPK die Systeme „Mailservice“ und „Gesundheitsberuferegister“ anhand der in Tabelle 23 angeführten sicherheitsrelevanten Maßnahmen. Bei einzelnen Aspekten der IT–Sicherheit zeigte der RH in seinem Bericht Verbesserungspotenziale in diesen Applikationen auf. Das BKA, das BMDW und das BMSGPK sagten in ihren Stellungnahmen die Umsetzung der Verbesserungspotenziale zu.

Schlussempfehlungen

29 Im Zusammenhang mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport verwies der RH auf seine Ausführungen in TZ 4.

Zusammenfassend empfahl der RH:

		Bundeskanzleramt	Bundesministerium für Digitalisierung und Wirtschaftsstandort	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport
(1)	Es wäre eine Regierungsvorlage zu erarbeiten, mit der im Bundesministeriengesetz eine Kompetenz zur Koordination der IT–Sicherheit klar und ausdrücklich festgelegt wird. (TZ 2)	X	X		
(2)	Es wäre die im IKT–Konsolidierungsgesetz vorgesehene Verordnung zu erlassen. (TZ 3)		X		
(3)	In einem Projekt wäre die Konsolidierung der IT–Ausstattung der Arbeitsplätze des Ressorts zu behandeln, um die Kosten der IT–Beschaffung und der Lizenzgebühren zu reduzieren, die Heterogenität der generellen Bürosoftwareausstattung zu verringern und die Betreuung der IT–Ausstattung der Arbeitsplätze zu bündeln. Die Verwendung einheitlicher Bürosoftware sowie die einheitliche und zeitgerechte Installierung der zugehörigen Sicherheits–Updates ermöglichen auch die Bündelung des für die IT–Sicherheit zuständigen Personals und können dazu einen Beitrag zur Erhöhung der IT–Sicherheit leisten. (TZ 3, TZ 13)	X	X	X	X
(4)	Das Management der IT und deren Sicherheit wären so zu gestalten, dass die grundlegenden Aufgaben der IT–Sicherheit vom Ressort selbst wahrgenommen werden können. (TZ 4)				X

		Bundeskanzleramt	Bundesministerium für Digitalisierung und Wirtschaftsstandort	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
(5)	In der geplanten neuen „Österreichischen Strategie für Cyber Sicherheit“ wären auch die Standards in Bezug auf die IT–Sicherheit festzulegen. (TZ 5)	X		
(6)	Es wäre eine Regierungsvorlage zu erarbeiten, welche ein einheitliches Regelungssystem zur elektronischen Verarbeitung klassifizierter Informationen für den internationalen und nationalen Geheimschutz schafft. (TZ 6)	X		
(7)	In der IT–Sicherheitsstrategie wäre auch die Verantwortung der obersten Führungsebene für die IT–Sicherheit zu definieren und die IT–Sicherheitsstrategie allen Bediensteten aktiv kundzumachen. (TZ 7)	X		
(8)	Die IT–Sicherheitsstrategie wäre zu aktualisieren, ihr Geltungsbereich umfassend festzulegen und alle nachgeordneten Dienststellen miteinzubeziehen. (TZ 7)		X	
(9)	Ein IT–spezifisches Risikomanagementsystem wäre einzuführen. (TZ 8)	X		
(10)	Die noch offenen Informationssicherheits– und Datenschutz–Risikoanalysen wären durchzuführen. (TZ 8)		X	
(11)	Das geplante umfassende und standardisierte Berichtswesen zur IT–Sicherheit wäre einzuführen und dabei auch die Struktur des internen Berichtswesens, insbesondere der konkrete Berichtsweg, und die notwendigen Inhalte festzulegen. (TZ 9)	X		
(12)	Die Struktur des internen Berichtswesens zur IT–Sicherheit und insbesondere der konkrete Berichtsweg und die Berichtsempfänger wären festzulegen. (TZ 9)		X	X
(13)	Die für die Bereiche „Soziales“ und „Gesundheit“ getrennten „Sicherheits– und Betriebsberichte“ wären im Sinne der Beschreibung der Sicherheitslage des gesamten Bundesministeriums zusammenzuführen. (TZ 9)			X
(14)	Die Agenden für die Steuerung der IT und der IT–Sicherheit des Ressorts wären zusammenzufassen und unter eine einheitliche Führung zu stellen. (TZ 10, TZ 11)			X
(15)	Für die gesamte Informations– und IT–Sicherheit wäre ein verantwortlicher fachkundiger Chief Information Security Officer (CISO) einzurichten. (TZ 11)		X	X

		Bundeskanzleramt	Bundesministerium für Digitalisierung und Wirtschaftsstandort	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
(16)	Im Rahmen der Überarbeitung der Cybersicherheitsstrategie wäre darauf hinzuwirken, auch im darauf beruhenden Informationssicherheitshandbuch die Aufgaben des IT–Sicherheitsbeauftragten derart anzupassen, dass dieser für die Agenden der IT–Sicherheit zuständig ist. Weiters wäre die Funktion des Chief Information Security Officers als Verantwortlicher für die gesamte Informations– und IT–Sicherheit als gemeinsamer Standard für alle Bundesministerien zu verankern und von der Funktion des Chief Information Officers (CIO) zu trennen. (TZ 11)	X		
(17)	Die Funktion des Chief Digital Officers (CDO) wäre rasch zu besetzen. (TZ 11)			X
(18)	Das geplante Informationssicherheitsmanagement–Team wäre einzurichten; dabei wäre auf eine zweckentsprechende Einbindung der Anwenderinnen und Anwender sowie der nachgeordneten Dienststellen zu achten. (TZ 12)	X		
(19)	Der Vorsitz des Informationssicherheitsmanagement–Teams sollte beim neu einzurichtenden, für die gesamte Informations– und IT–Sicherheit verantwortlichen Chief Information Security Officer (CISO) angesiedelt werden. Eine Mindestsitzungsfrequenz für das Informationssicherheitsmanagement–Team wäre festzulegen und diese auch einzuhalten. (TZ 12)		X	
(20)	Die Zwei–Faktor–Authentifizierung für die Arbeitsplatzrechner wäre flächendeckend zum Einsatz zu bringen. (TZ 14)	X	X	
(21)	Es wäre eine ressortintern einheitliche Softwarelösung für Videokonferenzen vorzusehen. (TZ 15)	X	X	
(22)	Gemeinsam wären einerseits Standards für Videokonferenz–Softwareprodukte zu erstellen, die eine gegenseitige Kommunikation in der Bundesverwaltung sicherstellen und IT–Sicherheitsaspekte besonders berücksichtigen. Andererseits wäre zu evaluieren, ob es eine für alle Ressorts der Bundesverwaltung geeignete Videokonferenz–Software gibt und diese in den Bundesclient–Standard integriert werden kann. (TZ 15)	X	X	
(23)	Die Telearbeit im regulären Dienstbetrieb wäre nur dann standardmäßig vorzusehen, wenn eine geeignete dienstliche IT–Ausstattung zur Verfügung steht und die technischen Sicherheitsvorkehrungen erfüllt sind, um die Risiken für die IT–Sicherheit zu minimieren. (TZ 17)	X	X	X
(24)	Auch im Hinblick auf mögliche weitere Phasen von krisenbedingtem Homeoffice wäre die IT–Ausstattung der Arbeitsplätze künftig so einzurichten, dass in dem zur Aufrechterhaltung des Dienstbetriebs erforderlichen Umfang eine Dienstverrichtung außerhalb der Dienststelle mit dienstlichen Geräten möglich ist. (TZ 17)	X	X	X

		Bundeskanzleramt	Bundesministerium für Digitalisierung und Wirtschaftsstandort	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
(25)	Insbesondere im Hinblick auf einen allfällig neuerlich notwendigen Übergang des Dienstbetriebs auf Homeoffice wären • ausdrückliche organisatorische und technische Vorgaben betreffend die allfällig notwendige Nutzung privater IT–Ausstattung im Netz des Bundesministeriums zu erstellen, • den Bediensteten die in den verschiedenen Regelungen vorgesehenen IT–Sicherheitsmaßnahmen für eine Dienstverrichtung auf IT–Arbeitsplätzen außerhalb der Dienststelle nachweislich zur Kenntnis zu bringen und • festzulegen, ob bestimmte dienstliche Aufgaben jedenfalls aus Sicherheitsgründen an der Dienststelle zu verrichten sind. (TZ 18)	X	X	X
(26)	Richtlinien zur Nutzung mobiler Endgeräte sowie eine zusammenfassende Richtlinie zur Telearbeit wären zu erstellen und in Kraft zu setzen. (TZ 20)	X		
(27)	Regelmäßig wären verpflichtende Awareness–Schulungen zur IT–Sicherheit durchzuführen, die eine nachweisliche Wissensvermittlung, etwa in Form von E–Learning–Kursen mit einer anschließenden Wissensabfrage, sicherstellen sollen. (TZ 21)	X	X	X
(28)	Für das IT–Schlüsselpersonal wären entsprechende Vertretungsregelungen festzulegen und zu dokumentieren, um auch in Krisensituationen und Notfällen einen reibungslosen Ablauf der Geschäftsprozesse sicherzustellen. (TZ 21)	X		
(29)	Beim künftigen Einsatz von externem IT–Personal mit Zugriff auf wichtige Dienste wären die Risiken hinsichtlich der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Bundesministerium verarbeiteten Daten derart zu berücksichtigen, dass der Dienstleister und damit auch das Bundesministerium als Auftraggeber unmittelbar Kontrolle und Überprüfungsmöglichkeiten über das externe IT–Personal hat. Diese unmittelbare Kontrolle und Überprüfungsmöglichkeit können bei einem Dienstort Österreich möglicherweise effektiver sichergestellt werden als bei einem Arbeitsort im EU–Ausland. (TZ 22)		X	
(30)	Der Einsatz eines umfassenden Endpoint–Protection–Systems als Beitrag zur IT–Sicherheit der IT–Arbeitsplätze wäre zu prüfen und ein solches System erforderlichenfalls einzusetzen. (TZ 23)			X
(31)	Es wäre zu evaluieren, ob der Einsatz eines umfassenden Endpoint–Protection–Systems in die Bundesclient–Architektur vorgesehen werden soll, um dadurch einen neuen IT–Sicherheitsstandard für alle Ressorts zu etablieren. (TZ 23)		X	

		Bundeskanzleramt	Bundesministerium für Digitalisierung und Wirtschaftsstandort	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
(32)	Es wäre zu prüfen, ob ein Security Information and Event Management System für den Bereich Soziales einen effektiven Beitrag zur Verbesserung der IT–Sicherheit der IT–Arbeitsplätze mit sich bringen würde; erforderlichenfalls wäre ein derartiges System einzuführen. (TZ 23)			X
(33)	Es wäre zu evaluieren, ob die Einrichtung einer vergleichbaren zentralen Überwachung (Security Operation Center) zum Schutz der IT–Infrastruktur sinnvoll wäre oder ob die laufende Kontrolle der IT–Sicherheit durch andere Einrichtungen sichergestellt ist. (TZ 23)			X
(34)	Es wäre jeweils innerhalb des Ressorts zu prüfen, ob die unterschiedlichen Produkte zum Schutz vor Schadsoftware betreffend die Server und Clients zur Erhöhung der IT–Sicherheit optimiert oder vereinheitlicht werden sollen. (TZ 23)	X	X	X
(35)	Der Bedarf an IT–Sicherheitsüberprüfungen in den verschiedenen Bereichen wäre festzustellen, auf dieser Grundlage wäre ein mittelfristiges Konzept zu entwickeln und umzusetzen. (TZ 24)		X	X
(36)	Informationen zu allen im Ressort stattfindenden IT–Sicherheitsüberprüfungen wären zentral in einer einzigen Organisationseinheit zusammenzuführen. (TZ 24)		X	
(37)	Für die intern betriebenen IT–Systeme und IT–Dienste wäre ein IT–Notfallhandbuch mit allen wichtigen IT–Notfallszenarien zu erstellen; darin wären klare Kriterien für den Eintritt von IT–Notfällen und eine eigene IT–Notfallorganisation festzulegen. (TZ 25, TZ 26)	X	X	
(38)	Das IT–Notfallhandbuch wäre zu aktualisieren. (TZ 25)			X
(39)	Die generellen Meldeprozesse für IT–Notfälle (neben den bereits bestehenden Meldeprozessen nach Netz– und Informationssystemsicherheitsgesetz, Datenschutz–Grundverordnung bzw. Informationssicherheitsgesetz) wären zu erweitern und die im Einzelfall (Business Continuity Management Konzept, Desaster Recovery Konzept, Datensicherungskonzept) fehlenden Konzepte zur IT–Sicherheit bzw. zur Wiederherstellung eines geregelten IT–Normalbetriebs zu erstellen. (TZ 26)	X		
(40)	Die IT–Notfallszenarien wären regelmäßig mit IT–Notfallübungen auf ihre Wirksamkeit zu überprüfen. (TZ 27)	X	X	X
(41)	Das IT–Notfallmanagement wäre künftig auch in externen IT–Audits zu berücksichtigen. (TZ 27)	X	X	X

Rechnungshof Österreich

Wien, im September 2021
Die Präsidentin:

Dr. Margit Kraker

R
H