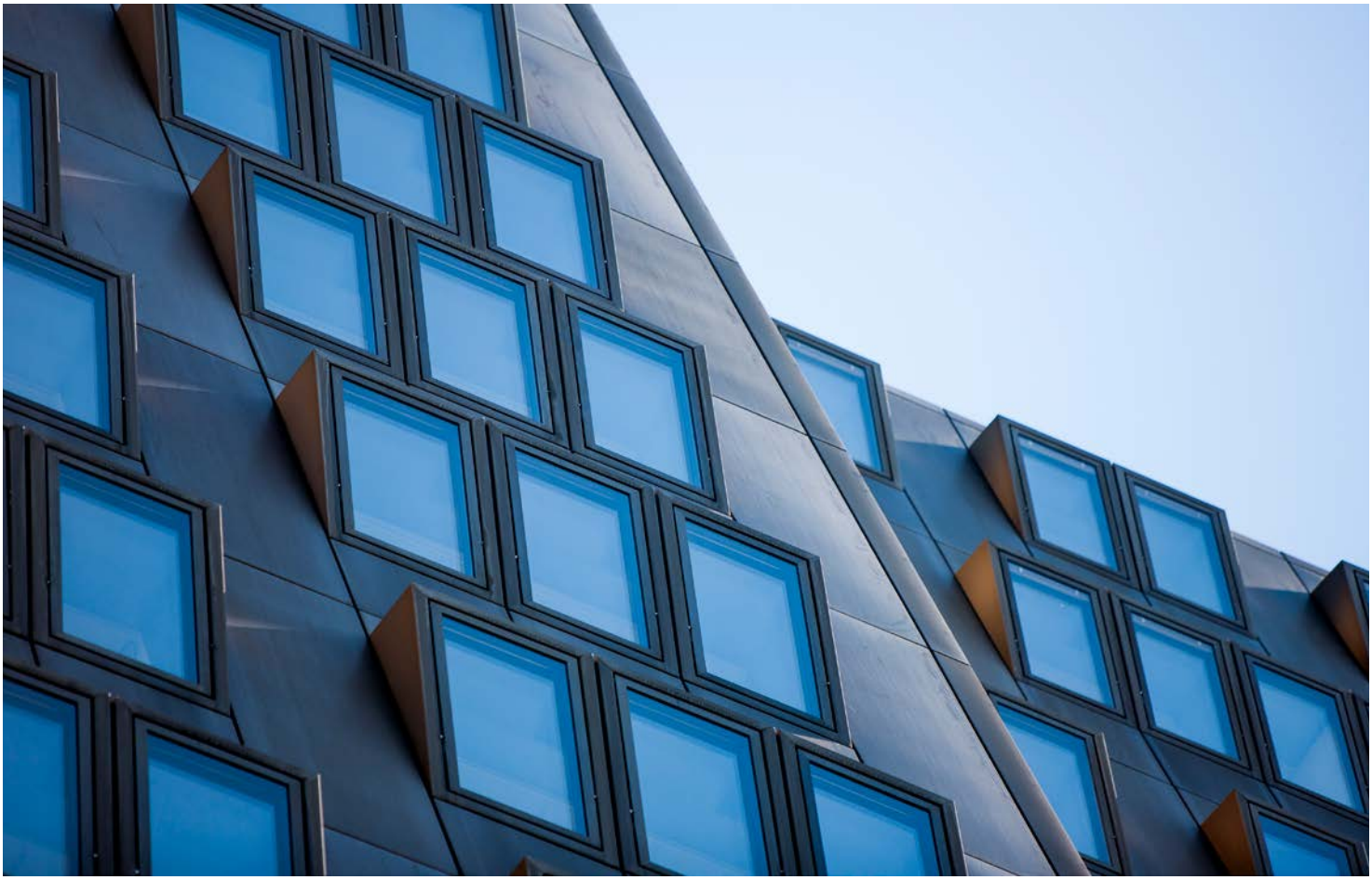
Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Koordination der Cyber–Sicherheit

Reihe BUND 2022/13

Bericht des Rechnungshofes



III–623 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP
Rechnungshof GZ 2022–0.281.048 (004.920)

Vorbemerkungen

Vorlage

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

Berichtsaufbau

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

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

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

IMPRESSUM
Herausgeber:
Rechnungshof Österreich
1030 Wien, Dampfschiffstraße 2
www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im April 2022

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
BGBl.	Bundesgesetzblatt
BKA	Bundeskanzleramt
BlgNR	Beilage zu den stenografischen Protokollen des Nationalrats
BMEIA	Bundesministerium für europäische und internationale Angelegenheiten
BMI	Bundesministerium für Inneres
BMLFUW	Bundesministerium für Land– und Forstwirtschaft, Umwelt und Wasserwirtschaft
BMLV	Bundesministerium für Landesverteidigung
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BRZ GmbH	Bundesrechenzentrum Gesellschaft mit beschränkter Haftung
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
bzw.	beziehungsweise
ca.	circa
CEF	Connecting Europe Facility
CERT	Computer Emergency Response Team (Computer–Notfallteam)
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CSP	Cyber Sicherheit Plattform
CSS	Cyber Sicherheit Steuerungsgruppe
CyCLONe	Cyber Crises Liaison Organisation Network
d.h.	das heißt
DNS	Domain Name System
DSGVO	Datenschutz–Grundverordnung
EECC	European Electronic Communications Code (Europäischer Kodex für die elektronische Kommunikation)
EG	Europäische Gemeinschaft
ELAK	elektronischer Akt
ENISA	Europäische Agentur für Netz– und Informationssicherheit
ErlRV	Erläuterungen zur Regierungsvorlage
EU	Europäische Union
EUR	Euro
f(f).	folgend(e)

GmbH	Gesellschaft mit beschränkter Haftung
GovCERT	Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung)
GP	Gesetzgebungsperiode
i.d.(g.)F.	in der (geltenden) Fassung
IKDOK	Innerer Kreis der Operativen Koordinierungsstruktur
IKT	Informations– und Kommunikationstechnologie
IPCR	Integrated Political Crisis Response
IT	Informationstechnologie
i.V.m.	in Verbindung mit
MilCERT	militärisches Computer Emergency Response Team (Computer–Notfallteam)
Mio.	Million(en)
NIS	Netz– und Informationssystemsicherheit
NISG	Netz– und Informationssystemsicherheitsgesetz
NISV	Netz– und Informationssystemsicherheitsverordnung
OpKoord	Operative Koordinierungsstruktur
rd.	rund
RH	Rechnungshof
Rz	Randziffer
S.	Seite
SOC	Security Operations Center (IT–Sicherheitsleitstelle)
SPOC	Single Point of Contact (zentrale Anlaufstelle)
TZ	Textzahl(en)
u.a.	unter anderem
VBÄ	Vollbeschäftigungsäquivalent(e)
vgl.	vergleiche
WFA	wirkungsorientierte Folgenabschätzung
Z	Ziffer
ZAS	Zentrales Ausweichrechenzentrum des Bundes
z.B.	zum Beispiel

Glossar

Anbieter digitaler Dienste
(§ 3 Z 12 und 13 Netz– und Informationssystemsicherheitsgesetz)

Das sind juristische Personen oder eingetragene Personengesellschaften, die einen Online–Marktplatz, einen Cloud–Computing–Dienst oder eine Online–Suchmaschine entgeltlich, im Fernabsatz, mit elektronischen Mitteln und auf individuellen Abruf anbieten, ausgenommen Klein– und Kleinstunternehmen.

Betreiber wesentlicher Dienste
(§ 3 Z 9 und 10 Netz– und Informationssystemsicherheitsgesetz)

Das sind Einrichtungen, die in einem der in § 2 Netz– und Informationssystemsicherheitsgesetz genannten Sektoren einen Dienst erbringen, der eine wesentliche Bedeutung für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations– und Kommunikationstechnologie hat und dessen Verfügbarkeit von Netz– und Informationssystemen abhängig ist.

Einrichtungen des Bundes
(§ 3 Z 19 i.V.m. § 22 Abs. 1 Netz– und Informationssystemsicherheitsgesetz)

Bundesministerien, Gerichtshöfe des öffentlichen Rechts, Rechnungshof, Volksanwaltschaft, Präsidentschaftskanzlei und Parlamentsdirektion unterliegen Verpflichtungen zu Sicherheitsvorkehrungen im Hinblick auf die Netz– und Informationssysteme, die sie für die Bereitstellung wichtiger Dienste nutzen. Die wichtigen Dienste sind nicht gesetzlich definiert.

Sicherheitsvorfall
(§ 3 Z 6 Netz– und Informationssystemsicherheitsgesetz)

Dieser Begriff bezeichnet eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder einem Ausfall der wesentlichen, digitalen bzw. wichtigen Dienste mit (tatsächlichen) erheblichen Auswirkungen führt. Als Ursache der Störung kommen alle Anlassfälle (z.B. auch Naturkatastrophen) in Betracht. Die Erheblichkeit der Auswirkungen ist nach der Zahl der betroffenen Nutzer, der Dauer der Störung, dem betroffenen Gebiet und den sonstigen Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten zu beurteilen. Die Netz– und Informationssystemsicherheitsverordnung legte dazu für die Betreiber wesentlicher Dienste je Sektor spezielle Schwellenwerte fest (z.B. wenn der wesentliche Dienst eine bestimmte Anzahl von Stunden ausfällt). Hinsichtlich der Anbieter digitaler Dienste waren die Schwellenwerte in der NIS–Durchführungsverordnung der Europäischen Kommission für alle Mitgliedstaaten harmonisiert.

WIRKUNGSBEREICH

- Bundeskanzleramt
- Bundesministerium für europäische und internationale Angelegenheiten
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung

Koordination der Cyber–Sicherheit

Prüfungsziel

Der RH überprüfte von Februar 2021 bis Mai 2021 die Koordination der Cyber–Sicherheit im Bundeskanzleramt, im Bundesministerium für Inneres, im Bundesministerium für Landesverteidigung und im Bundesministerium für europäische und internationale Angelegenheiten. Prüfungsziele waren die Darstellung und Beurteilung der Koordination der Cyber–Sicherheit in der Bundesverwaltung. Dies betraf insbesondere die Themen Rechtsgrundlagen der Cyber–Sicherheit, strategische und operative Koordination der Cyber–Sicherheit, Vorfalls– und Krisenmanagement sowie Rollen und Aufgaben der überprüften Bundesministerien. Überprüft wurde auch die Bewältigung der bislang einzigen Cyber–Sicherheitskrise Ende 2019/Anfang 2020 im Bundesministerium für europäische und internationale Angelegenheiten. Der überprüfte Zeitraum umfasste die Jahre 2018 bis Mai 2021.

Kurzfassung

Ausgangslage und rechtliche Grundlagen

Die Cyber–Sicherheit ist in allen Bereichen der elektronischen Datenverarbeitung, Datenübermittlung und Kommunikation maßgeblich. Darüber hinaus ist sie Grundlage einer sicheren Informationstechnologie in Bezug auf Funktion und Datenintegrität in allen staatlichen und privatwirtschaftlichen Sektoren. Da die Cyber–Sicherheit in all diesen Bereichen zu gewährleisten ist, kommt ihrer Koordination entscheidende Bedeutung zu. In der Bundesverwaltung sind dafür das **Bundeskanzleramt**,

das Bundesministerium für Inneres (in der Folge: **Innenministerium**), das Bundesministerium für Landesverteidigung (in der Folge: **Verteidigungsministerium**) und das Bundesministerium für europäische und internationale Angelegenheiten (in der Folge: **Außenministerium**) zuständig. (TZ 1)

Ziel der Cyber–Sicherheit ist es, ein hohes Sicherheitsniveau von Netz– und Informationssystemen zu gewährleisten. Dazu ist es notwendig, dass die Anbieter der für die Gesellschaft wichtigen technischen Infrastruktur („Betreiber wesentlicher Dienste" in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur) und der digitalen Dienste entsprechende Sicherheitsvorkehrungen zur Aufrechterhaltung ihrer Leistungen treffen. (TZ 1)

Diese Netz– und Informationssicherheit soll dazu beitragen, dass beispielsweise die Versorgung mit Energie (Elektrizität, Erdöl, Erdgas), der öffentliche Verkehr sowie das Verkehrsmanagement, das Bankwesen, die Finanzmarktinfrastrukturen, das Gesundheitswesen (Krankenhäuser), die Versorgung mit Trinkwasser und die digitale Infrastruktur (Betrieb von Internetknoten) gewährleistet werden. (TZ 1)

Eine wesentliche rechtliche Grundlage dafür ist das Netz– und Informationssystemsicherheitsgesetz (**NISG**). Es basiert auf einer entsprechenden Richtlinie der EU vom August 2016. Diese sieht vor, dass die Mitgliedstaaten die für die Netz– und Informationssystemsicherheit zuständigen nationalen Behörden und sonstigen Stellen eindeutig festlegen und den Betreibern wesentlicher Dienste in sieben Sektoren sowie den Anbietern digitaler Dienste Pflichten zu Sicherheitsvorkehrungen und zur Meldung von Sicherheitsvorfällen auferlegen. Die Umsetzung in nationales Recht hätte bis Mai 2018 erfolgen sollen. Tatsächlich brachte das Bundeskanzleramt die Regierungsvorlage für das NISG erst im November 2018 in den Nationalrat ein. Die nationale Netz– und Informationssystemsicherheitsverordnung (**NISV**) mit wesentlichen Durchführungsbestimmungen wurde im Juli 2019 erlassen, obwohl auch sie für eine vollständige Umsetzung der NIS–Richtlinie ab Mai 2018 erforderlich gewesen wäre. (TZ 2)

Das NISG bezog – im Gegensatz zur EU–Richtlinie – auch Einrichtungen des Bundes als Bereitsteller wichtiger Dienste[1] und damit als Adressaten der Verpflichtungen zu Sicherheitsvorkehrungen ein. Die wichtigen Dienste waren allerdings gesetzlich nicht definiert. Die Einrichtungen des Bundes hatten daher anhand eines unverbind-

[1] beispielsweise elektronische Aktenverwaltung, Haushalts– und Personalverwaltung, öffentliche Register

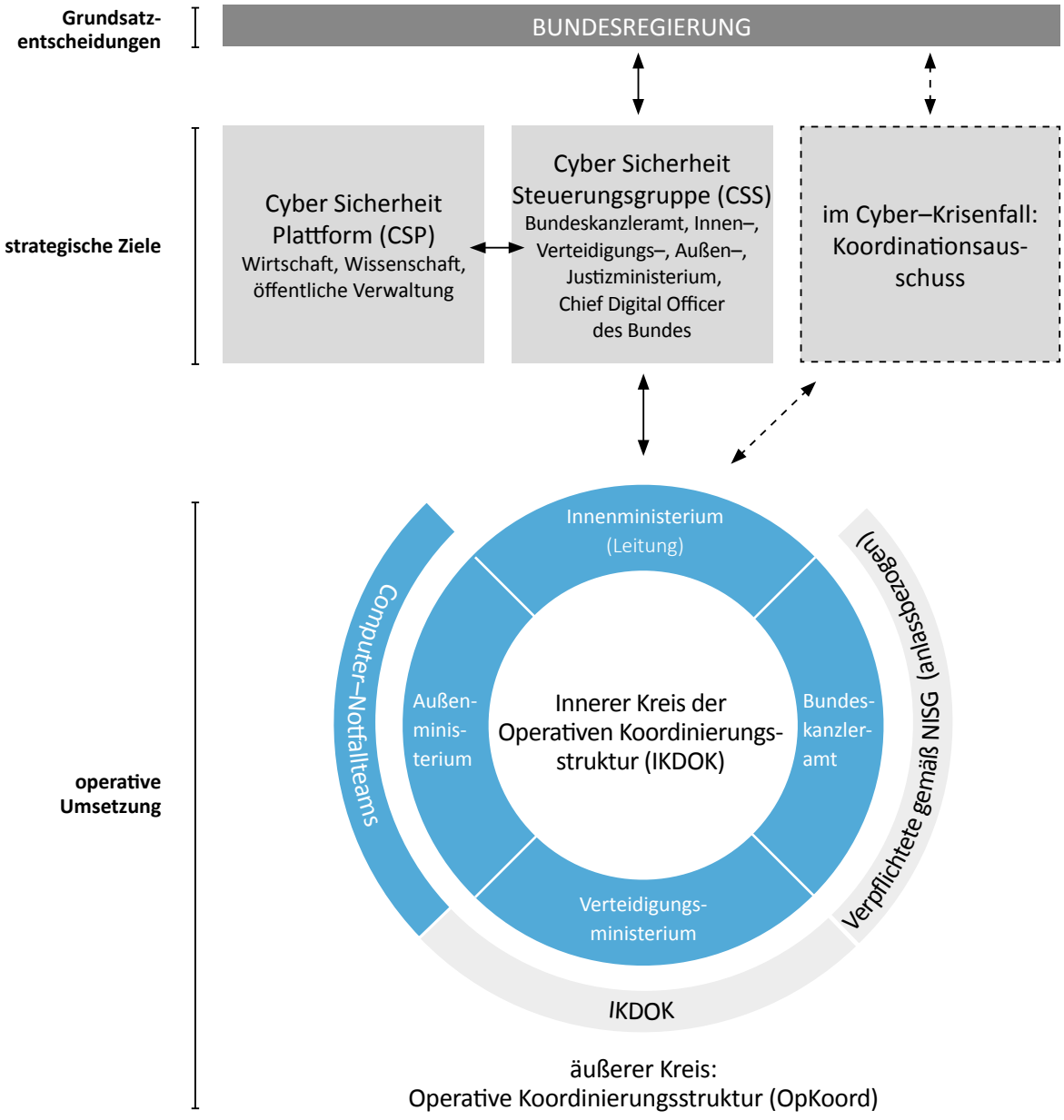
lichen Umsetzungsleitfadens des Bundeskanzleramts selbst zu beurteilen, welche ihrer Netz– und Informationssysteme sie für wichtige Dienste nutzten, und sie hatten die erforderlichen Sicherheitsvorkehrungen zu treffen. Eine Überprüfung war nicht vorgesehen. Auch lag kein zentraler Gesamtüberblick über die wichtigen IT–Dienste des Bundes vor. (TZ 2, TZ 4)

Die „Österreichische Strategie für Cyber Sicherheit“ (in der Folge: **Cyber–Sicherheitsstrategie**) aus dem Jahr 2013 sah erstmals die Einrichtung organisatorischer Strukturen für die Koordination der Cyber–Sicherheit vor. Die festgelegten Handlungsfelder und Maßnahmen waren zur Zeit der Gebarungsüberprüfung im Mai 2021 größtenteils umgesetzt. 2021 bestand jedoch Aktualisierungsbedarf aufgrund neuer Herausforderungen vor allem durch neue Technologien. Die Cyber–Sicherheitsstrategie legte bereits 2013 fest, dass der Austausch von Expertinnen und Experten zwischen den beteiligten staatlichen, privatwirtschaftlichen und wissenschaftlichen Organisationen gestärkt werden sollte. Das für diesen regelmäßigen und vertieften Austausch geplante Austauschprogramm lag acht Jahre nach Beschluss der Cyber–Sicherheitsstrategie allerdings noch nicht vor. (TZ 3, TZ 10)

Strategische und operative Cyber–Koordination

Entsprechend den rechtlichen und strategischen Vorgaben bestand folgende Struktur der Koordination der Cyber–Sicherheit in der Bundesverwaltung: (TZ 6)

Abbildung: Organisation der Cyber–Sicherheit



Quellen: BKA; BMI; Darstellung: RH

Der Innere Kreis der Operativen Koordinierungsstruktur (**IKDOK**) setzte sich unter Leitung des Innenministeriums aus den Vertreterinnen und Vertretern des Bundeskanzleramts, des Verteidigungsministeriums und des Außenministeriums zusammen. Er war als wichtigstes interministerielles Gremium der Cyber–Sicherheit für die Lagebilderstellung und –erörterung sowie im Cyber–Krisenfall zuständig. Die Operative Koordinierungsstruktur (**OpKoord**) entfaltete bisher keine eigenständige Tätigkeit, auch waren weder das für die Koordination und die zusammenfassende Behandlung in Angelegenheiten der Informationstechnologie zuständige Bundesministerium für Digitalisierung und Wirtschaftsstandort (in der Folge: **Digitalisierungsministerium**) noch die Länder eingebunden. (TZ 13, TZ 16)

Für das Vorfalls– und Krisenmanagement waren folgende Meldestrukturen vorgesehen:

Sicherheitsvorfälle[2] waren von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen der öffentlichen Verwaltung jedenfalls über das jeweils zuständige Computer–Notfallteam an den Bundesminister für Inneres zu melden. Sonstige Vorfälle und Risiken konnten freiwillig gemeldet werden. Die nach dem NISG eingehenden Meldungen wurden im Innenministerium zwar aktenmäßig erfasst, in einer Meldungsübersicht eingetragen und an das Bundeskanzleramt sowie das Verteidigungsministerium weitergeleitet. Allerdings war rund zweieinhalb Jahre nach dem Inkrafttreten des NISG noch keine informations– und kommunikationstechnische Lösung zur Umsetzung des im NISG vorgesehenen Meldeanalysesystems in Betrieb. Im Zeitraum Jänner 2019 bis Dezember 2020 wurden im Innenministerium insgesamt 107 Meldungen zu Risiken, Vorfällen und Sicherheitsvorfällen gemäß NISG erfasst, darunter 42 Meldungen zu Sicherheitsvorfällen. (TZ 21, TZ 22)

Das vom Innenministerium bereits für 2020 geplante Frühwarnsystem zur Erkennung von Risiken, Vorfällen und Sicherheitsvorfällen von Netz– und Informationssystemen fehlte. Ein derartiges Sensornetzwerk war im Jahr 2021 erst in der Konzeptionsphase. (TZ 20, TZ 26)

Cyber–Angriff auf Systeme des Außenministeriums

Das System der Cyber–Sicherheit wurde Ende 2019/Anfang 2020 einer Bewährungsprobe unterzogen: Im Dezember 2019 erfolgte ein verdeckter Cyber–Angriff auf die Systeme des Außenministeriums, der in weiterer Folge erstmals in Österreich zur Feststellung einer Cyber–Krise und damit auch zur Aktivierung der dafür vorgesehenen Strukturen führte. (TZ 24)

[2] Ein „Sicherheitsvorfall“ ist gemäß § 3 Z 6 NISG definiert als eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat.

Rückblickend ist festzuhalten, dass diese Cyber–Krise innerhalb von zwei Monaten grundsätzlich erfolgreich bewältigt werden konnte. Mit der Feststellung der Cyber–Krise am 4. Jänner 2020 wurden die Krisenmechanismen und –strukturen aktiviert und unter der Federführung des Innenministeriums übernahm eine Einsatzstruktur – bestehend aus den gebündelten Cyber–Sicherheitskräften der verantwortlichen Bundesministerien und einem externen Unternehmen – die operativen Aufgaben zur Bewältigung der Krise. Damit konnten die grundsätzlichen personellen und zeitlichen Anforderungen für die Dauer der Krisenbewältigung abgedeckt werden. (TZ 25, TZ 27)

Aus Sicht des RH sind übergeordnete Krisen–, Kontinuitäts– und Einsatzpläne für ein funktionierendes Cyber–Krisenmanagement wesentlich. Diese sollten nicht nur die grundlegende Einsatzstruktur behandeln, sondern auch aufbauend auf den Notfall– und Kontinuitätsplänen der Bundesministerien eine koordinierte und effiziente Krisenbewältigung sicherstellen. Solche Krisen–, Kontinuitäts– und Einsatzpläne lagen jedoch nicht vor, obwohl die Cyber Sicherheit Steuerungsgruppe die Ausarbeitung solcher Pläne bereits 2014 und 2019 beschlossen hatte. Das Bundeskanzleramt und das Innenministerium wären dafür zuständig gewesen. (TZ 9, TZ 26)

Es fehlte auch eine Cyber–Krisen–Infrastruktur: So mussten Räumlichkeiten und sonstige Ausstattung wie Hardware und Software erst unmittelbar in der Cyber–Krise organisiert und beschafft werden, um eine Einsatzbereitschaft herzustellen. (TZ 14, TZ 24, TZ 26)

Ein ständig verfügbares Einsatzteam (Rapid Response Team) stand nicht zur Verfügung. Es gab auch kein Cyber Security Operations Center im Sinne einer staatlichen Cyber–Sicherheitsleitstelle mit Einsatzzentrale und einsatzbereitem Personal. (TZ 25, TZ 26)

In Summe wendeten die zur Bewältigung der Cyber–Krise tätigen Bundesministerien rd. 10.732 Arbeitsstunden auf, das entsprach rd. 67 Personenmonaten. Das Außenministerium musste aufgrund der Dringlichkeit und Unvorhersehbarkeit für wichtige fehlende Software und Expertise eine Notfallbeschaffung von 1,69 Mio. EUR durchführen. Eine zusammenfassende Betrachtung der für die Bewältigung der Cyber–Krise insgesamt angefallenen Kosten lag nicht vor. Damit fehlte eine Grundlage für die Weiterentwicklung des Cyber–Krisenmanagements. (TZ 25)

Personalressourcen

Für die Umsetzung des NISG und damit für die Sicherstellung der Cyber–Sicherheit waren – laut wirkungsorientierter Folgenabschätzung – im Bundeskanzleramt sieben Vollbeschäftigungsäquivalente (**VBÄ**) vorgesehen, im Innenministerium 36. In den Jahren 2020 und 2021 waren jedoch nur 1,7 VBÄ im Bundeskanzleramt und 16 VBÄ im Innenministerium tatsächlich besetzt. Das Innenministerium verwies dazu auf die Schwierigkeit, im Bereich der Cyber–Sicherheit spezialisiertes Personal zu rekrutieren. Die Frage der Cyber–Sicherheit im Rahmen der Erfüllung des NISG betraf nicht nur das jeweilige Bundesministerium, sondern war eine zentrale koordinative Aufgabe für die gesamte Bundesverwaltung und die gesamte Infrastruktur der Republik Österreich. Demzufolge wären die im NISG festgelegten Aufgaben zu erfüllen und dabei auch das dafür notwendige Personal sicherzustellen. (TZ 27)

Einbeziehung der Länder

Die Länder hatten keine Regelungen auf landesgesetzlicher Ebene getroffen, um Pflichten zu Sicherheitsvorkehrungen bei wichtigen IT–Diensten und zur Meldung von Sicherheitsvorfällen entsprechend den öffentlichen Einrichtungen des Bundes zu übernehmen. Auch waren die Länder weder in die strategische noch in die operative Koordination der Cyber–Sicherheit regelmäßig eingebunden. (TZ 13, TZ 29)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

ZENTRALE EMPFEHLUNGEN

- Vom Bundeskanzleramt und vom Bundesministerium für Inneres wären konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement auszuarbeiten. (TZ 26)

- Dem Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) und der Operativen Koordinierungsstruktur (OpKoord) wäre vom Bundesministerium für Inneres ein Cyber–Lagezentrum mit der für die Zwecke der Erfüllung ihrer Aufgaben erforderlichen Infrastruktur unter Beachtung von Kosten–Nutzen–Aspekten einzurichten und zur Verfügung zu stellen. Dieses sollte aufgrund der dem Bundesminister für Inneres zukommenden Leitungsaufgaben im IKDOK (und OpKoord) beim Bundesministerium für Inneres eingerichtet werden. (TZ 14)

- Vom Bundesministerium für Inneres wäre das Projekt zur Implementierung des Frühwarnsystems (Sensornetzwerk) verstärkt zu betreiben und umzusetzen. Im Sinne des gesamtstaatlichen und sektorübergreifenden Ziels, Cyber–Angriffe zu erkennen bzw. deren Auswirkungen so gering wie möglich zu halten sowie Muster und Vorgehensweisen bei Cyber–Angriffen zu analysieren, sollten möglichst viele Organisationen an diesem Frühwarnsystem (Sensornetzwerk) teilnehmen, um dadurch eine großflächige Abdeckung der Risiken zu erreichen. (TZ 20)

- Vom Bundeskanzleramt, vom Bundesministerium für Inneres, vom Bundesministerium für Landesverteidigung und vom Bundesministerium für europäische und internationale Angelegenheiten wäre ein permanent verfügbares Cyber–Einsatzteam (Rapid Response Team) zu schaffen; dies in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam. (TZ 25)

- Die Aufgaben der Operativen Koordinierungsstruktur betreffend Cyber–Sicherheit wären vom Bundeskanzleramt, vom Bundesministerium für Inneres, vom Bundesministerium für Landesverteidigung und vom Bundesministerium für europäische und internationale Angelegenheiten zu evaluieren und das Bundesministerium für Digitalisierung und Wirtschaftsstandort sowie die Länder wären auf geeignete Weise zu integrieren. Hierbei wäre auch festzulegen, ob die Operative Koordinierungsstruktur regelmäßig oder nur im Bedarfsfall einzuberufen wäre. (TZ 13)

Zahlen und Fakten zur Prüfung

Koordination der Cyber–Sicherheit	
wichtige Rechtsgrundlagen und Vorgaben	Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen in der Union, ABl. L 2016/194, 1 Netz– und Informationssystemsicherheitsgesetz (NISG), BGBl. I 111/2018 i.d.g.F. Netz– und Informationssystemsicherheitsverordnung (NISV), BGBl. II 215/2019 i.d.g.F. Österreichische Strategie für Cyber Sicherheit 2013, Ministerratsbeschluss vom 20. März 2013
wichtige Organisationseinheiten für Cyber–Sicherheit	Cyber Sicherheit Steuerungsgruppe (Steuerungsgruppe–CSS) Koordinationsausschuss im Cyberkrisenmanagement (CKM–KA) Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK) Operative Koordinierungsstruktur (OpKoord) Computer–Notfallteams (CERTs)
Abstufungen der Cyber–Sicherheits–Gefährdungen (Definitionen laut NISG)	
Risiko	alle Umstände oder Ereignisse, die **potenziell** nachteilige Auswirkungen auf die Sicherheit von Netz– und Informationssystemen haben
Vorfall	alle Ereignisse, die **tatsächlich** nachteilige Auswirkungen auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen haben und kein Sicherheitsvorfall sind
Sicherheitsvorfall	eine **Störung** der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen führt
Krise	ein oder mehrere Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können
Meldungen erfasst[1] von der operativen NIS–Behörde im Innenministerium	
Meldung von Cyber–Sicherheits–Gefährdungen[2] von Jänner 2019 bis Dezember 2020	107
davon	
Sicherheitsvorfälle nach NISG	*42*
Cyber–Sicherheitskrisen	*1*

[1] Bis 2020 waren noch nicht alle Betreiber ermittelt.
[2] freiwillige Meldungen und Meldungen nach NISG

Quellen: BKA; BMI; BMLV; BMEIA

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von Februar 2021 bis Mai 2021 die Koordination der Cyber–Sicherheit[3] im **Bundeskanzleramt**, im Bundesministerium für Inneres (in der Folge: **Innenministerium**), im Bundesministerium für Landesverteidigung (in der Folge: **Verteidigungsministerium**) und im Bundesministerium für europäische und internationale Angelegenheiten (in der Folge: **Außenministerium**). Die genannten Bundesministerien bildeten den Inneren Kreis der Operativen Koordinierungsstruktur (**IKDOK**), der das Zentrum der Koordination der Cyber–Sicherheit des Bundes darstellte.

Die Cyber–Sicherheit zeichnet sich dadurch aus, dass sie in allen Bereichen der elektronischen Datenverarbeitung, Datenübermittlung und Kommunikation maßgeblich ist. Darüber hinaus ist sie Grundlage einer sicheren Informationstechnologie in Bezug auf Funktion und Datenintegrität in allen staatlichen und privatwirtschaftlichen Sektoren. Da die Cyber–Sicherheit in all diesen Bereichen zu gewährleisten ist, kommt ihrer Koordination entscheidende Bedeutung zu.

Ziel der Cyber–Sicherheit ist es, ein hohes Sicherheitsniveau von Netz– und Informationssystemen zu gewährleisten. Dazu ist es notwendig, dass die Anbieter der für die Gesellschaft wichtigen technischen Infrastruktur („Betreiber wesentlicher Dienste“ in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur) und der digitalen Dienste entsprechende Sicherheitsvorkehrungen zur Aufrechterhaltung ihrer Leistungen treffen.

Diese Netz– und Informationssicherheit soll dazu beitragen, dass beispielsweise die Versorgung mit Energie (Elektrizität, Erdöl, Erdgas), der öffentliche Verkehr sowie das Verkehrsmanagement, das Bankwesen, das Gesundheitswesen (Krankenhäuser), die Versorgung mit Trinkwasser und die Telekommunikation gewährleistet werden.

Die gegenständliche Gebarungsüberprüfung befasste sich daher mit der Koordination jener Maßnahmen der Bundesverwaltung, die für eine verlässliche und funktionierende digitale Infrastruktur, auch im Hinblick auf die Daseinsvorsorge für die Bevölkerung und die dafür notwendigen essenziellen Dienstleistungen durch die öffentliche Verwaltung, von Bedeutung sind.

[3] Der vorliegende Bericht verwendet bei Begriffen mit dem Präfix „Cyber–“ grundsätzlich die Schreibweise mit Bindestrich (z.B. „Cyber–Sicherheit“). Ausnahmen bilden Eigennamen – etwa von Gremien oder Strategien – oder wörtliche Zitate.

Ziele dieser Gebarungsüberprüfung waren die Darstellung und Beurteilung der Koordination der Cyber–Sicherheit in der Bundesverwaltung. Dies betraf insbesondere die Themen

- Rechtsgrundlagen der Cyber–Sicherheit,
- strategische Koordination der Cyber–Sicherheit,
- operative Koordination der Cyber–Sicherheit,
- operative Cyber–Sicherheit,
- Vorfalls– und Krisenmanagement sowie
- weitere Entwicklung der Cyber–Sicherheit.

Darüber hinaus überprüfte der RH in diesen Bundesministerien die Koordination der Cyber–Krise im Außenministerium, die von Jänner bis März 2020 andauerte.

Nicht Gegenstand der Gebarungsüberprüfung waren die internen Cyber–Sicherheitsvorkehrungen in den überprüften Bundesministerien.

Der überprüfte Zeitraum umfasste insbesondere die Jahre 2018 bis Mai 2021. Soweit erforderlich, nahm der RH auch auf frühere Entwicklungen Bezug.

(2) Zu dem im November 2021 übermittelten Prüfungsergebnis nahmen das Bundeskanzleramt und das Verteidigungsministerium im Jänner 2022 sowie das Außenministerium und das Innenministerium im Februar 2022 Stellung.

Das Außenministerium hielt in seiner Stellungnahme fest, dass die Schlussempfehlungen 3, 4, 30 und 33 die Zuständigkeit des Bundeskanzleramts und die Schlussempfehlungen 12, 25 und 27 die Zuständigkeit des Innenministeriums beträfen. Das Außenministerium werde bei der Umsetzung dieser Empfehlungen unterstützend zur Verfügung stehen.

Der RH erstattete seine Gegenäußerungen an das Bundeskanzleramt, das Innenministerium und das Außenministerium im April 2022. Gegenüber dem Verteidigungsministerium verzichtete der RH auf eine Gegenäußerung.

Rechtsgrundlagen zur Netz– und Informationssystemsicherheit

2.1 (1) 2013 stellte die Europäische Union (**EU**) ihre erste Cybersicherheitsstrategie[4] vor. Damit verbunden war ein Vorschlag der Europäischen Kommission für eine Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen (**NIS**) in der Union. Die darauf basierende NIS–Richtlinie[5] trat im August 2016 in Kraft. Diese sah insbesondere vor, dass die Mitgliedstaaten die für die Netz– und Informationssystemsicherheit zuständigen nationalen Behörden und sonstigen Stellen eindeutig festlegen. Weiters haben sie den Betreibern wesentlicher Dienste in sieben Sektoren (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur) und den Anbietern digitaler Dienste Pflichten zu Sicherheitsvorkehrungen und zur Meldung von Sicherheitsvorfällen[6] aufzuerlegen.

(2) Die Vorarbeiten zur Umsetzung der NIS–Richtlinie in nationales Recht oblagen dem Bundeskanzleramt als strategischem Koordinator der Netz– und Informationssicherheit. Die entsprechende Regierungsvorlage zum Netz– und Informationssystemsicherheitsgesetz (**NISG**) wurde im November 2018 (Beschluss Dezember 2018), rund sechs Monate nach dem in der NIS–Richtlinie vorgesehenen Umsetzungstermin (Mai 2018), im Nationalrat eingebracht. Die nationale Netz– und Informationssystemsicherheitsverordnung (**NISV**) mit wesentlichen Durchführungsbestimmungen (z.B. Schwellenwerte für die Bestimmung wesentlicher Dienste) wurde im Juli 2019 erlassen, obwohl auch sie für eine vollständige Umsetzung der NIS–Richtlinie ab Mai 2018 erforderlich gewesen wäre. Die verspätete Umsetzung hatte auch eine zeitverzögerte Ermittlung der Betreiber wesentlicher Dienste zur Folge (TZ 4). Das Bundeskanzleramt begründete die verspätete Umsetzung damit, dass im Zuge der Ausarbeitung des Gesetzesentwurfs eine politische Neubewertung hinsichtlich der Einbeziehung des Verteidigungsministeriums in das NISG stattfand und datenschutzrechtliche Aspekte nachgeschärft wurden.

[4] JOIN(2013) 1 final

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

[6] Diese Meldepflichten bei Einschränkung oder Ausfall der Verfügbarkeit von Netz– und Informationssystemen wurden im Netz– und Informationssystemsicherheitsgesetz (NISG) umgesetzt. Bezüglich einer allenfalls auch vorliegenden Verletzung des Schutzes personenbezogener Daten bestand eine Meldepflicht nach der Datenschutz–Grundverordnung (DSGVO, ABl. L 2016/119, 1) (siehe Anhang B „Berührungspunkte mit anderen Rechtsgrundlagen“).

Weitere mögliche Verordnungen – zur Aufteilung der Pflichten der datenschutzrechtlich Verantwortlichen für ein NIS–Meldeanalysesystem[7] sowie zur Festlegung einer Abgeltung für die Nutzung von IKT–Lösungen zur Erkennung von Sicherheitsvorfällen[8] – wurden noch nicht erlassen, insbesondere da derartige IKT–Lösungen bis Mai 2021 noch nicht in Betrieb waren.

(3) Bereits vor 2016 wurden einige unmittelbar anwendbare EU–Verordnungen sowie in nationales Recht umzusetzende EU–Richtlinien für spezielle Sektoren erlassen, die auch Vorgaben zur Cyber–Sicherheit enthalten: Ergänzung Telekom–Rahmenrichtlinie 2009, Verordnung Vertrauensdiensteanbieter 2014, Zweite Finanzmarktrichtlinie 2014, Zweite Zahlungsdiensterichtlinie 2015. Diese sektorspezifischen Rechtsgrundlagen einschließlich der Umsetzungen in nationales Recht gehen als speziellere Rechtsvorschriften den Rechtsgrundlagen zur Netz– und Informationssystemsicherheit (NIS) vor.

(4) Die folgende Tabelle gibt einen Überblick über die wesentlichen Inhalte der einschlägigen europäischen und österreichischen Rechtsgrundlagen im Bereich der Netz– und Informationssystemsicherheit bzw. Cyber–Sicherheit (aus Gründen der Übersichtlichkeit enthält diese Tabelle nur die Kurzbezeichnung der Rechtsgrundlagen; die vollständige Bezeichnung samt Fundstelle ist dem Anhang A „Verzeichnis der Rechtsgrundlagen“ zu entnehmen):

Tabelle 1: Wesentliche Rechtsgrundlagen im Bereich der Netz– und Informationssystemsicherheit bzw. Cyber–Sicherheit

Rechtsgrundlage	Inkrafttreten	wesentliche Inhalte
EU–Vorgaben zur Netz– und Informationssystemsicherheit (NIS)		
NIS–Richtlinie	August 2016 (Umsetzung bis 9. Mai 2018)	– nationale Cyber–Sicherheits–Strategien (TZ 3) – europäische Zusammenarbeit in der EU–Kooperationsgruppe und dem Netzwerk der Computer–Notfallteams (TZ 17) – Benennung der zuständigen nationalen Behörden und Computer–Notfallteams (TZ 17, TZ 18) – Sicherheitsanforderungen und Meldepflichten bei erheblichen Sicherheitsvorfällen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste in sieben Sektoren[1] (TZ 4)
NIS–Durchführungsverordnung	unmittelbar anwendbar ab Mai 2018	für Anbieter digitaler Dienste (TZ 4): Präzisierung (verstärkte Harmonisierung) der – Sicherheitsanforderungen und – erheblichen Auswirkungen von Sicherheitsvorfällen

[7] durch den Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres als Betreiber und der Bundesministerin für Landesverteidigung

[8] durch den Bundesminister für Inneres

Rechtsgrundlage	Inkrafttreten	wesentliche Inhalte
Umsetzung der NIS–Richtlinie in Österreich		
NISG	Dezember 2018	– Umsetzung der NIS–Richtlinie in innerstaatliches Recht – Festlegung der Koordinierungsstrukturen (TZ 6) – Einbeziehung der Einrichtungen des Bundes als Bereitsteller wichtiger Dienste (TZ 4) – qualifizierte Stellen zur Überprüfung der getroffenen Sicherheitsvorkehrungen (TZ 4) – Rahmenbedingungen für IKT–Lösungen
NISV	Juli 2019	für Betreiber wesentlicher Dienste (TZ 4): Präzisierung der – Wesentlichkeit der Dienste – erheblichen Auswirkungen von Sicherheitsvorfällen – Sicherheitsanforderungen – Ausnahmen von den Verpflichtungen gemäß NISG aufgrund sektorspezifischer Rechtsakte
Verordnung über qualifizierte Stellen	Juli 2019	– Erfordernisse an qualifizierte Stellen – Verfahren zur Feststellung durch den Bundesminister für Inneres
sektorspezifische[2] Rechtsgrundlagen		
§§ 85, 86 Zahlungsdienstegesetz 2018	Juni 2018	für Zahlungsdienstleister (Sektor Bankwesen): – Sicherheitsanforderungen und Meldepflichten – Befugnisse der Finanzmarktaufsichtsbehörde
§ 11 Börsegesetz 2018	Jänner 2018	Sicherheitsanforderungen an algorithmische Handelssysteme (Sektor Finanzmarktinfrastrukturen)
§ 44 Telekommunikationsgesetz 2021	November 2021	für Betreiber öffentlicher Kommunikationsnetze und Anbieter öffentlicher Kommunikationsdienste (Telekommunikation[3]): – Sicherheitsanforderungen und Meldepflichten – Befugnisse der Telekom–Regulierungsbehörde
Art. 19 EU–eIDAS–Verordnung[4]	unmittelbar anwendbar ab Juli 2016	für Vertrauensdiensteanbieter[3] (elektronische Signaturen, Zertifikate): – Sicherheitsanforderungen und Meldepflichten – Befugnisse der Aufsichtsstelle (Telekom–Regulierungsbehörde)

NISG = Netz– und Informationssystemsicherheitsgesetz Quellen: bezughabende Rechtsquellen
NISV = Netz– und Informationssystemsicherheitsverordnung

[1] Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur
[2] Die nationalen, sektorspezifischen Rechtsakte setzen folgende EU–Richtlinien um: Zweite Zahlungsdienstericht-linie und Zweite Finanzmarktrichtlinie, EECC–Richtlinie (ersetzt ab 21. Dezember 2020 die Telekom–Rahmenricht-linie; von November 2011 bis Oktober 2021 galt § 16a Telekommunikationsgesetz 2003).
[3] Telekommunikation und Vertrauensdiensteanbieter gehören nicht zu den sieben Sektoren der NIS–Richtlinie.
[4] Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen

Die NIS–Richtlinie erfordert die Umsetzung von Sicherheitsvorkehrungen und Meldepflichten für die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste; das heißt, sie erfasste nicht die öffentliche Verwaltung. Das österreichische NISG verpflichtet darüber hinaus auch Einrichtungen des Bundes als Bereitsteller wichtiger Dienste und sieht dazu Pflichten zu Sicherheitsvorkehrungen und zur Meldung von Sicherheitsvorfällen vor. Die Länder hatten von der Möglichkeit nicht Gebrauch gemacht, diese Pflichten für ihre Einrichtungen für anwendbar zu erklären.

2.2 Der RH beurteilte das NISG als wichtige rechtliche Verankerung der Koordinierungsstrukturen und der dafür vorgesehenen Gremien im Bereich der Cyber–Sicherheit (zum Überblick über diese Gremien siehe TZ 6).

Weiters sah er es als positiv an, dass gemäß NISG – über die Vorgaben der NIS–Richtlinie hinausgehend – auch den Einrichtungen des Bundes Pflichten zu Sicherheitsvorkehrungen und zur Meldung von Sicherheitsvorfällen hinsichtlich der von ihnen betriebenen wichtigen Dienste oblagen. Zu den Ländern verwies der RH auf seine Feststellungen in TZ 29.

Der RH hielt jedoch kritisch fest, dass das Bundeskanzleramt den Ministerratsvortrag für die Regierungsvorlage zur Umsetzung der NIS–Richtlinie erst sechs Monate nach dem in der Richtlinie vorgegebenen Umsetzungstermin vorlegte.

Österreichische Strategie für Cyber Sicherheit

3.1 (1) Kurz nach der Veröffentlichung der ersten EU–Cybersicherheitsstrategie im Jahr 2013 beschloss die Bundesregierung im März 2013 erstmals die „Österreichische Strategie für Cyber Sicherheit“ (in der Folge: **Cyber–Sicherheitsstrategie**) unter Federführung des Bundeskanzleramts. 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.

Die Cyber–Sicherheitsstrategie definierte sieben Handlungsfelder[9] und sah dafür jeweils Ziele und Maßnahmen vor. In Zusammenhang mit der Koordination der Cyber–Sicherheit waren insbesondere die Handlungsfelder zur Einrichtung organisatorischer Strukturen für eine übergeordnete Koordination und zur Schaffung eines rechtlichen Rahmens relevant:

- So waren die operativen Gremien „Operative Koordinierungsstruktur“ (**OpKoord**) und deren „Innerer Kreis der Operativen Koordinierung“ (**IKDOK**) erstmals in der Cyber–Sicherheitsstrategie festgehalten (TZ 13 ff.).
- Zudem sollten folgende Gremien Teil der organisatorischen Struktur sein:
  - die mit Ministerratsbeschluss vom Mai 2012 eingerichtete Cyber Sicherheit Steuerungsgruppe (in der Folge: **Steuerungsgruppe–CSS**) (TZ 9),

[9] 1. Strukturen und Prozesse, 2. Governance, 3. Kooperation Staat, Wirtschaft und Gesellschaft, 4. Schutz kritischer Infrastrukturen, 5. Sensibilisierung und Ausbildung, 6. Forschung und Entwicklung, 7. internationale Zusammenarbeit

- eine als Public Private Partnership zu gründende Cyber Sicherheit Plattform (**CSP**) zur Zusammenarbeit und zum Austausch zwischen Verwaltung, Wirtschaft und Wissenschaft (TZ 10) und
- die bereits bestehenden, aber ausbaufähigen Computer Emergency Response Teams (**CERTs**) (TZ 18 ff.).

Weitere wesentliche Maßnahmen waren die Einrichtung eines Cyber–Krisenmanagements (TZ 11), die Einführung von Pflichten zu Sicherheitsvorkehrungen und zur Meldung schwerer Cyber–Vorfälle (TZ 4) und die Durchführung außenpolitischer Maßnahmen.[10]

Diese 2013 festgelegten Handlungsfelder und Maßnahmen waren zur Zeit der Gebarungsüberprüfung im Mai 2021 großteils umgesetzt. Konkretisierungsbedarf bestand beim Cyber–Krisenmanagement, das nur in Grundzügen beschrieben war. Aktualisierungsbedarf ergab sich bei der Bewertung der Risiken, denn die der Cyber–Sicherheitsstrategie beiliegende Risikomatrix stammte bereits aus 2011. Weiters erforderten die Veränderungen von 2013 bis 2021 durch neue Technologien, wie der Cloud–Technologie, und die faktisch stark ansteigenden Cyber–Angriffe auch neue Maßnahmen.

(2) Die im August 2016 in Kraft getretene NIS–Richtlinie verpflichtete die EU–Mitgliedstaaten, eine nationale Strategie für die Gewährleistung der Netz– und Informationssystemsicherheit festzulegen, die mit einer Cyber–Sicherheitsstrategie gleichzusetzen war. Dazu nannte die NIS–Richtlinie einige Mindestinhalte der nationalen Strategien, etwa die Aufgaben und Zuständigkeiten der staatlichen Stellen oder Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung. Diese Mindestinhalte waren durch die österreichische Cyber–Sicherheitsstrategie aus 2013 im Wesentlichen bereits erfasst. Aufgrund der zeitlichen Abfolge nahm die Cyber–Sicherheitsstrategie 2013 jedoch keinen direkten Bezug auf die 2016 angenommene NIS–Richtlinie und das dazu 2018 erlassene NISG samt den darin enthaltenen konkreten Verpflichtungen. Ebenso war das Verhältnis zur 2016 angenommenen Datenschutz–Grundverordnung nicht definiert.

(3) Die Steuerungsgruppe–CSS (TZ 9) war gemäß der Cyber–Sicherheitsstrategie für die Überprüfung der Umsetzung der Strategie sowie ihres Aktualisierungsbedarfs verantwortlich. Die Steuerungsgruppe–CSS empfahl bereits im Oktober 2017 aufgrund der geänderten Rahmenbedingungen (z.B. durch Inkrafttreten der NIS–Richtlinie), dass eine aktualisierte Fassung der Cyber–Sicherheitsstrategie auszuarbeiten und diese als Maßnahme in das Regierungsprogramm aufzunehmen wäre. In der Folge sahen die Regierungsprogramme 2017–2022 bzw. 2020–2024 die Aktua-

[10] Weitere, nicht in direktem Zusammenhang mit der Koordination der Cyber–Sicherheit stehende Maßnahmen betrafen die Forschung und Entwicklung, die Kommunikation an die Öffentlichkeit, Sensibilisierungsinitiativen sowie die Aus– und Weiterbildung.

lisierung der Cyber–Sicherheitsstrategie vor. Im Jänner 2018 beschloss die Steuerungsgruppe–CSS, bis Mai 2018 einen entsprechenden Entwurf zu erstellen. Nach Auskunft des Bundeskanzleramts[11] war ein Fachentwurf zu einer aktualisierten Cyber–Sicherheitsstrategie ausgearbeitet und befand sich in Abstimmung mit den anderen Bundesministerien. Zur Wirksamkeit der neuen Strategie bedarf es abschließend einer Beschlussfassung der Bundesregierung im Ministerrat.

(4) Auf Ebene der EU lag seit Dezember 2020 eine neue Cyber–Sicherheitsstrategie mit neuen Zielen und Aktionsbereichen vor, zu der der Rat im März 2021 Schlussfolgerungen annahm.[12] In Zusammenhang mit dem damit verbundenen Vorschlag der Europäischen Kommission für eine Weiterentwicklung der NIS–Richtlinie[13] von Dezember 2020 sowie der Stellungnahme des Rates dazu von Dezember 2021[14] (TZ 30) wird auch zukünftig weiterer Anpassungsbedarf der österreichischen Cyber–Sicherheitsstrategie bestehen. Der Vorschlag in der Fassung von Dezember 2021 sieht z.B. vor:

- eine verpflichtende Evaluierung der nationalen Cyber–Sicherheitsstrategien im Abstand von fünf Jahren auf Basis von messbaren Zielen und Leistungskennzahlen,
- eine (aktuelle) Risikobewertung oder
- neue verpflichtende Konzepte, wie die Berücksichtigung der Cyber–Sicherheit von IKT–Produkten in der Lieferkette oder bei öffentlichen Beschaffungen.

3.2 Der RH kritisierte die ausständige Aktualisierung der österreichischen Cyber–Sicherheitsstrategie und verwies in diesem Zusammenhang auch auf seinen Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 5) sowie auf seinen Bericht „Prävention und Bekämpfung von Cyberkriminalität“ (Reihe Bund 2021/23, TZ 7).

Er bewertete die Aktualisierung der österreichischen Cyber–Sicherheitsstrategie aus 2013 als vordringliche Aufgabe, weil besonders im Bereich der Cyber–Sicherheit neue Herausforderungen und Bedrohungen auftreten, die neuer Zielsetzungen und aktueller Maßnahmen bedürfen. Die für die Überprüfung der Umsetzung der Strategie verantwortliche Steuerungsgruppe–CSS hatte dies bereits 2017 erkannt.

[11] Dem Bundeskanzleramt fiel nach dem Bundesministeriengesetz (BGBl. 76/1986 i.d.g.F.) die Zuständigkeit für strategische Angelegenheiten der Netz– und Informationssicherheit zu. Nach dem NISG war der Bundeskanzler für die Koordination der Strategie zuständig.

[12] z.B. Reform der NIS–Richtlinie, EU–weite gemeinsame Cyberstelle zur verstärkten Zusammenarbeit unter Einbeziehung von Cyber–Diplomatie und Cyber–Defence, Netz von Sicherheitseinsatzzentren

[13] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, SEC(2020) 430 final

[14] Allgemeine Ausrichtung des Rates der Europäischen Union, Pressemitteilung vom 3. Dezember 2021

Der RH empfahl daher dem Bundeskanzleramt als Koordinator der Strategie, die Aktualisierung der Cyber–Sicherheitsstrategie aus 2013 ehestmöglich voranzutreiben, insbesondere die politische Abstimmung des Fachentwurfs abzuschließen und die Beschlussfassung durch die Bundesregierung vorzubereiten. Da einerseits aufgrund der sich rasch ändernden faktischen Gegebenheiten und andererseits aufgrund europäischer Vorgaben auch in naher Zukunft Änderungsbedarf zu erwarten ist, wäre es zweckmäßig, darin auch flexible Instrumente und vereinfachte Adaptierungen vorzusehen.

3.3 Das Bundeskanzleramt teilte in seiner Stellungnahme mit, dass die österreichische Bundesregierung im Dezember 2021 die „Österreichische Strategie für Cybersicherheit 2021“ im Ministerrat beschlossen und veröffentlicht habe.

Verpflichtete gemäß NISG

4.1 (1) Das NISG verpflichtet Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und – über den Anwendungsbereich der NIS–Richtlinie hinausgehend – auch Einrichtungen des Bundes zu technischen und organisatorischen Sicherheitsvorkehrungen und zur Meldung von Sicherheitsvorfällen hinsichtlich der von ihnen betriebenen wesentlichen digitalen bzw. wichtigen Dienste. Die eingegangenen Pflichtmeldungen (und auch die freiwilligen Meldungen) sind Grundlage des vom Bundesminister für Inneres regelmäßig zu erstellenden IKDOK–Lagebildes.

(2) Unterschiede zwischen den Verpflichteten

Der bedeutendste – bereits von der NIS–Richtlinie vorgegebene – Unterschied zwischen Betreibern wesentlicher Dienste[15] und Anbietern digitaler Dienste[16] bestand darin, dass nur die Betreiber wesentlicher Dienste von den nationalen Behörden zu ermitteln (Bundeskanzleramt) und regelmäßig zu überprüfen (Innenministerium) waren. Demgegenüber hatten die Anbieter digitaler Dienste selbst zu beurteilen, ob sie den Pflichten des NISG unterlagen. Eine behördliche Feststellung

[15] Betreiber wesentlicher Dienste sind private oder öffentliche Einrichtungen mit einer Niederlassung in Österreich, die einen Dienst in einem der gesetzlich festgelegten Sektoren erbringen. Der erbrachte Dienst muss eine wesentliche Bedeutung für die Aufrechterhaltung der Versorgung der Gesellschaft (in den Sektoren Energie (Elektrizität, Erdöl, Erdgas), Verkehr sowie das Verkehrsmanagement, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen (Krankenhäuser), Trinkwasserversorgung und digitale Infrastruktur (Betrieb von Internetknoten)) haben und von der Verfügbarkeit von Netz– und Informationssystemen abhängig sein.

[16] Anbieter digitaler Dienste sind juristische Personen oder eingetragene Personengesellschaften, die als Unternehmer einen digitalen Dienst in Österreich anbieten und entweder eine Hauptniederlassung in Österreich haben oder einen in Österreich niedergelassenen Vertreter namhaft gemacht haben. Erfasste Dienste sind Online–Marktplätze (Online–Kaufverträge, Online–Dienstleistungsverträge), Online–Suchmaschinen (Links zu anderen Websites aufgrund von Suchanfragen) und Cloud–Computing–Dienste (Pool von Rechenressourcen). Diese müssen entgeltlich, im Fernabsatz, mit elektronischen Mitteln und auf individuellen Abruf angeboten werden.

war nicht vorgesehen und ohne konkreten Anlassfall einer offenkundigen Pflichtverletzung auch nicht zulässig. Darüber hinaus war der Handlungsrahmen der Mitgliedstaaten als Gesetzgeber bezüglich der Anbieter digitaler Dienste durch eine von der Europäischen Kommission erlassene Durchführungsverordnung[17] europaweit stärker harmonisiert; diese Durchführungsverordnung definierte u.a. die erheblichen Auswirkungen eines Sicherheitsvorfalls und die erforderlichen (im Vergleich mit den Betreibern wesentlicher Dienste geringeren) Sicherheitsvorkehrungen. Meldepflichten für Anbieter digitaler Dienste bestanden nur, wenn der Anbieter Zugang zu den notwendigen Informationen hatte, um die Auswirkungen des Sicherheitsvorfalls zu bewerten (Näheres zu den Meldepflichten[18] siehe TZ 21).

Die öffentliche Verwaltung war von der geltenden NIS–Richtlinie nicht umfasst. Im Gegensatz dazu integrierte das NISG die Einrichtungen des Bundes betreffend seine wichtigen Dienste[19] in seinen Anwendungsbereich, diese Dienste waren allerdings gesetzlich nicht definiert. Die Einrichtungen des Bundes (Tabelle 2) hatten daher – vornehmlich anhand eines vom Bundeskanzleramt erstellten unverbindlichen Umsetzungsleitfadens – selbst zu beurteilen, welche ihrer Netz– und Informationssysteme sie für wichtige Dienste nutzten. Ein zentraler Gesamtüberblick, welche Einrichtung wie viele und welche wichtigen Dienste mit Netz– und Informationssystemen bereitstellte, lag nicht vor.

17 Durchführungsverordnung (EU) 2018/151 vom 13. Jänner 2018, ABl. L 2018/26, 48

18 Die Nichterfüllung von Melde– sowie Nachweispflichten durch die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste stellte eine Verwaltungsübertretung dar. Bis zur Gebarungsüberprüfung gab es nach Auskunft der strategischen NIS–Behörde im Bundeskanzleramt sowie der operativen NIS–Behörde im Innenministerium keine Anlassfälle für Verwaltungsstrafverfahren bei den zuständigen Bezirksverwaltungsbehörden. Die öffentlichen Einrichtungen waren von den Strafbestimmungen nicht erfasst.

19 Das heißt, wenn Einrichtungen des Bundes einen wichtigen Dienst mittels Netz– und Informationssystemen erbringen, wie beispielsweise mittels elektronischer Systeme zur Aktenbearbeitung, Haushaltsverrechnung, Personalverwaltung oder beim Betrieb öffentlicher Register. Beispielhaft waren im Bundeskanzleramt 13, im Bundesministerium für Digitalisierung und Wirtschaftsstandort 14 und im Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz 21 wichtige Dienste definiert (RH–Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 8)).

Die folgende Tabelle gibt einen Überblick über die zentralen Regelungen des NISG zu den Verpflichteten und über ihre im Detail unterschiedlich ausgestalteten Pflichten:

Tabelle 2: Verpflichtete gemäß Netz– und Informationssystemsicherheitsgesetz (NISG)

Regelungen im NISG	Betreiber wesentlicher Dienste	Anbieter digitaler Dienste	Einrichtungen des Bundes
Definition/ Anwendungsbereich (§ 3 Z 9, §§ 10, 12, 13, 18, 19)	privater oder öffentlicher Betreiber eines Dienstes, der – abhängig von Netz– und Informationssystemen ist und – wesentliche Bedeutung[1] für die Funktionsfähigkeit bestimmter Sektoren (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur) hat	– juristische Person oder eingetragene Personengesellschaft, die einen Online–Marktplatz, eine Online–Suchmaschine oder einen Cloud–Computing–Dienst anbietet[2] – ausgenommen Klein– und Kleinstunternehmen	– aufgezählte Einrichtungen des Bundes[3]: Bundesministerien, Gerichtshöfe des öffentlichen Rechts, Rechnungshof, Volksanwaltschaft, Präsidentschaftskanzlei, Parlamentsdirektion – soweit sie wichtige Dienste bereitstellen
Feststellung der Verpflichteten (§ 16)	Ermittlung durch den Bundeskanzler (Bescheid) Kriterien: Schwellenwerte für die Wesentlichkeit gemäß NISV je Teilsektor	Beurteilung durch die Anbieter selbst	Beurteilung durch die Einrichtung selbst
Meldepflichten (§§ 19, 21, 22) (TZ 21)	Meldung eines Sicherheitsvorfalls unverzüglich an Computer–Notfallteam	Meldung eines Sicherheitsvorfalls unverzüglich an Computer–Notfallteam, wenn Informationen zu den Auswirkungen zugänglich sind	Meldung eines Sicherheitsvorfalls unverzüglich an Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) bzw. IKDOK–Teilnehmende direkt an IKDOK
Kriterien Sicherheitsvorfall	Schwellenwerte für die Erheblichkeit gemäß NISV je Teilsektor	Schwellenwerte für die Erheblichkeit aus der NIS–Durchführungsverordnung der EU	individuelle Beurteilung im Anlassfall
Sicherheitsvorkehrungen (§§ 17, 21, 22)	Anforderungen gemäß NISV nach elf Kategorien (z.B. Risikomanagement oder Betriebskontinuität)	Anforderungen gemäß NIS–Durchführungsverordnung der EU (z.B. Informationssicherheit oder Betriebskontinuität)	Beurteilung der Anforderungen durch die Einrichtung, Orientierung an der NISV zulässig
Überprüfung (§§ 17, 21)	Nachweis der Erfüllung der Sicherheitsvorkehrungen regelmäßig (alle drei Jahre) Kontrolle durch den Bundesminister für Inneres jederzeit möglich	Nachweis der Erfüllung der Sicherheitsvorkehrungen und Kontrolle durch den Bundesminister für Inneres nur bei nachweislicher Pflichtverletzung	nicht vorgesehen

GovCERT = Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung) Quelle: NISG
IKDOK = Innerer Kreis der Operativen Koordinierungsstruktur
NISV = Netz– und Informationssystemsicherheitsverordnung

[1] Die Definition der wesentlichen Dienste im NISG orientiert sich an der Definition der kritischen Infrastrukturen in § 22 Sicherheitspolizeigesetz (BGBl. 566/1991 i.d.g.F.).
[2] Dies muss entgeltlich, im Fernabsatz, mit elektronischen Mitteln und auf individuellen Abruf erfolgen.
[3] Einrichtungen der Länder wären nur bei Vorliegen entsprechender Landesgesetze einbezogen (TZ 29).

(3) Umsetzungsvorschriften für Betreiber wesentlicher Dienste

Gemäß der NIS–Richtlinie waren die Betreiber wesentlicher Dienste bis November 2018 zu ermitteln. Die tatsächliche Ermittlung durch den Bundeskanzler verzögerte sich, weil die entsprechenden österreichischen Umsetzungsvorschriften erst zu einem späteren Zeitpunkt in Kraft traten (NISG Ende Dezember 2018, NISV Juli 2019; zu den Personalkapazitäten betreffend die Umsetzung des NISG siehe TZ 27).

Laut NISG war die Wesentlichkeit einzelner Dienste nach der Zahl der Nutzerinnen und Nutzer, der Abhängigkeit anderer Sektoren, dem Marktanteil des Betreibers, der geografischen Ausbreitung des betroffenen Gebiets, der möglichen Auswirkungen von Sicherheitsvorfällen und der Aufrechterhaltung vergleichbarer Dienste zu beurteilen. Die NISV legte dazu je Sektor spezielle Schwellenwerte fest, um die Wesentlichkeit bestimmen zu können (z.B. wenn der Dienst von einer bestimmten Anzahl von Personen genutzt wurde).

(4) Ermittlungsverfahren für Betreiber wesentlicher Dienste

Die Ermittlung der Betreiber wesentlicher Dienste erfolgte in einzelnen, von Amts wegen einzuleitenden Verwaltungsverfahren, die durch konstitutiven Bescheid abgeschlossen wurden. Im Zuge der Ermittlungsverfahren war festzustellen, ob ein Betreiber in einem vom NISG erfassten Sektor[20] tätig war, welche konkreten von Netz– und Informationssystemen abhängigen Dienste er erbrachte und ob diese die festgelegten Schwellenwerte für die Wesentlichkeit überschritten. Schon vor Einleitung des Verwaltungsverfahrens nahm die strategische NIS–Behörde im Bundeskanzleramt auch Amtshilfe in Anspruch, z.B. von Aufsichtsbehörden in den betroffenen Sektoren. Wenn ein Betreiber den Dienst auch in anderen Mitgliedstaaten der EU bereitstellte, musste laut NIS–Richtlinie ein Konsultationsverfahren mit den Behörden dieser anderen Mitgliedstaaten durchgeführt werden. Insgesamt war daher das Ermittlungsverfahren aufwändig. Eine abschließende Feststellung und eine zahlenmäßige Festlegung der Betreiber wesentlicher Dienste waren nicht möglich; grundsätzlich war aufgrund der Amtswegigkeit der Einleitung der Verfahren eine laufende Aktualisierung erforderlich.

Von August bis Ende Dezember 2019 erließ der Bundeskanzler 35 rechtskräftige Bescheide, bis Ende 2020 weitere 41, Anfang 2021 wurden weitere elf Bescheide rechtskräftig. Insgesamt waren zur Zeit der Gebarungsüberprüfung sohin 87 Verfah-

[20] Die sieben Sektoren waren: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser und digitale Infrastruktur. Auch für jene Betreiber wesentlicher Dienste in den Sektoren Bankwesen, Finanzmarktinfrastrukturen und digitale Infrastruktur, die hinsichtlich Sicherheitsvorkehrungen und/oder Meldepflichten sektorspezifischen Rechtsgrundlagen unterlagen, sah das NISG die Ermittlung vor (TZ 2).

ren abgeschlossen, die 83 Betreiber betrafen. Im ersten Halbjahr 2021 waren noch weitere Ermittlungsverfahren im Sektor Gesundheit anhängig bzw. ausständig.

Nach dem Vorschlag der Europäischen Kommission für eine Weiterentwicklung der NIS–Richtlinie von Dezember 2020 (siehe TZ 30) soll die generelle Pflicht zur Ermittlung der Betreiber wesentlicher Dienste entfallen.

(5) Sicherheitsvorkehrungen und Überprüfungen

- Die ermittelten Betreiber wesentlicher Dienste hatten ausgehend von einer Risikoanalyse sowohl technische als auch organisatorische Sicherheitsmaßnahmen zu setzen. Nähere Anforderungen dazu waren in der NISV festgelegt und wurden in einem gemeinsamen Leitfaden der NIS–Behörden des Bundeskanzleramts und des Innenministeriums erläutert. Zum Nachweis der Erfüllung der Sicherheitsanforderungen hatten sie mindestens alle drei Jahre nach ihrer Ermittlung als Betreiber wesentlicher Dienste der operativen NIS–Behörde im Innenministerium eine Aufstellung der getroffenen Sicherheitsmaßnahmen zu übermitteln.[21] Zusätzlich mussten sie die entsprechenden Zertifizierungen oder das Ergebnis von Überprüfungen durch qualifizierte Stellen nachweisen. Als qualifizierte Stellen kamen nur vom Innenministerium auf Antrag mit Bescheid festgestellte Prüfeinrichtungen, die bestimmte Kriterien zu erfüllen hatten, in Betracht. Ende 2020 standen den Betreibern 17 qualifizierte Stellen zur Verfügung. Das Innenministerium hatte eigene Prozesse zur Überprüfung der erbrachten Nachweise und zur Feststellung qualifizierter Stellen eingerichtet. Kontrollen durch Einschauen führte die operative NIS–Behörde bis zur Zeit der Gebarungsüberprüfung keine durch, da seit der Ermittlung der ersten Betreiber noch keine drei Jahre vergangen waren.
- Auf Grundlage eines risikobasierten Ansatzes waren die einzelnen Sicherheitsanforderungen an die Anbieter digitaler Dienste in der NIS–Durchführungsverordnung der Europäischen Kommission weniger streng ausgestaltet als die Anforderungen an die Betreiber wesentlicher Dienste. Sie unterlagen auch nur einer eingeschränkten Überprüfung ex post im Anlassfall, wenn nachweisliche Umstände einer Pflichtverletzung vorlagen.
- Die Einrichtungen des Bundes waren jeweils verantwortlich, die Anforderungen an die verpflichtenden Sicherheitsvorkehrungen für ihre wichtigen Dienste selbst zu beurteilen. Zu ihrer Unterstützung gab das Bundeskanzleramt im September 2019 einen unverbindlichen Umsetzungsleitfaden heraus. Darin wurde es als zweckmäßig bezeichnet, wenn sich die Einrichtungen des Bundes an den Vorschriften für die Betreiber wesentlicher Dienste in der NISV orientieren. Weiters wurden Self Assessments und Audits zur Überprüfung der Sicherheitsvorkehrungen vorgeschlagen.

[21] In den Sektoren Bankwesen sowie Finanzmarktinfrastrukturen und im Subsektor DNS–Dienste waren die speziellen Aufsichtsbehörden (Finanzmarktaufsichtsbehörde und Rundfunk und Telekom Regulierungs–GmbH (RTR–GmbH)) für allfällige Überprüfungen zuständig.

4.2 Der RH verkannte nicht die Komplexität der Verfahren zur Ermittlung der Betreiber wesentlicher Dienste. Er stellte jedoch kritisch fest, dass im Dezember 2020, zwei Jahre nach Inkrafttreten des NISG, die erste Runde der Ermittlungsverfahren noch nicht in allen Sektoren (beispielsweise im Sektor Gesundheit) abgeschlossen war. Weitere Überlegungen zu einer künftigen Vereinfachung der zur Zeit der Gebarungsüberprüfung verwaltungsaufwändigen Ermittlungsverfahren – beispielsweise durch eine Verpflichtung der Betreiber wesentlicher Dienste zur Selbstbeurteilung und Registrierung – hingen davon ab, ob entsprechend dem Vorschlag der Europäischen Kommission zu einer Weiterentwicklung der NIS–Richtlinie (TZ 30) die Ermittlung der Betreiber künftig entfällt und die Anzahl der Sektoren (und damit die Anzahl der Betreiber) erhöht wird. Der RH hielt dazu fest, dass jedenfalls auch künftig ein zentraler Gesamtüberblick über die Betreiber wesentlicher Dienste zweckmäßig wäre.

Er wies weiters kritisch darauf hin, dass – aufgrund der autonomen Identifikation wichtiger Dienste durch die Einrichtungen des Bundes – kein zentraler Gesamtüberblick vorlag, welche IT–Anwendungen als wichtige Dienste bezeichnet und damit besonders schützenswert waren. Im Fall einer Cyber–Krise bzw. eines größeren Sicherheitsvorfalls könnten die operativen Gremien IKDOK und GovCERT[22] daher für die Einrichtungen des Bundes nicht unmittelbar eine spezifische Risikoanalyse oder Lagebeurteilung vornehmen.

Der RH empfahl dem Bundeskanzleramt, in Zusammenarbeit mit dem Innenministerium den operativen Gremien IKDOK und GovCERT einen Gesamtüberblick der wichtigen Dienste des Bundes zur Kenntnis zu bringen und diesen in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement zu berücksichtigen.

Zur Überprüfung der Sicherheitsvorkehrungen bei wichtigen Diensten der Einrichtungen des Bundes verwies der RH auf seinen Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 24). Er kam darin zum Ergebnis, dass nicht alle der überprüften Bundesministerien umfassende Audits durchgeführt hatten.

Der RH empfahl daher dem Bundeskanzleramt, dem Innenministerium, dem Verteidigungsministerium und dem Außenministerium, die getroffenen Sicherheitsvorkehrungen insbesondere betreffend die wichtigen Dienste regelmäßig, vergleichbar mit den Vorschriften des NISG für die Betreiber wesentlicher Dienste, zumindest alle drei Jahre zu auditieren.

Er empfahl den überprüften Bundesministerien, im OpKoord auch die übrigen Bundesministerien und die Länder auf die Bedeutung der regelmäßigen Sicherheitsüberprüfung ihrer wichtigen Dienste hinzuweisen.

[22] Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung)

4.3 (1) Das Bundeskanzleramt verwies in seiner Stellungnahme in Bezug auf einen Gesamtüberblick der wichtigen Dienste des Bundes auf den Cybersicherheitsleitfaden (mit gemeinsamen Empfehlungen der Generalsekretäre zum Vollzug des NISG). Dieser ziele auf eine strukturierte Identifikation und Verwaltung der wesentlichen Dienste gemäß NISG sowie sonstiger essenzieller Tätigkeiten und Vorgänge in allen Ressorts ab. Darüber hinaus würden die Vorhaltung und Pflege der wichtigen Dienste des Bundes sowie deren kontinuierliche Neubeurteilung im Bundeskanzleramt nicht vorhandene Ressourcen voraussetzen. Das Bundeskanzleramt habe diesen Personalbedarf schon bei allen Budget– und Personalplangesprächen mehrmals angemeldet.

Im Zuge der Umsetzung des Projekts „Stärkung der Cyber Defense im BKA“ strebe das Bundeskanzleramt regelmäßige Audits der wichtigen Dienste an; es habe eine begleitende legistische Umsetzung in Evidenz genommen.

Darüber hinaus sagte es die Umsetzung der Empfehlung, die übrigen Bundesministerien und die Länder im Gremium OpKoord auf die Bedeutung regelmäßiger Sicherheitsüberprüfungen hinzuweisen, im Zuge der nächsten Sitzung zu.

(2) Das Innenministerium teilte in seiner Stellungnahme mit, dass das Bundeskanzleramt im Jahr 2019 eine Initiative zur Erhebung der wichtigen Dienste gestartet habe. Es bekräftigte, dem Bundeskanzleramt für eine Wiederaufnahme dieser Initiative jederzeit zur Verfügung zu stehen. Denn aufbauend auf einer solchen Erfassung könnten eine akkordierte Priorisierung und damit Einordnung in die Krisen–, Kontinuitäts– und Einsatzpläne erfolgen.

Für die Informations– und Kommunikationstechnologie des Innenministeriums sei ein Informationssicherheits–Audit–Prozess im Rahmen des Information Security Management System (**ISMS**) in Kraft gesetzt; mit diesem sei sichergestellt, dass alle abgedeckten Geschäftsprozesse, insbesondere die als wichtige Dienste anzusehenden IKT–Services, mindestens einmal in drei Jahren auditiert würden. Darüber hinaus fänden auch jährlich technische Penetrationstests und Code–Reviews durch externe Dienstleister statt. Seit Juni 2021 werde eine Kritikalitätsanalyse durchgeführt, die Ausarbeitung der in der Folge umzusetzenden Maßnahmen werde bis Mitte 2022 abgeschlossen sein.

In Kooperation mit dem Bundeskanzleramt und GovCERT werde eine Information der Vertreter der öffentlichen Verwaltung (Bund und Länder) zur Bedeutung der regelmäßigen Sicherheitsüberprüfung ihrer wichtigen Dienste stattfinden. In dieser solle auf die Möglichkeit der Kooperation und des Informationsaustausches im Rahmen der OpKoord und auf die Notwendigkeiten des NISG hingewiesen werden.

(3) Das Verteidigungsministerium begrüßte in seiner Stellungnahme die Empfehlungen des RH, den operativen Gremien einen Gesamtüberblick über die wichtigen Dienste des Bundes zu übermitteln, diesen in den Krisen–, Kontinuitäts– und Einsatzplänen zu berücksichtigen sowie die Sicherheitsvorkehrungen regelmäßig zu auditieren.

4.4 Zum Hinweis des Bundeskanzleramts auf die nicht vorhandenen Ressourcen hielt der RH fest, dass er die Verantwortung jedes einzelnen Ressorts für die Identifikation seiner wichtigen Dienste nicht verkannte und dass er den Cybersicherheitsleitfaden als gemeinsame Basis zur Erfüllung dieser Verantwortung begrüßte.

Er wiederholte jedoch seine Empfehlung, den operativen Cyber–Sicherheitsgremien IKDOK und GovCERT einen gesammelten Gesamtüberblick zur Verfügung zu stellen, da dieser für das Cyber–Krisenmanagement essenziell ist. Er wiederholte außerdem seine Empfehlung in TZ 27, die für die Aufgabenwahrnehmung zur Aufrechterhaltung der Cyber–Sicherheit als notwendig definierten Personalressourcen in der Abteilung für Cyber–Sicherheit sicherzustellen.

In diesem Zusammenhang verwies der RH auch auf die Möglichkeit, über die das Bundeskanzleramt im Rahmen der Planstellenbewirtschaftung verfügt (Überschreitungsermächtigung im Personalplan 2022).

Darüber hinaus verwies der RH auch auf die zwischenzeitlich erfolgte Modernisierung der „Richtverwendungen für IT–Sonderverträge des Bundes“ (per 1. Jänner 2022 erlassen), mit der laut Innenministerium „im öffentlichen Dienst bestehende Personalrekrutierungsprobleme durch ein modernes Personalmanagement gelöst“ werden sollen (siehe Stellungnahme des Innenministeriums zu TZ 27).

Wirkungs– und leistungsorientierte Steuerung

5.1 (1) Das Bundeskanzleramt und das Innenministerium legten im Rahmen der wirkungsorientierten Haushaltsführung (gemäß Bundeshaushaltsgesetz 2013)[23] zur Erreichung ihrer Wirkungsziele auch Maßnahmen und Kennzahlen (Meilensteine) fest, die sich aus ihren Aufgaben im Bereich der (Koordination der) Cyber–Sicherheit ableiteten.

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

(a) Das Bundeskanzleramt setzte die meisten der im Rahmen der Angaben zur Wirkungsorientierung selbst festgelegten Maßnahmen im Zusammenhang mit der Koordination der Cyber–Sicherheit in den Jahren 2018 bis 2020 verspätet oder nicht um:

Tabelle 3: Angaben des Bundeskanzleramts zur Wirkungsorientierung in den Bundesvoranschlägen 2018 bis 2021[1]

Bundeskanzleramt – Wirkungsziele in Zusammenhang mit Cyber–Sicherheit			
Wirkungsziele	– hoher Nutzen der Koordinationsleistungen des Bundeskanzleramts (2018 bis 2020) – hoher Beitrag des Bundeskanzleramts für ein friedliches, sicheres und chancengleiches Zusammenleben (2021)		
Umsetzung	Maßnahmen zur Erreichung der Wirkungsziele	Kennzahl/Meilenstein zur Messung des Erfolgs	erfüllt
2018	Einrichtung der strategischen NIS–Behörde und Inkrafttreten NISG	NISG bis Mai 2018	verspätet (Dezember 2018) (TZ 2)
	Ermittlung der Betreiber wesentlicher Dienste	150 Betreiber ermittelt	nein (TZ 4)
2019	Monitoring der Betreiber wesentlicher Dienste hinsichtlich der ergriffenen Sicherheitsvorkehrungen	– Bewertungskriterien zur Umsetzung der Sicherheitsvorkehrungen festgelegt und – 50 Betreiber überprüft	nein, mangels Zuständigkeit (Innenministerium nach später erlassenem NISG zuständig)
2020	Aktualisierung der Österreichischen Strategie für Cyber Sicherheit	Vorlage an Bundesregierung bis Ende 2020	nein, Ausarbeitung verzögert (TZ 3)
	Ermittlung der Betreiber wesentlicher Dienste	Ermittlungsquote 100 %	nein, Verfahren verzögert (TZ 4)
	rasche Reaktion auf Cyber–Angriffe gegen IT–Einrichtungen des Bundes	Einsatzbereitschaft vor Ort innerhalb von drei Stunden	keine Anlassfälle 2020
2021	Koordination europäischer Cyber–Übungen	Anzahl der Teilnehmerinnen und Teilnehmer (14) und Bewertung der Cyber–Übungen (Note 2)	noch nicht beurteilbar
	transparentes und lückenloses Meldesystem (zur Überprüfung der Meldeschwellenwerte der NISV)	gemeldete Cyber–Vorfälle (mindestens 20)	noch nicht beurteilbar

NIS = Netz– und Informationssystemsicherheit
NISG = Netz– und Informationssystemsicherheitsgesetz
NISV = Netz– und Informationssystemsicherheitsverordnung

[1] gemäß § 23 Bundeshaushaltsgesetz 2013 Quellen: Budgets 2018 bis 2021 mit Detaildokumenten; BKA

(b) Das Innenministerium konnte die im Rahmen der Angaben zur Wirkungsorientierung selbst festgelegten Zielwerte der Kennzahlen im Zusammenhang mit der Koordination der Cyber–Sicherheit 2018 und 2019 übererfüllen. 2020 war die vollständige Umsetzung der Maßnahmen aufgrund der COVID–19–Pandemie nicht möglich:

Tabelle 4: Angaben des Innenministeriums zur Wirkungsorientierung in den Bundesvoranschlägen 2018 bis 2021[1]

Innenministerium – Wirkungsziele in Zusammenhang mit Cyber–Sicherheit			
Wirkungsziel	Ausbau des hohen Niveaus der öffentlichen Ruhe, Ordnung und Sicherheit in Österreich, insbesondere durch bedarfsorientierte polizeiliche Präsenz, Verkehrsüberwachung, Schutz kritischer Infrastrukturen und sinnvolle internationale Kooperation		
Umsetzung	Maßnahmen zur Erreichung des Wirkungsziels	Kennzahl zur Messung des Erfolgs	erfüllt (Ist–Wert)
2018	Stärkung der Cyber–Sicherheit und des Schutzes kritischer Infrastrukturen	Anzahl der Präventionsveranstaltungen zur Cyber–Sicherheit (31)	ja (48)
		Bewertung der Präventionsveranstaltungen (Note 1,9)	ja (1,0)
2019	Stärkung der Cyber–Sicherheit und des Schutzes kritischer Infrastrukturen	Anzahl der Präventionsveranstaltungen zur Cyber–Sicherheit (36)	ja (78)
		Bewertung der Präventionsveranstaltungen (Note 1,9)	ja (1,1)
2020	Stärkung der Cyber–Sicherheit und des Schutzes kritischer Infrastrukturen	Anzahl der Präventionsveranstaltungen zur Cyber–Sicherheit (41)	nein[2] (6)
		Bewertung der Präventionsveranstaltungen (Note 1,1)	nein[2] (keine Note)
2021	Stärkung der Cyber–Sicherheit und des Schutzes kritischer Infrastrukturen	Anzahl der Präventionsveranstaltungen zur Cyber–Sicherheit (41)	noch nicht beurteilbar
		Bewertung der Präventionsveranstaltungen (Note 1,1)	noch nicht beurteilbar

[1] gemäß § 23 Bundeshaushaltsgesetz 2013
[2] geringe Anzahl und keine Benotung aufgrund der COVID–19–Pandemie

Quellen: Budgets 2018 bis 2021 mit Detaildokumenten; BMI

(2) Das Außenministerium war bei der Koordination der Cyber–Sicherheit von besonderer Bedeutung, da Sicherheitsvorfälle in der Regel einen Auslandsbezug aufweisen und sich daraus eine außenpolitisch relevante Situation ergeben kann und insbesondere die „Fachexpertise in Bereichen wie Cyberdiplomatie“ notwendig ist. Das Außenministerium definierte in den Bundesvoranschlägen 2018 bis 2021

jedoch keine Wirkungsziele, Maßnahmen oder Kennzahlen im Zusammenhang mit der Koordination der Cyber–Sicherheit.

(3) Das Verteidigungsministerium führte 2018 bis 2020 in den ergänzenden Dokumenten zum Bundesvoranschlag und 2021 im Bundesvoranschlag im Rahmen seiner Kernkompetenz Cyber–Defence ein Projekt zum Aufbau von Kompetenzen sowie den geplanten Realisierungsgrad an.

5.2 Grundsätzlich bewertete der RH es als positiv, dass das Bundeskanzleramt und das Innenministerium zur Erreichung ihrer Wirkungsziele in den Budgets 2018 bis 2021 u.a. auch konkrete Maßnahmen und Kennzahlen aus dem Bereich der Koordination der Cyber–Sicherheit festgelegt hatten.

Zur verzögerten bzw. verspäteten Durchführung der vom Bundeskanzleramt im Budget 2018 und 2020 angeführten Maßnahmen und zur daraus resultierenden Nichterfüllung der festgelegten Kennzahlen verwies der RH auf seine Feststellungen bzw. Empfehlungen in TZ 2 (Inkrafttreten NISG), TZ 3 (Aktualisierung Cyber–Sicherheitsstrategie) und TZ 4 (Ermittlung der Betreiber wesentlicher Dienste).

Der RH hielt fest, dass das Innenministerium zwar die definierte Anzahl an Präventionsveranstaltungen und die angestrebte Benotung (durch die Teilnehmenden) 2018 und 2019 in hohem Ausmaß übererfüllt hatte, die gewählten Indikatoren (Anzahl und Bewertung von Veranstaltungen) waren allerdings nicht ausreichend relevant für die Beurteilung der Koordination bzw. Stärkung der Cyber–Sicherheit.

Der RH empfahl dem Innenministerium, für die Angaben zur Wirkungsorientierung aussagekräftigere Kennzahlen im Hinblick auf seine Kernaufgaben bei der Koordination der Cyber–Sicherheit auszuwählen.

Der RH stellte kritisch fest, dass das Außenministerium in den Angaben zur Wirkungsorientierung in den Bundesvoranschlägen 2018 bis 2021 keinen Bezug auf die Koordination der Cyber–Sicherheit nahm, obwohl es bei der Koordination der Cyber–Sicherheit aufgrund des regelmäßigen Auslandsbezugs von Sicherheitsvorfällen und seiner Expertise im Bereich der Cyber–Diplomatie von besonderer Bedeutung war.

Er empfahl daher dem Außenministerium, seine Aufgaben bei der Koordination der Cyber–Sicherheit in den Angaben zur Wirkungsorientierung abzubilden.

Weiters stellte der RH fest, dass das Verteidigungsministerium zu seiner zentralen Aufgabe der Cyber–Defence eine Maßnahme auswies.

Aufgrund der vorgegebenen Koordinierungsstrukturen und Aufgabenverteilung zwischen den vier vorwiegend betroffenen Bundesministerien (Bundeskanzleramt, Innenministerium, Verteidigungsministerium und Außenministerium) sah der RH die Gewährleistung der Cyber–Sicherheit als Querschnittsmaterie. Der RH verwies diesbezüglich auch auf seinen Bericht „Umsetzung der Gleichstellung im Rahmen der Wirkungsorientierung im BKA, BMLFUW und BMVIT“ (Reihe Bund 2017/51), in dessen TZ 6 er festgestellt hatte, dass eine gemeinsame, strategisch und operativ abgestimmte Vorgehensweise die Wirkung der gesetzten Einzelmaßnahmen verstärken und die Zielerreichung positiv unterstützen kann.

Er empfahl daher dem Bundeskanzleramt als strategischem Koordinator der Cyber–Sicherheit, verstärkt auf die ressortübergreifende Abstimmung bei den Angaben zur Wirkungsorientierung, die die Querschnittsmaterie Cyber–Sicherheit betreffen, hinzuwirken.

5.3 (1) Das Bundeskanzleramt sagte in seiner Stellungnahme zu, in der Steuerungsgruppe–CSS die Empfehlung vorzustellen, verstärkt auf die ressortübergreifende Abstimmung der Querschnittsmaterie Cyber–Sicherheit bei den Angaben zur Wirkungsorientierung hinzuwirken.

(2) Das Innenministerium teilte in seiner Stellungnahme mit, dass im Hinblick auf die mit 1. Dezember 2021 durchgeführte Umorganisation und Einrichtung der Abteilung Netz– und Informationssystemsicherheit für das Jahr 2021 eine Änderung der Kennzahlen unterblieben sei. Eine Überarbeitung der Kennzahlen sei für das Jahr 2022 geplant.

(3) Das Außenministerium verwies in seiner Stellungnahme darauf, dass sein Wirkungsziel 2 die Sicherstellung der außen–, sicherheits–, europa– und wirtschaftspolitischen Interessen Österreichs in Europa und in der Welt umfasse und dies auch die Koordination der Cyber–Sicherheit beinhalte. Es werde daher die Empfehlung berücksichtigen.

Gremien zur Koordination der Cyber–Sicherheit

6 Die nachfolgende Tabelle stellt wesentliche Gremien zur Koordination der Cyber–Sicherheit dar. Weiters zeigt sie, welche der von der Gebarungsüberprüfung umfassten Bundesministerien (Bundeskanzleramt, Innenministerium, Verteidigungsministerium, Außenministerium) darin vertreten waren und welche Rolle sie jeweils wahrnahmen (die Gremien werden in den nachfolgenden TZ 7 bis TZ 20 beschrieben):

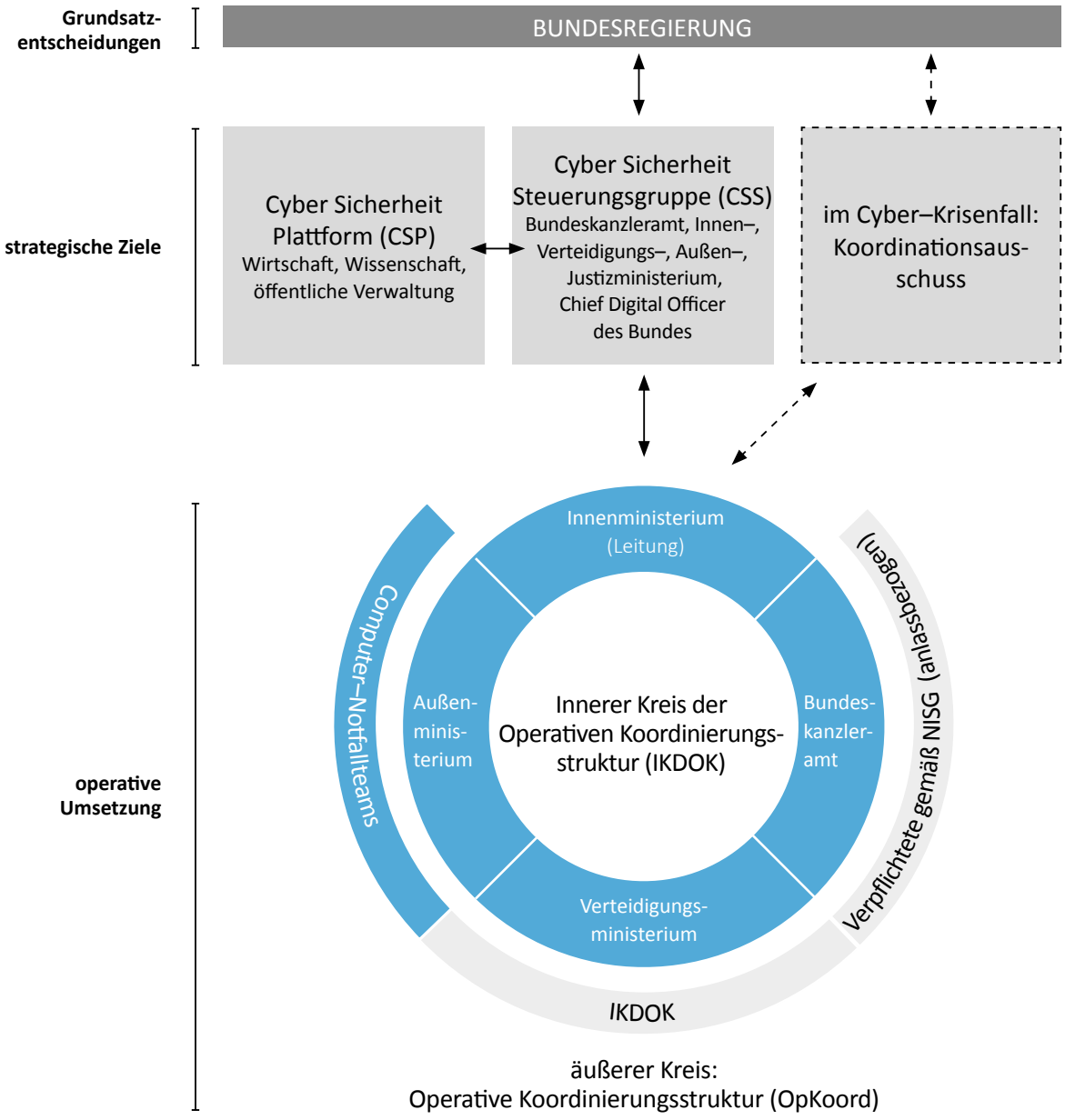
Tabelle 5: Strategische und operative Gremien zur Koordination der Cyber–Sicherheit

Gremium	Bundes-kanzleramt	Innen-ministe-rium	Verteidi-gungs-ministerium	Außen-ministe-rium	sonstige Mitglieder (Teilnehmende)	Ver-weis TZ
strategische und Krisen–Koordination						
Cyber Sicherheit Steuerungsgruppe (Steuerungsgruppe–CSS)	Vorsitz	Mitglied	Mitglied	Mitglied	Justizministerium ab 2013 Chief Information Officer (CIO) des Bundes themenorientiert: weitere Bundesministerien bzw. Länder	TZ 8
Cyber Sicherheit Plattform (CSP)	Sekretariat	nicht anwendbar, da personenbezogene (nicht organisationsbezogene) Mitgliedschaft				TZ 9
Cyberkrisen-management–Koordinations-ausschuss (CKM–KA)	Mitglied	Vorsitz	Mitglied	Mitglied	Generaldirektor für die öffentliche Sicherheit (Innenministerium), Chef des Generalstabs (Verteidigungsministerium), Generalsekretär des Bundeskanzleramts und des Außenministeriums; weitere Vertreterinnen und Vertreter von Bundes– und Landesbehörden, von Betreibern wesentlicher Dienste, CERTs und Einsatzorganisationen (soweit erforderlich)	TZ 10
Lagebild und operative Koordination						
Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)	Mitglied	Vorsitz	Mitglied	Mitglied	keine	TZ 11
Operative Koordinierungsstruktur (OpKoord)	Mitglied	Vorsitz	Mitglied	Mitglied	Computer–Notfallteams der Sektoren CERTs, Vertreterinnen und Vertreter von Betreibern wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung	TZ 11
Computer–Notfallteams (CERTs)						
CERT–Verbund	Vorsitz	keine Teilnahme	Mitglied	keine Teilnahme	16 CERTs, 14 davon scheinen öffentlich auf	TZ 18
GovCERT	Vorsitz	keine Teilnahme	keine Teilnahme	keine Teilnahme	Bundesministerien, Länder, teilweise Städte und Gemeinden	TZ 19

CERT = Computer Emergency Response Team (Computer–Notfallteam) Quelle: BKA
GovCERT= Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung)

Die folgende Abbildung stellt die Struktur der Koordination der Gremien zur Koordination der Cyber–Sicherheit überblicksmäßig dar:

Abbildung 1: Organisation der Cyber–Sicherheit gemäß NISG



Quellen: BKA; BMI; Darstellung: RH

Strategische Cyber–Koordination

Überblick

7 Die strategische Steuerung der Cyber–Sicherheit teilte sich in organisatorischer Hinsicht wie folgt auf:

(a) Die Bundesregierung machte mit ihrem (jeweiligen) Regierungsprogramm grundsätzliche Vorgaben und konnte über einzelne Beschlüsse gesetzliche Regelungen initiieren oder konkrete Aufträge erteilen, welche von den Bundesministerinnen und Bundesministern in ihrem jeweiligen Wirkungsbereich umzusetzen waren (TZ 8).

(b) 2012 richtete die Bundesregierung die Steuerungsgruppe–CSS beim Bundeskanzleramt (als vorsitzführendem Bundesministerium) ein. Ihren Kern bildeten Vertreterinnen und Vertreter des Bundeskanzleramts, des Innen–, des Verteidigungs–, des Außen– und des Justizministeriums sowie der Chief Information Officer des Bundes. Sie konnte im Bedarfsfall um Vertreterinnen und Vertreter weiterer Bundesministerien und der Länder erweitert werden. Ihre zentralen Aufgaben waren die Erarbeitung und Aktualisierung der Cyber–Sicherheitsstrategie, die Erstellung regelmäßiger Berichte zur Cyber–Sicherheit und die Beratung der Bundesregierung in Angelegenheiten der Cyber–Sicherheit (TZ 9).

(c) Mit Beschluss der Steuerungsgruppe–CSS wurde 2014 die Cyber Sicherheit Plattform (CSP) eingerichtet. Sie diente der Vernetzung von Verwaltung, Wirtschaft, Wissenschaft und Forschung und sollte damit auch die Arbeit der Steuerungsgruppe–CSS unterstützen. Sie hatte rd. 300 Mitglieder und wurde als öffentlich–private Partnerschaft (Public Private Partnership) betrieben: Den Vorsitz führten zwei Experten aus der Wirtschaft, die administrative Unterstützung (Sekretariat) übernahm das Bundeskanzleramt (TZ 10).

Bundesregierung

8.1 (1) Seit 2018 war das Bundeskanzleramt ausdrücklich auch für „Angelegenheiten der strategischen Netz– und Informationssicherheit“[24] und damit auch für die zentrale Koordination in Angelegenheiten der Cyber–Sicherheit zuständig. Unter dem Vorsitz des Bundeskanzlers konnte daher die Bundesregierung – als Gesamtheit der jeweils ressortverantwortlichen Bundesministerinnen und Bundesminister[25] – zentrale strategische Vorgaben zur Cyber–Sicherheit beschließen. Diese kamen im jeweiligen Regierungsprogramm sowie in einzelnen Beschlüssen der Bundesregie-

[24] Bundesministeriengesetz–Novelle 2017, BGBl. I 164/2017

[25] vgl. dazu Art. 69 Bundes–Verfassungsgesetz

rung zum Ausdruck. Das Regierungsprogramm 2020–2024 legte dazu im Kapitel „Cybersicherheit und Digitalisierung“ u.a. folgende Ziele fest:

- Aktualisierung der österreichischen Cyber–Sicherheitsstrategie,
- Verbesserung der Kooperation der Institutionen bzw. Verstärkung der Koordination zwischen den bestehenden Organisationen im Bereich Cyber–Sicherheit unter Absicherung des bisherigen Informationsaustausches,
- Schaffung eines staatlichen Cyber–Sicherheitszentrums und der dafür notwendigen Rechtsgrundlagen,
- Förderung eines strukturierten und institutionalisierten Wissenstransfers zwischen Bildung, Wissenschaft, Forschung und Wirtschaft,
- Koordinierung der politischen Positionierung bei interdisziplinären Cyber–Sicherheitsthemen (z.B. 5G–Sicherheitsstandards, künstliche Intelligenz, Internet der Dinge),
- Umsetzung verbindlicher, überprüfbarer und durchsetzbarer Sicherheitsstandards im Rahmen der NIS–Richtlinie im öffentlichen Sektor.

(2) Seit 2012 fasste die Bundesregierung insgesamt vier konkrete für die Koordination der Cyber–Sicherheit relevante Beschlüsse:

- 2012 richtete sie die Steuerungsgruppe–CSS (TZ 9) ein und beauftragte diese gleichzeitig mit der Erarbeitung der Cyber–Sicherheitsstrategie,
- 2013 beschloss sie die von der Steuerungsgruppe–CSS ausgearbeitete Strategie (TZ 3),
- 2015 nahm sie einen Umsetzungsbericht der Steuerungsgruppe–CSS dazu zur Kenntnis und
- 2018 beschloss sie die Regierungsvorlage zum NISG (TZ 2).

8.2 Der RH wies kritisch darauf hin, dass die Bundesregierung seit 2012 lediglich vier Beschlüsse im Zusammenhang mit der Koordination der Cyber–Sicherheit gefasst hatte. Das aktuelle Regierungsprogramm 2020–2024 enthielt zwar grundsätzliche Vorhaben zur Cyber–Sicherheit, wie das Ziel, die Cyber–Sicherheitsstrategie zu aktualisieren oder ein staatliches Cyber–Sicherheitszentrum zu schaffen. Diese waren jedoch allgemein und offen formuliert und bedurften daher der genaueren Konkretisierung, beispielsweise durch weitere Beschlüsse der Bundesregierung.

Der RH hielt dazu fest, dass eine solche Beschlussfassung eine regelmäßige Beratung und Information über aktuelle Entwicklungen und darauf aufbauende inhaltliche Vorarbeiten der für die Koordination der Cyber–Sicherheit eingerichteten nationalen Gremien voraussetzte. Er verwies daher auf seine Feststellungen und Empfehlungen in TZ 9 betreffend die für die regelmäßige Beratung und Information zuständige Steuerungsgruppe–CSS.

Der RH empfahl dem Bundeskanzleramt als dem für die zentrale Koordination in Angelegenheiten der Cyber–Sicherheit zuständigen Bundesministerium, der Bundesregierung weitere Beschlüsse bzw. Projekte zur Umsetzung der im Regierungsprogramm 2020–2024 angeführten Schwerpunkte zur Cyber–Sicherheit vorzubereiten. Dabei wären insbesondere die regelmäßigen Berichte der Steuerungsgruppe–CSS zu beachten.

8.3 Das Bundeskanzleramt teilte dazu in seiner Stellungnahme mit, dass es im Zuge der Maßnahmenerhebung zur Umsetzung der Cyber–Sicherheitsstrategie verstärkt auf Projekte zur Umsetzung der im Regierungsprogramm angeführten Schwerpunkte zur Cyber–Sicherheit hinweisen werde. Mittels der dynamischen, flexiblen Plattform zur Erhebung und Steuerung konkreter Maßnahmen zur Umsetzung der Strategie würden zukünftig der Steuerungsgruppe–CSS regelmäßige Status– und Fortschrittsberichte vorgelegt.

Cyber Sicherheit Steuerungsgruppe

9.1 (1) Im Mai 2012 richtete die (damalige) Bundesregierung die Steuerungsgruppe–CSS ein und beauftragte sie mit der Erarbeitung einer gesamtstaatlichen Cyber–Sicherheitsstrategie (TZ 3). Mit Beschluss der Cyber–Sicherheitsstrategie im Jahr 2013 wurde die Steuerungsgruppe–CSS auf Dauer eingerichtet. Sie bestand aus Vertreterinnen und Vertretern des Bundeskanzleramts, des Innen–, des Verteidigungs–, des Außen– und des Justizministeriums sowie dem Chief Information Officer des Bundes. Themenbezogen konnte die Steuerungsgruppe–CSS auch um Vertreterinnen und Vertreter der anderen Bundesministerien, der Länder sowie der Cyber Sicherheit Plattform (CSP) (TZ 10) und weiterer sicherheitsrelevanter Organisationen und Unternehmen erweitert werden.

Die Steuerungsgruppe–CSS sollte auf „politisch–strategischer Ebene“

- die Maßnahmen zur Cyber–Sicherheit koordinieren,
- die Umsetzung der Cyber–Sicherheitsstrategie beobachten und begleiten,
- regelmäßig zur Cyber–Sicherheit berichten (jährlich ein Bericht an die Öffentlichkeit und alle zwei Jahre ein Bericht zur Umsetzung der Cyber–Sicherheitsstrategie an die Bundesregierung) sowie
- die Bundesregierung in Angelegenheiten der Cyber–Sicherheit beraten.

(2) Ihre Geschäftsordnung sah vor, dass das vorsitzführende Bundeskanzleramt die Steuerungsgruppe–CSS mindestens zweimal jährlich einberuft. Seit 2012 fanden insgesamt 14 Sitzungen statt, davon in den Jahren 2015, 2016, 2018 und 2019 jeweils eine. Die letzte Sitzung des überprüften Zeitraums datierte vom Juli 2019.

Insgesamt elfmal tagte die Steuerungsgruppe–CSS unter Beteiligung der anderen Bundesministerien, ab 2015 nahmen auch die Vorsitzenden der Cyber Sicherheit Plattform (CSP) an den Sitzungen teil. Ländervertreterinnen und –vertreter nahmen fünfmal, zuletzt im Oktober 2017, an den Sitzungen teil.

(3) Wesentliche Arbeitsergebnisse der Steuerungsgruppe–CSS waren:

- In der Anfangsphase ihres Bestehens erstellte sie u.a. einen Implementierungsplan für die Cyber–Sicherheitsstrategie und beschloss 2014 die Einrichtung der Cyber Sicherheit Plattform (CSP). Sie leistete außerdem umfassende Vorarbeiten zur legistischen Umsetzung der NIS–Richtlinie durch das NISG. Zudem setzte sie sich auch mit Themen wie den Sicherheitsaspekten im Zusammenhang mit Künstlicher Intelligenz und dem neuen Mobilfunkstandard 5G auseinander.
- Weiters erstellte die Steuerungsgruppe–CSS jährlich einen Bericht zur Cyber–Sicherheit, welcher auf der Website des Bundeskanzleramts publiziert wurde. Mit der Kundmachung des NISG im Dezember 2018 kam die Verantwortung für diesen Bericht ausdrücklich dem Bundeskanzler zu.
- Den in der Cyber–Sicherheitsstrategie alle zwei Jahre vorgesehenen Umsetzungsbericht zu dieser Strategie an die Bundesregierung erstattete die Steuerungsgruppe–CSS nur 2015. Im Oktober 2017 empfahl sie die Aufnahme der Überarbeitung der Cyber–Sicherheitsstrategie in das (damals) neue Regierungsprogramm 2017–2022 (TZ 3). Damit begründete das Bundeskanzleramt auch das Unterbleiben weiterer Umsetzungsberichte an die Bundesregierung.
- Im Oktober 2014 beschloss die Steuerungsgruppe–CSS ein Grundsatzkonzept zum Cyber–Krisenmanagement und darauf aufbauend die Ausarbeitung entsprechender „Krisen– und Kontinuitätspläne“; eine Ausarbeitung dieser Pläne unterblieb. In ihrer letzten Sitzung im Juni 2019 beschloss die Steuerungsgruppe–CSS neuerlich ein Konzept mit dem Titel „Gesamtstaatliches Cyber Krisenmanagement“, welches wiederum die „Vorbereitung eines Krisen– und Einsatzplanes“ für Cyber–Krisen vorsah; im Mai 2021 lag dieser Plan noch nicht vor.
- Im Oktober 2017 beschloss die Steuerungsgruppe–CSS, bis Anfang 2018 einen Konzeptentwurf zur Koordination von Cyber–Übungen auszuarbeiten. Ziel war es, einen Überblick über die vergangenen und geplanten Übungsaktivitäten in Österreich zu erhalten und so ein abgestimmtes Vorgehen zu ermöglichen. Im Mai 2021 lag ein derartiges Konzept noch nicht vor. Das Bundeskanzleramt verwies dazu auf ein Projekt (CURSOR – Cyber security exercise concept and framework) im Rahmen der österreichischen Förderplattform für Sicherheitsforschung KIRAS, mit dem ein solches Konzept erarbeitet werden sollte. Nachdem das Projekt im März 2021 abgeschlossen worden war, rechnete das Bundeskanzleramt mit der zeitnahen „Operationalisierung eines Konzepts zur Koordination von Cyber–Übungen im Rahmen interministerieller Abstimmung“.

9.2 (1) Der RH erachtete die Steuerungsgruppe–CSS als grundsätzlich geeignetes Gremium zur gesamtstaatlichen strategischen Koordinierung der Cyber–Sicherheit. Die Steuerungsgruppe–CSS war auch geeignet, die im Regierungsprogramm 2020–2024 enthaltenen Vorgaben der Bundesregierung zur Cyber–Sicherheit weiter zu konkretisieren (TZ 8).

Der RH anerkannte insbesondere die von der Steuerungsgruppe–CSS erbrachten inhaltlichen Vorarbeiten zur Umsetzung der NIS–Richtlinie, die Etablierung der Cyber Sicherheit Plattform (CSP), die jährlichen Berichte zur Cyber–Sicherheit und auch die Bearbeitung weiterer relevanter Themen, wie der Sicherheitsaspekte im Zusammenhang mit Künstlicher Intelligenz und dem neuen Mobilfunkstandard 5G.

(2) Der RH wies allerdings auf den im Aufgabenkatalog der Steuerungsgruppe–CSS enthaltenen Berichts– und Beratungsauftrag gegenüber der Bundesregierung hin. Über diesen sollte die Bundesregierung mit aktuellen Informationen insbesondere zur Umsetzung der Cyber–Sicherheitsstrategie versorgt und in weiterer Folge auch in die Lage versetzt werden, ihre strategischen Vorgaben laufend weiterzuentwickeln, konkrete Umsetzungsaufträge zu erteilen und allfällig notwendige gesetzliche Änderungen zu initiieren.

Der RH kritisierte, dass

- seit Juli 2019 keine Sitzung der Steuerungsgruppe–CSS mehr stattgefunden hatte, obwohl das Bundeskanzleramt diese mindestens zweimal im Jahr einzuberufen gehabt hätte, und
- lediglich ein Umsetzungsbericht zur Cyber–Sicherheitsstrategie (im Jahr 2015) an die Bundesregierung erstattet wurde, obwohl diese Strategie eine Berichterstattung alle zwei Jahre vorsah.

Damit wurde das Potenzial der Steuerungsgruppe–CSS nicht ausgeschöpft, hiedurch fehlte der Bundesregierung eine wichtige Grundlage zur Weiterentwicklung ihrer strategischen Vorgaben sowie der rechtlichen Grundlagen zur Cyber–Sicherheit. Der RH verwies weiters auf den gesamtstaatlichen Ansatz der Cyber–Sicherheitsstrategie, der eine Einbeziehung des Bundesministeriums für Digitalisierung und Wirtschaftsstandort (in der Folge: **Digitalisierungsministerium**) und der Länder auch auf Ebene der strategischen Koordination notwendig machte.

Der RH empfahl daher dem Bundeskanzleramt,

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

(3) Der RH hielt positiv fest, dass die Steuerungsgruppe–CSS bereits im Oktober 2014 und neuerlich im Juni 2019 die Ausarbeitung von Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement beschlossen hatte. Er kritisierte jedoch, dass diese Pläne im Mai 2021, d.h. über sechs Jahre nach dem ersten Beschluss zu ihrer Ausarbeitung, noch nicht vorlagen, obwohl Krisen–, Kontinuitäts– und Einsatzpläne essenzielle Bestandteile eines funktionierenden Cyber–Krisenmanagements sind. Dazu verwies der RH auf seine Feststellungen in TZ 26 und auf seine Empfehlung, dass das Innenministerium und das in der Steuerungsgruppe–CSS den Vorsitz führende Bundeskanzleramt konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement ausarbeiten sollten.

(4) Der RH hielt auch positiv fest, dass die Steuerungsgruppe–CSS bereits im Oktober 2017 die Ausarbeitung eines Konzeptentwurfs zur Koordination von Cyber–Übungen beschlossen hatte. Er kritisierte jedoch, dass dieses Konzept im Mai 2021, d.h. mehr als drei Jahre später, noch nicht vorlag, und verwies darauf, dass die Nutzung der im Rahmen von Cyber–Übungen gewonnenen Erkenntnisse zur Aufdeckung bestehender Schwachstellen im System der Koordination notwendig ist.

Er empfahl daher dem Bundeskanzleramt, ein gesamtstaatliches Cyber–Übungsprogramm zu etablieren, um einen Überblick über die vergangenen und geplanten Übungsaktivitäten in Österreich zu erhalten und ein auf nationaler Ebene abgestimmtes Vorgehen zu ermöglichen.

9.3 Das Bundeskanzleramt teilte in seiner Stellungnahme mit, die Empfehlung bereits aufgegriffen und mittlerweile die regelmäßige Einberufung der Steuerungsgruppe–CSS wieder aufgenommen zu haben. Eine Einbindung des Digitalisierungsministeriums erachte das Bundeskanzleramt als wertvoll; dies sei in der neuen Strategie für Cybersicherheit bereits festgelegt.

Zur Etablierung eines gesamtstaatlichen Cyber–Übungsprogramms werde das Bundeskanzleramt die Umsetzung prüfen.

9.4 Der RH nahm von den ersten Umsetzungsschritten des Bundeskanzleramts Kenntnis. Darüber hinaus wiederholte er seine Empfehlung für regelmäßige Berichte zur Cyber–Sicherheit an die Bundesregierung, um dieser eine wichtige Grundlage zur Weiterentwicklung ihrer strategischen Vorgaben sowie der rechtlichen Grundlagen zur Cyber–Sicherheit zur Verfügung zu stellen.

Cyber Sicherheit Plattform

10.1 (1) Die Cyber–Sicherheitsstrategie sah die Einrichtung einer Plattform zur laufenden Kommunikation „mit allen Stakeholdern aus Verwaltung, Wirtschaft und Wissenschaft“ vor. Daher beschloss die Steuerungsgruppe–CSS im Oktober 2014 die Einrichtung der Cyber Sicherheit Plattform (CSP), die sich im November 2015 bei ihrer ersten Arbeitssitzung konstituierte. Sie sollte einen periodischen Informationsaustausch zu wesentlichen Fragen der Cyber–Sicherheit gewährleisten, Kooperationen zwischen den Mitgliedern erleichtern und die Steuerungsgruppe–CSS beraten und unterstützen.

Die Plattform wurde vom Bundeskanzleramt als öffentlich–private Partnerschaft (Public Private Partnership) eingerichtet. Die Mitgliedschaft war nicht organisations–, sondern personenbezogen. Den Vorsitz führten zwei Experten aus der Wirtschaft, die administrative Unterstützung übernahm das Bundeskanzleramt.

(2) Zur Bearbeitung konkreter Themen konnte der Vorsitz innerhalb der Plattform eigene Arbeitsgruppen einrichten. Von dieser Möglichkeit machte der Vorsitz im überprüften Zeitraum fünfmal Gebrauch. Diese Arbeitsgruppen beschäftigten sich insbesondere mit der Sicherheitsforschung, den rechtlichen und regulatorischen Rahmenbedingungen, dem betrieblichen Krisenmanagement, Mindestsicherheitsstandards von IKT–Produkten und der Erarbeitung eines Beitrags zur Überarbeitung der Cyber–Sicherheitsstrategie (TZ 3). Die Arbeiten zu den beiden letztgenannten Themen waren zur Zeit der Gebarungsüberprüfung abgeschlossen.

Die Plattform tagte zwischen 2015 und April 2021 elfmal, wobei an den Arbeitssitzungen jeweils zwischen 95 und 150 Personen teilnahmen. Aktuelle Entwicklungen im Bereich der Cyber–Sicherheit sowie die (Teil–)Ergebnisse der einzelnen Arbeitsgruppen wurden regelmäßig im Plenum berichtet und diskutiert. Um den Informationsfluss zur Steuerungsgruppe–CSS sicherzustellen, nahmen die Vorsitzenden der Plattform ab 2015 auch an den Sitzungen der Steuerungsgruppe–CSS teil.

(3) Die Cyber–Sicherheitsstrategie legte 2013 im Kapitel zur Cyber Sicherheit Plattform weiters fest, dass der Austausch von Expertinnen und Experten zwischen den beteiligten staatlichen, privatwirtschaftlichen und wissenschaftlichen Organisationen gestärkt werden soll, um das gegenseitige Verständnis für die Herausforderun-

gen und die Handlungsmöglichkeiten der beteiligten Stellen zu fördern. Dazu sollte unter Führung der Steuerungsgruppe–CSS mithilfe der Cyber Sicherheit Plattform ein Austauschprogramm erarbeitet werden. Dieses lag zur Zeit der Gebarungsüberprüfung noch nicht vor. Das Bundeskanzleramt teilte dazu mit, dass die Entwicklung des Austauschprogramms ruhend gestellt sei, um es gegebenenfalls nach Beschluss der aktualisierten Cyber–Sicherheitsstrategie (TZ 3) „gleich kompatibel" aufsetzen zu können.

10.2 Der RH beurteilte die Cyber Sicherheit Plattform (CSP) als geeignetes Gremium zur Erreichung der Ziele Vernetzung und Informationsaustausch in Verwaltung, Wirtschaft und Wissenschaft. Er anerkannte auch, dass die Plattform diese Ziele durch regelmäßige Arbeitssitzungen verfolgte und auch die Steuerungsgruppe–CSS – z.B. mit einem Beitrag zur Überarbeitung der Cyber–Sicherheitsstrategie – in ihrer Arbeit unterstützte.

Der RH wies in diesem Zusammenhang auf die Cyber–Sicherheitsstrategie hin, die bereits 2013 festlegte, dass der Austausch von Expertinnen und Experten zwischen den beteiligten staatlichen, privatwirtschaftlichen und wissenschaftlichen Organisationen gestärkt werden sollte. Er kritisierte, dass das für diesen regelmäßigen und vertieften Austausch geplante Austauschprogramm acht Jahre nach Beschluss der Cyber–Sicherheitsstrategie noch nicht vorlag.

Der RH empfahl daher dem Bundeskanzleramt (als dem in der Steuerungsgruppe–CSS vorsitzführenden Bundesministerium), ein Austauschprogramm für Cyber–Sicherheits–Expertinnen und –Experten aus der staatlichen Verwaltung, der Privatwirtschaft und der Wissenschaft zu erarbeiten.

10.3 Das Bundeskanzleramt teilte in seiner Stellungnahme dazu mit, dass es in seiner Rolle als vorsitzführende Stelle in der Steuerungsgruppe–CSS einen entsprechenden Prozess starten werde. Es verwies erneut auf seine aktuelle Personalsituation (TZ 4).

Cyber–Krisenmanagement

11.1 (1) Das NISG (§ 3 Z 22) definierte die Cyber–Krise als „ein[en] oder mehrere Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können".

Die Entscheidung, ob eine solche Cyber–Krise tatsächlich vorlag, oblag dem Bundesminister für Inneres. Bejahendenfalls trat das Cyber–Krisenmanagement in Kraft. Dies war ein „Koordinierungsverfahren zur Bewältigung von Cyberkrisen", das eine effektive (gesamtstaatliche) Reaktion sicherstellen sollte. Das Cyber–Krisenmanagement war Teil des (allgemeinen) staatlichen Krisen– und Katastrophenschutzmanagements, wodurch im Anlassfall bei zu erwartenden schwerwiegenden gesellschaftlichen Auswirkungen alle relevanten staatlichen Stellen inklusive der Blaulichtorganisationen unter Federführung des Bundesministers für Inneres abgestimmt werden konnten. Im Falle eines souveränitätsgefährdenden Angriffs auf die Republik Österreich durch ein anderes Völkerrechtssubjekt ging die federführende Zuständigkeit (im Rahmen des Art. 79 Bundes–Verfassungsgesetz) auf die Bundesministerin für Landesverteidigung über.

(2) Die Leitung und Koordination der (operativen) Maßnahmen zur Bewältigung einer Cyber–Krise oblagen dem Bundesminister für Inneres. Zu seiner Unterstützung war im NISG ein eigener Cyberkrisenmanagement–Koordinationsausschuss (in der Folge: **Koordinationsausschuss**) vorgesehen. Dieser sollte

- den Bundesminister für Inneres bei der Entscheidung über das Vorliegen einer Cyber–Krise sowie hinsichtlich der operativen Maßnahmen zu ihrer Bewältigung und
- die Bundesregierung bei der Koordination der Öffentlichkeitsarbeit

beraten. Der Koordinationsausschuss bestand aus dem Generaldirektor für die öffentliche Sicherheit (Vorsitz: Innenministerium), dem Chef des Generalstabs (Verteidigungsministerium) und den Generalsekretären des Bundeskanzleramts und des Außenministeriums. Diese Zusammensetzung sollte sicherstellen, dass die „strategischen Entscheidungen des Ausschusses und die abgestimmten Maßnahmen" in den jeweiligen Ressortbereichen effizient umgesetzt werden. Die operative Unterstützung oblag dem IKDOK (TZ 13). Erforderlichenfalls konnte der Koordinationsausschuss auch um weitere Bundes– oder Landesbehörden, Betreiber wesentlicher Dienste, Computer–Notfallteams sowie Einsatzorganisationen erweitert werden.

11.2 Der RH erachtete die Definition der Cyber–Krise gemäß NISG, ihre Abgrenzung zum Fall der Cyber–Verteidigung, in dem das Verteidigungsministerium die Federführung übernahm, und die Einbettung des Cyber–Krisenmanagements in das (allgemeine) staatliche Krisen– und Katastrophenschutzmanagement als zweckmäßig. Er erachtete weiters den Koordinationsausschuss als grundsätzlich geeignetes Gremium zur Beratung des Bundesministers für Inneres bei der Bewältigung einer Cyber–Krise: Die konkrete personelle Zusammensetzung dieses Ausschusses mit den höchsten administrativen Funktionsträgern konnte einerseits den unmittelbaren Informationsfluss an die verantwortlichen Regierungsmitglieder und andererseits auch die Umsetzung der Maßnahmen in den jeweiligen Ressortbereichen sicherstellen.

Operative Cyber–Koordination

Überblick

12 Mit dem NISG wurde auf Basis sowie unter Einbindung bestehender operativer Strukturen eine neue Struktur zur Koordination auf der operativen Ebene geschaffen, die aus einem „inneren Kreis“ und einem „äußeren Kreis“ bestand (siehe auch Tabelle 5 sowie Abbildung 1 in TZ 6).

(a) Der Innere Kreis der Operativen Koordinationsstruktur (**IKDOK**) war eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz– und Informationssystemen. Sie bestand aus Vertreterinnen und Vertretern des Bundeskanzlers, der Bundesminister für Inneres und europäische und internationale Angelegenheiten sowie der Bundesministerin für Landesverteidigung (§ 3 Z 4 NISG).

(b) Der „äußere Kreis“, das war die Operative Koordinierungsstruktur (**OpKoord**), bestand aus dem IKDOK und den Computer–Notfallteams.

Organisation und Aufgaben der Koordinierungsgremien

13.1 (1) Der IKDOK hatte folgende in § 7 NISG festgelegte Aufgaben:

(a) Erörterung und Aktualisierung des vom Bundesminister für Inneres erstellten Cyber–Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle:

Das Cyber–Lagebild (siehe auch TZ 15) wurde monatlich erstellt, darüber hinaus gab es auch wöchentliche Besprechungen und Aktualisierungen.

(b) Erörterung der Erkenntnisse, die aus dem Betrieb von solchen IKT–Lösungen gewonnen wurden, welche

- zur Früherkennung von Risiken und Vorfällen von Netz– und Informationssystemen dienten und
- zur Erkennung von Mustern von Angriffen auf Netz– und Informationssysteme.

Derartige IKT–Lösungen waren zur Zeit der Gebarungsüberprüfung noch nicht in Betrieb (TZ 21). IKDOK–Teilnehmende brachten einzelne ihnen bekannt gewordene Erkenntnisse zur Cyber–Sicherheitslage in die IKDOK–Sitzungen ein, sie wurden dort analysiert und gingen direkt in die regelmäßige Cyber–Lagebilderstellung oder in aktuell erforderliche Sonderlagebilder ein. Zusätzlich erstellte und versandte der

IKDOK anlassbezogen Warnschreiben und hielt anlass– und vorfallsbezogene Informationsveranstaltungen ab.

(c) Unterstützung des Koordinationsausschusses im Cyber–Krisenmanagement:

Derartige Unterstützungsleistungen erbrachte der IKDOK im Rahmen der Cyber–Krise im Außenministerium 2020 (siehe TZ 24 bis TZ 26), indem er den im Jänner und Februar 2020 regelmäßig tagenden Koordinationsausschuss laufend über das aktuelle Lagebild informierte.

(2) Folgende Organisationseinheiten aus den vier überprüften Bundesministerien entsandten Vertreterinnen und Vertreter in den IKDOK:

- Bundeskanzleramt: die Abteilung „Cybersicherheit, GovCERT, NIS–Büro[26] und ZAS[27]“ (I/8) einschließlich Vertreter des GovCERT (TZ 18); bei Bedarf wurde weitere Expertise aus dem Bundeskanzleramt hinzugezogen;
- Innenministerium: die Abteilung Cybersicherheit (II/BVT/5) aus dem damaligen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (**BVT**)[28] und das Büro Cybercrime Competence Center inklusive Meldestelle (II/BK/5.2) aus dem Bundeskriminalamt;
- Verteidigungsministerium: das Abwehramt, das Heeresnachrichtenamt und das Militärische Cyberzentrum;
- Außenministerium: die Abteilung Sicherheitsangelegenheiten (I/2) und die Abteilung Sicherheitspolitische Angelegenheiten (II/2).

Die zu entsendenden Personen waren einer Sicherheitsüberprüfung für den Zugang zu geheimer Information zu unterziehen.[29] Zur Zeit der Gebarungsüberprüfung umfasste der für den IKDOK nominierte Teilnehmerkreis insgesamt rd. 40 Personen; an den einzelnen IKDOK–Sitzungen nahmen jeweils etwa 15 bis 20 Personen teil. Je Ressort war eine verantwortliche Kontaktperson festgelegt, die personelle Änderungen ressortweit sammelte und an das federführend zuständige Innenministerium übermittelte.

[26] Büro für Strategische Netz– und Informationssicherheit

[27] Zentrales Ausweichrechenzentrum des Bundes

[28] Im Dezember 2021 wurden die Aufgaben der Abteilung Cybersicherheit aus dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung auf die Abteilung „Netz– und Informationssystemsicherheit“ (einschließlich Cyber–Lagezentrum) in der Sektion IV und auf die Abteilung „Cybersicherheit und Technische Infrastruktur ND“ in der neuen Direktion Staatsschutz und Nachrichtendienst übertragen.

[29] § 3 Z 4 NISG; Zugang zu geheimer Information im Sinne des § 55 Abs. 3 Z 2 Sicherheitspolizeigesetz (BGBl. 566/1991 i.d.g.F.)

(3) Die organisatorische Leitung von IKDOK und OpKoord war gemäß NISG (§ 5 Abs. 1 Z 2) eine der zentralen Aufgaben des Bundesministers für Inneres. Die Durchführung dieser Aufgabe und die Vorsitzführung im Rahmen der Sitzungen oblagen ressortintern der Abteilung Cybersicherheit.

(4) Die OpKoord hatte gemäß § 7 NISG die Aufgabe, das gesamtheitliche Lagebild, das auch die freiwilligen Meldungen enthielt, zu erörtern. Sie bestand aus den Vertretern des IKDOK und der Computer–Notfallteams (nationales CERT (CERT.at; TZ 18) und Austrian Energy CERT (AEC; TZ 18)). Zusätzlich konnten auch Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung miteinbezogen werden, wenn deren Wirkungsbereich von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen war.

Da sowohl für das im IKDOK vertretene GovCERT als auch für die in der OpKoord vertretenen Computer–Notfallteams (CERT.at und Austrian Energy CERT) teilweise dieselben Personen tätig wurden und auch die jeweiligen Organisationen in beiden Gremien vertraten, ergaben sich starke personelle Überschneidungen. Aus diesem Grund wie auch aus Ressourcengründen fanden neben den IKDOK–Sitzungen keine separaten OpKoord–Sitzungen statt.

(5) Wesentliche Aufgaben der Koordinierung der IT kamen auch dem Digitalisierungsministerium zu. Gemäß Bundesministeriengesetz war es für Angelegenheiten der Digitalisierung einschließlich der staatlichen Verwaltung für das Service und die Interaktion mit Bürgerinnen und Bürgern sowie Unternehmen zuständig.[30] Trotz dieser umfassenden Zuständigkeit, die strategische und koordinierende Aufgaben der Digitalisierung über sämtliche Wirtschaftssektoren hinweg sowie die Bereitstellung wesentlicher IT–Dienste beinhaltete, sah das NISG eine Einbindung des Digitalisierungsministeriums in die Gremien der operativen Koordination der Cyber–Sicherheit nicht vor.

[30] Abschnitt F Z 26 der Anlage zu § 2 Bundesministeriengesetz; zu diesen Angelegenheiten gehören „insbesondere auch“:

- allgemeine Digitalisierungsstrategie;
- Angelegenheiten des E–Governments;
- Koordination und zusammenfassende Behandlung in Angelegenheiten der Informationstechnologien;
- allgemeine Angelegenheiten einschließlich der Koordination, der Planung und des Einsatzes der automationsunterstützten Datenverarbeitung sowie der Beurteilung von Anwendungen der automationsunterstützten Datenverarbeitung unter Gesichtspunkten der Wirtschaftlichkeit, Zweckmäßigkeit und Sparsamkeit und des ressortübergreifenden Wirkungscontrollings sowie der Verwaltungsreform und des Datenschutzes;
- Koordination in Angelegenheiten der elektronischen Informationsübermittlung;
- Bereitstellung eines ressortübergreifenden elektronischen Bürgerinformationssystems;
- Bereitstellung des Rechtsinformationssystems und des E–Rechts;
- Angelegenheiten der Bundesrechenzentrum Gesellschaft mit beschränkter Haftung.

13.2 Der RH beurteilte den IKDOK als wichtigstes interministerielles Gremium für die Cyber–Sicherheit. Der IKDOK erfüllte die im NISG festgelegten Aufgaben.

Der RH stellte fest, dass die vom NISG vorgesehene OpKoord keine gegenüber dem IKDOK eigenständige Tätigkeit entfaltete, sondern ihre Tätigkeit im Wesentlichen lediglich darin bestand, IKDOK–Ergebnisse für ihren Adressatenkreis geringfügig zu modifizieren (TZ 15).

Der RH stellte weiters fest, dass das Digitalisierungsministerium trotz der Zuständigkeit für wesentliche Aufgaben auf dem Gebiet der IT nicht in die Koordination der Cyber–Sicherheit eingebunden war. Nach Ansicht des RH war Cyber–Sicherheit als wesentlicher Aspekt bei Fragen der Digitalisierung zu berücksichtigen. Aufgrund dieses engen Zusammenhangs erachtete er die Frage der Einbindung des Digitalisierungsministeriums in die operative Koordination der Cyber–Sicherheit für bedeutend. Da der IKDOK in erster Linie die operative Aufgabe wahrnahm, das Cyber–Lagebild zu erstellen, und hierbei dem Digitalisierungsministerium keine Aufgabe zukommen konnte, kam nach Ansicht des RH nur eine Einbindung in die OpKoord infrage.

Der RH empfahl den überprüften Bundesministerien, die Aufgaben der OpKoord zu evaluieren und das Digitalisierungsministerium sowie die Länder auf geeignete Weise zu integrieren. Hierbei wäre auch festzulegen, ob die OpKoord regelmäßig oder nur im Bedarfsfall einzuberufen wäre.

13.3 (1) Das Bundeskanzleramt wies in seiner Stellungnahme auf die Zuständigkeit des Innenministeriums zur Umsetzung der Empfehlung hin.

(2) Zur Möglichkeit der Kooperation und des Informationsaustausches im Rahmen der OpKoord verwies das Innenministerium in seiner Stellungnahme auf den für das erste Quartal 2022 geplanten Termin mit den zuständigen Vertretern (siehe TZ 4) der öffentlichen Verwaltung (Bund und Länder). Aus diesem Termin resultierende Ergebnisse sollten in die Evaluierung der OpKoord miteinfließen. Weiters sei geplant, das Thema des OpKoord–Formats als einen Hauptpunkt der – im ersten Quartal 2022 geplanten – IKDOK–Klausur zu behandeln.

Das Digitalisierungsministerium nehme als aktives Mitglied der Steuerungsgruppe–CSS an den seit Beginn 2021 regelmäßig stattfindenden Sitzungen dieses Gremiums teil, in welchen regelmäßig auch das aktuelle IKDOK–Lagebild präsentiert werde; hierdurch sei ein Informationsfluss zwischen IKDOK und Digitalisierungsministerium bereits sichergestellt. Dennoch sei eine erweiterte Einbeziehung des Digitalisierungsministeriums und insbesondere der Länder in die OpKoord notwendig. Die Österreichische Strategie für Cybersicherheit 2021 sehe bereits die Möglichkeit vor, die OpKoord um Vertreterinnen und Vertreter von Einrichtungen der öffentlichen Verwaltung zu erweitern. Ab 2022 könne, beispielsweise im Rahmen der IKDOK–

Klausur bzw. des geplanten Termins, mit Vertretern der öffentlichen Verwaltung an einem Format gearbeitet werden, in welchem das Digitalisierungsministerium und die Länder eingebunden würden.

(3) Das Verteidigungsministerium bekundete in seiner Stellungnahme seine Unterstützung bei der Evaluierung der OpKoord und hinsichtlich der regelmäßigen Einbindung des Digitalisierungsministeriums sowie der Länder in die OpKoord.

13.4 Der RH anerkannte, dass ein Informationsfluss zum Digitalisierungsministerium betreffend die Cyber–Lage mittlerweile bestand und dass weitere Überlegungen sowie erste vorbereitende Schritte zur Einbindung desselben wie auch insbesondere der Länder in die OpKoord stattfanden. Er wies jedoch nochmals auf seine Empfehlung hin, die Aufgaben der OpKoord zu evaluieren und in diesem Zusammenhang die Frequenz der Einberufung dieses Gremiums festzulegen.

Arbeitsweise der Koordinierungsgremien

14.1 (1) Die Vertreter der im IKDOK repräsentierten Organisationseinheiten hielten regelmäßige Sitzungen ab. Anfangs – der IKDOK wurde 2015 gegründet – fanden diese unregelmäßig, ab 2018 monatlich statt; zusätzlich wurden ab Februar 2019 wöchentliche Besprechungen in Form von Videokonferenzen zum Status–Update und zur Informationsverdichtung abgehalten. Darüber hinaus konnte jede der im IKDOK repräsentierten Organisationseinheiten die Einberufung des IKDOK verlangen, etwa bei Verdacht, dass eine Cyber–Krise vorliege.

Anlässlich der Cyber–Krise im Außenministerium ab Jänner 2020 bis zu deren Ende im März 2020 hielt der IKDOK laufend Sitzungen in einem provisorischen Cyber–Krisen– und Lagezentrum vor Ort im Außenministerium ab.

Die monatlichen Sitzungen des IKDOK fanden in gelegentlich wechselnden Besprechungsräumen statt, die einzelne am IKDOK teilnehmende Organisationseinheiten zur Verfügung stellten. Ein fixer Besprechungsort stand dem IKDOK nicht zur Verfügung.

(2) Zentrales Arbeitsergebnis der monatlichen Sitzungen des IKDOK war ein unter den Teilnehmenden abgestimmtes und dokumentiertes, österreichweites Cyber–Lagebild (TZ 15). Insbesondere in den Jahren 2018 und 2019 waren zusätzliche Sitzungsprotokolle und in manchen Fällen auch „To–do–Listen“ erstellt worden. Ab dem Jahr 2020 fehlten diese, weil nach Auskunft des Innenministeriums die Ressourcen dafür aufgrund der gestiegenen sonstigen Aufgaben im Rahmen des IKDOK nicht mehr verfügbar waren. Eine Planstelle in der Abteilung Cybersicherheit mit der

Wertigkeit A2/5 bzw. v2/4, deren Verwendung u.a. für die Besorgung von IKDOK–Backoffice–Aufgaben vorgesehen war, war bis zur Zeit der Gebarungsüberprüfung unbesetzt. In Abstimmung mit den Teilnehmenden des IKDOK wurde beschlossen, dass Erfassung und Nachverfolgung von Aufgaben jeweils in den spezifischen Teilnehmerorganisationen selbst erfolgten und es bis auf Weiteres keine zentrale Bearbeitung gab.

Über die wöchentlichen Videokonferenzen (ab 2019) lagen Protokolle vor. Gegenstand dieser Besprechungen waren die gegenseitige Information über aktuelle Cyber–Vorfälle, Neuerungen zu strategischen Themen betreffend Cyber–Sicherheit sowie Terminankündigungen und –koordinierungen. Zu etlichen Themen wurden auch aus der Diskussion abgeleitete Handlungserfordernisse oder sonstige weitere Vorgehensweisen festgehalten.

(3) Laut NISG (§ 7 Abs. 3) konnte der Bundesminister für Inneres in einer Geschäftsordnung nähere Regelungen zum Zusammenwirken der Koordinierungsstrukturen, insbesondere über die Einberufung von Sitzungen, die Zusammensetzung sowie deren Entscheidungsfindung treffen. Nach Auskunft des Innenministeriums hätten erste Arbeiten dazu zwar schon stattgefunden, diese seien allerdings nicht weiterverfolgt worden; dies einerseits aufgrund vorrangiger sonstiger Aufgaben, andererseits weil es derzeit keinen unmittelbaren Bedarf an einer Geschäftsordnung gebe. Dies sei insbesondere dem Umstand geschuldet, dass der an IKDOK mitwirkende Personenkreis gut eingespielt sei und großes gegenseitiges Vertrauen bestehe.

(4) Weiters konnte der Bundesminister für Inneres laut NISG (§ 12 Abs. 1) für die Organisation und Aufgabenwahrnehmung des IKDOK eine IKT–Lösung („IKDOK–Plattform“) betreiben, die für diesen Fall den anderen beteiligten Bundesministerinnen und Bundesministern bereitzustellen wäre.

Nach Auskunft des Innenministeriums sollte die IKDOK–Plattform insbesondere dazu dienen, das gemeinsame Cyber–Lagebild IKT–unterstützt zu erstellen (TZ 15), aber auch dazu, die Einrichtung und Abwicklung von Arbeitskreisen im IKDOK zu erleichtern.

Im Mai 2021 war diese IKT–Lösung noch nicht eingerichtet. Das Innenministerium teilte mit, dass eine IKDOK–Plattform zur Zeit der Gebarungsüberprüfung aufgebaut werde. Die technische Betriebsführung werde in einem IT–System des Innenministeriums im Referat IKT der Abteilung Cybersicherheit erfolgen, während die fachliche Betriebsführung der operativen NIS–Behörde obliege. Die Hard– und Softwarebeschaffung sei abgeschlossen; die Rekrutierung einer geeigneten Person für die technische Betriebsführung, ohne die eine Inbetriebnahme der Plattform nicht möglich sei, sei jedoch noch im Gange. Ein genauer Zeitpunkt zur Fertigstellung und Inbe-

triebnahme sei vom Ergebnis der Ausschreibung abhängig und könne daher noch nicht abgeschätzt werden.

14.2 (1) Der RH hielt die zur Zeit der Gebarungsüberprüfung praktizierte Frequenz der monatlich (in Präsenz) und wöchentlich (per Videokonferenz) stattfindenden IKDOK–Sitzungen für angemessen und zweckmäßig. Für die in Präsenz stattfindenden Besprechungen bestand jedoch keine fixe Räumlichkeit, sondern die teilnehmenden Organisationseinheiten mussten Räume zur Verfügung stellen. Im Hinblick auf das vom IKDOK regelmäßig zu erstellende Cyber–Lagebild, das von zentraler Bedeutung für die Cyber–Sicherheit war, insbesondere aber im Hinblick darauf, dass ein Zentrum für die Bearbeitung von Cyber–Vorfällen (wie die Cyber–Krise im Außenministerium) unmittelbar verfügbar sein sollte, erachtete der RH ein eigenes, dauerhaft eingerichtetes und jederzeit benutzbares Cyber–Lagezentrum für den IKDOK (und die OpKoord) für zweckmäßig.

Der RH empfahl daher dem Innenministerium, ein Cyber–Lagezentrum mit der für die Zwecke der Erfüllung der Aufgaben erforderlichen Infrastruktur unter Beachtung von Kosten–Nutzen–Aspekten einzurichten und dem IKDOK (und der OpKoord) zur Verfügung zu stellen. Dieses sollte aufgrund der dem Bundesminister für Inneres zukommenden Leitungsaufgaben im IKDOK (und der OpKoord) beim Innenministerium eingerichtet werden.

(2) Der RH stellte weiters fest, dass Protokolle und To–do–Listen über die monatlichen IKDOK–Sitzungen ab 2020 aus Kapazitätsgründen in der Abteilung Cybersicherheit nicht mehr erstellt werden konnten. Dies war auf eine bis zur Zeit der Gebarungsüberprüfung unbesetzt gebliebene Planstelle für den IKDOK–Backoffice–Bereich zurückzuführen. Das Cyber–Lagebild als wesentlichster Output der Sitzungen war dokumentiert vorhanden. Die zentrale Dokumentation weiterer Sitzungsinhalte, insbesondere Handlungserfordernisse („To–dos“) teilnehmender Organisationseinheiten sowie die Nachverfolgung ihrer Erfüllung, unterblieb dadurch; die Dokumentation sollte ab 2020 stattdessen dezentral in den Teilnehmerorganisationen erfolgen. Der RH erachtete es jedoch für bedeutsam, Handlungserfordernisse zur Erhaltung oder Erhöhung der Cyber–Sicherheit zentral schriftlich festzuhalten und ihre Umsetzung nachzuverfolgen und zu dokumentieren.

Der RH empfahl daher dem Innenministerium, die Funktionalität der Geschäftsstelle des IKDOK und der OpKoord für die Protokollerstellung sicherzustellen.

(3) Der RH stellte fest, dass der Bundesminister für Inneres keine Geschäftsordnung für das Zusammenwirken der Koordinierungsstrukturen IKDOK und OpKoord erlassen hatte. Die zur Zeit der Gebarungsüberprüfung gegebene Zusammenarbeit basierte auf dem Expertenwissen und dem gegenseitigen Vertrauen der handelnden Personen. Der RH gab allerdings zu bedenken, dass vor allem in Krisen die Funk-

tionsfähigkeit des IKDOK unabhängig von dem dann verfügbaren Personenkreis gegeben sein muss. Es war daher geboten, die Zusammenarbeit im IKDOK, der für die Cyber–Sicherheit der Daseinsvorsorge und die Erfüllung staatlicher Aufgaben von zentraler Bedeutung ist, dauerhaften und von den jeweils handelnden Personen unabhängigen Regelungen zu unterwerfen.

Der RH empfahl dem Innenministerium, eine Geschäftsordnung für das Zusammenwirken der Koordinierungsstrukturen gemäß der gesetzlichen Ermächtigung in § 7 Abs. 3 NISG aufgrund der hohen Bedeutung dieser Strukturen für die Cyber–Sicherheit in Österreich zu erlassen. In dieser sollte jedenfalls auch der Prozess zur Erstellung des Lagebildes festgelegt werden (siehe dazu auch TZ 15).

(4) Der RH stellte fest, dass sich die vom NISG optional vorgesehene IKT–Lösung „IKDOK–Plattform“ im Innenministerium zur Zeit der Gebarungsüberprüfung im Aufbau befand. Er hielt den Aufbau dieser IKT–Lösung im Sinne einer Vereinfachung und Modernisierung der Zusammenarbeit im Rahmen des IKDOK für notwendig und anerkannte die bisherigen Vorbereitungsarbeiten des Innenministeriums. Er betonte die Bedeutung einer möglichst zeitnahen Inbetriebnahme und verwies dazu auch auf seine Empfehlung in TZ 15 zur Nutzung dieser IKT–Lösung für die effiziente Erstellung des Cyber–Lagebildes.

14.3 Das Innenministerium hielt in seiner Stellungnahme fest, dass ein Cyber–Lagezentrum integraler Bestandteil eines aktuellen Projekts zur Novellierung des NISG und zu Vorbereitungen auf die Weiterentwicklung der NIS–Richtlinie sei.

Betreffend die Empfehlung, die Funktionalität der Geschäftsstelle von IKDOK und OpKoord sicherzustellen, würden die noch offenen Interessentensuchen für die offenen Arbeitsplätze in der seit 1. Dezember 2021 eingerichteten Abteilung Netz– und Informationssystemsicherheit ehestmöglich erfolgen. Die Abteilungsleitung sei bereits ausgeschrieben.

Weiters werde die Geschäftsordnung (basierend auf der geltenden Rechtslage) in Abhängigkeit von den Ergebnissen der für das erste Quartal 2022 geplanten IKDOK–Klausur erstellt.

14.4 Der RH anerkannte, dass ein Cyber–Lagezentrum bereits Gegenstand geplanter Projekte war, wies jedoch nochmals nachdrücklich auf die Bedeutung der tatsächlichen Einrichtung eines Cyber–Lagezentrums hin. Diese wichtige infrastrukturelle Maßnahme sollte – unabhängig von einer Novellierung des NISG und von der Weiterentwicklung der NIS–Richtlinie – möglichst rasch eingerichtet werden; dies angesichts der Tatsache, dass jederzeit mit Cyber–Vorfällen zu rechnen ist, die mit größtmöglicher Effizienz zu bekämpfen sein werden.

Cyber–Lagebild

15.1 (1) Das Ergebnis der monatlichen Sitzungen des IKDOK bestand im Wesentlichen aus dem unter den Teilnehmenden abgestimmten und dokumentierten Cyber–Lagebild. Seit 2018 wurde dieses in neu strukturierter Form erstellt: Es war in die Teilbereiche Cyber–Sicherheit, Cybercrime, internationale Lage und militärische Lage untergliedert. Die Beiträge lieferten Teilnehmende entsprechend den ihnen zur Verfügung stehenden Informationsquellen. Inhalte des Lagebildes waren in erster Linie kurze Berichte über aktuelle Sicherheitsthemen und –vorfälle, aber auch über aktuelle politische und strategische Entwicklungen auf den Gebieten Cyber–Sicherheit, Cybercrime, Cyber–Defence und Cyber–Diplomatie.

(2) Das Cyber–Lagebild wurde in einem gleichbleibend ablaufenden und von den Teilnehmenden akzeptierten Prozess erstellt; dieser Prozess war jedoch nicht ausdrücklich schriftlich festgelegt: Im Vorfeld einer IKDOK–Sitzung wurden die einzelnen Organisationseinheiten aufgefordert, ihre inhaltlichen Beiträge zum Lagebild spätestens zwei Tage vor der anberaumten Sitzung an das Referat Netz– und Informationssicherheit der Abteilung Cybersicherheit mittels „gesicherter E–Mails“ zu übermitteln. Dieses Referat leitete die Beiträge an das Referat Cyber Security Center weiter, welches die Agenda sowie eine allfällige To–do–Liste für die nächste IKDOK–Sitzung an die Teilnehmenden versandte. Die Beiträge wurden im Rahmen der IKDOK–Sitzung zu einem finalen Cyber–Lagebild (IKDOK–Lagebild) verarbeitet, das – falls erforderlich – üblicherweise unmittelbar anschließend in einer weiteren Version erstellt wurde, in der keine klassifizierten Informationen enthalten waren (OpKoord–Lagebild).

(3) Die Implementierung einer gesicherten Kommunikation im Rahmen der zur Zeit der Gebarungsüberprüfung im Aufbau befindlichen IKDOK–Plattform (TZ 14) war noch nicht umgesetzt. Nach Fertigstellung dieser IKDOK–Plattform wird der Austausch von klassifizierten Informationen bis zur Stufe „eingeschränkt“ ermöglicht, was – laut Innenministerium – für die Arbeiten im IKDOK erfahrungsgemäß ausreichend sei. Darüber hinaus bestand mit dem Heeresnachrichtenamt und dem Abwehramt bereits zur Zeit der Gebarungsüberprüfung die Möglichkeit zum Austausch von Informationen bis zur Klassifikationsstufe „geheim“[31].

(4) Das Referat Netz– und Informationssicherheit übermittelte die beiden finalisierten Lagebilder an den jeweiligen Adressatenkreis: das IKDOK–Lagebild an die Chief Information Security Officers (CISO) der verfassungsmäßigen Einrichtun-

[31] Klassifizierte Informationen im Sinne der Informationssicherheitsverordnung (InfoSiV) können in die Klassifikationsstufen „eingeschränkt“, „vertraulich“, „geheim“ und „streng geheim“ eingeteilt werden (§ 3 Abs. 1 InfoSiV).

gen[32] des Bundes, nicht jedoch an jene der Länder; das OpKoord–Lagebild an die Chief Information Security Officers der Einrichtungen und Unternehmen, die zu den kritischen Infrastrukturen[33] gehören, sowie an die Kontaktstellen der Betreiber wesentlicher Dienste.

15.2 (1) Der RH hielt fest, dass der Prozess zur Erstellung des Lagebildes zwar erprobt und den daran Beteiligten geläufig, jedoch nicht schriftlich festgelegt war. Er gab zu bedenken, dass der beteiligte Personenkreis Veränderungen unterworfen sein könnte, wodurch die Akzeptanz des Prozesses nicht mehr gegeben sein und somit ein reibungsloser Ablauf der Lagebilderstellung erschwert werden könnte. Zur schriftlichen Festlegung des Prozesses erachtete der RH eine Geschäftsordnung für den IKDOK und die OpKoord als geeignet; diese war allerdings bis zur Gebarungsüberprüfung nicht erlassen worden.

Der RH verwies daher auf seine Empfehlung an das Innenministerium in TZ 14, eine Geschäftsordnung für das Zusammenwirken der Koordinierungsstrukturen zu erlassen und in dieser den Prozess zur Erstellung des Lagebildes festzulegen.

(2) Der RH stellte weiters fest, dass zur Vorbereitung der Erstellung des Lagebildes die eingebundenen Stellen ihre Beiträge mittels gesicherter E–Mails bei der organisatorisch federführenden Abteilung im Innenministerium einmeldeten, der die weitere Bearbeitung und nochmalige Versendung als Vorbereitung auf die IKDOK–Sitzung oblagen. Der RH erachtete diese Vorgehensweise für kompliziert und auch für wenig effizient, weil die Teilnehmenden parallel gleiche Risiken meldeten bzw. melden konnten. Der RH sah in der im Aufbau befindlichen IKT–Lösung „IKDOK–Plattform“ eine Möglichkeit, die Erstellung des Lagebildes, z.B. durch gleichzeitigen Zugriff der eingebundenen Stellen, rascher, effizienter und sicherer zu gestalten.

Der RH stellte kritisch fest, dass der Informationsaustausch der Teilnehmenden im IKDOK nur mittels „gesicherter E–Mails“ erfolgte. Er verwies dazu darauf, dass die IKT–Lösung „IKDOK–Plattform“, die den Austausch von klassifizierten Informationen bis zur Stufe „eingeschränkt“ ermöglichen wird, noch nicht fertiggestellt war.

Er empfahl daher dem Innenministerium, die im Aufbau befindliche „IKDOK–Plattform“ (TZ 14) fertigzustellen, zur Lagebilderstellung einzusetzen und auch für eine gesicherte Kommunikation technisch auszugestalten.

[32] Verfassungsmäßige Einrichtungen sind beispielsweise Bundespräsident, Bundesregierung, Nationalrat, Landesregierung, Landeshauptmann, Bundesheer.

[33] Kritische Infrastrukturen sind gemäß § 22 Abs. 1 Z 6 Sicherheitspolizeigesetz Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher IKT, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben.

(3) Der RH stellte fest, dass das Cyber–Lagebild (in Form des IKDOK–Lagebildes) zwar an die verfassungsmäßigen Einrichtungen des Bundes übermittelt wurde, nicht jedoch an verfassungsmäßige Einrichtungen der Länder. Er kritisierte, dass damit wesentliche Teile der öffentlichen Verwaltung in Österreich keine Information über die jeweils aktuelle Situation der Cyber–Sicherheit in der für öffentliche Einrichtungen vorgesehenen Form erhielten. Die fehlende Information der jeweils aktuellen Bedrohungslage brachte das Risiko mit sich, dass die Länder über die allfällige Notwendigkeit, ihre Cyber–Sicherheitsmaßnahmen zu optimieren, nicht regelmäßig informiert waren.

Der RH empfahl daher dem Innenministerium, zu prüfen, ob das jeweils aktuelle Cyber–Lagebild (in Form des OpKoord–Lagebildes) auch den verfassungsmäßigen Einrichtungen der Länder zur Kenntnis gebracht werden kann.

15.3 Das Innenministerium gab in seiner Stellungnahme an, dass die Empfehlung zum Aufbau der IKDOK–Plattform nach Interessentensuche und Besetzung der Arbeitsplätze im Referat IV/10/c (NIS technische Einrichtungen) umgesetzt werde.

Das OpKoord–Lagebild werde seit dem dritten Quartal 2021 den Ämtern der Landesregierungen übermittelt, womit die Empfehlung bereits umgesetzt sei.

Resümee der Koordinierungsgremien

16.1 Der IKDOK setzte sich unter Leitung des Innenministeriums aus den Vertreterinnen und Vertretern des Bundeskanzleramts, des Verteidigungsministeriums und des Außenministeriums zusammen. Er war als wichtigstes interministerielles Gremium der Cyber–Sicherheit für die Lagebilderstellung und –erörterung sowie im Cyber–Krisenfall zuständig.

Aufgrund von Personenidentitäten der im IKDOK bzw. der OpKoord vertretenen Computer–Notfallteams fanden keine eigenen OpKoord–Sitzungen statt.

16.2 Der RH erachtete die Koordinationsstruktur des IKDOK für geeignet, die ihm durch das NISG übertragenen Aufgaben zu erfüllen, insbesondere die regelmäßige oder anlassbezogene Erstellung des Cyber–Lagebildes. Hinsichtlich einer Optimierung des IKDOK verwies der RH allerdings auf seine Empfehlungen zur erweiterten Dokumentation (TZ 14), zur Ausarbeitung einer Geschäftsordnung (TZ 14), die auch den Prozess der Lagebilderstellung beschreibt, zur Sicherstellung einer geeigneten Infrastruktur für die Aufgabenwahrnehmung (Cyber–Lagezentrum) (TZ 14) und zur Umsetzung der IKT–Lösung „IKDOK–Plattform“ für eine effizientere Generierung des Lagebildes und eine gesicherte Kommunikation (TZ 15).

Vor dem Hintergrund, dass das vom NISG vorgesehene Gremium OpKoord bis zur Zeit der Gebarungsüberprüfung gegenüber dem IKDOK keine eigenständige Tätigkeit entfaltete, verwies der RH auf seine Empfehlung in TZ 13, die Aufgaben der OpKoord zu evaluieren und das Digitalisierungsministerium sowie die Länder auf geeignete Weise zu integrieren. Hierbei wäre auch zu prüfen, ob die OpKoord regelmäßig oder nur im Bedarfsfall einzuberufen wäre.

Operative Cyber–Sicherheit

Zentrale Anlaufstelle

17.1 (1) Gemäß NISG (§ 6 Abs. 1) war eine zentrale Anlaufstelle beim Bundesminister für Inneres – als operative Verbindungsstelle – zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zuständigen Stellen in den anderen EU–Mitgliedstaaten sowie der EU–Kooperationsgruppe[34] und dem CSIRTs–Netzwerk[35] zu schaffen. Dafür richtete das Innenministerium die zentrale Anlaufstelle für Netz– und Informationssysteme (Single Point of Contact – SPOC) im Referat Netz– und Informationssicherheit bei der NIS–Meldestelle der Abteilung Cybersicherheit ein. Sie nahm mit der Notifikation an die Europäische Kommission 2019 ihre Tätigkeit auf, die Kommunikation erfolgte über eine eigene E–Mail–Adresse.

Diese zentrale Anlaufstelle sollte gemäß § 6 Abs. 2 NISG

- eingehende Meldungen und Anfragen unmittelbar an die Mitglieder des IKDOK und an Computer–Notfallteams weiterleiten, soweit dies zur Erfüllung einer gesetzlich übertragenen Aufgabe des jeweiligen Mitglieds erforderlich ist, und
- über Aufforderung die zentralen Anlaufstellen in anderen EU–Mitgliedstaaten unterrichten, wenn ein Sicherheitsvorfall einen oder mehrere andere EU–Mitgliedstaaten betrifft.[36]

[34] Die EU–Kooperationsgruppe ist ein gemäß Art. 11 NIS–Richtlinie eingerichtetes Gremium, das sich aus Vertreterinnen und Vertretern der EU–Mitgliedstaaten, der Europäischen Kommission und der Europäischen Agentur für Netz– und Informationssicherheit (**ENISA**) zusammensetzt und der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den EU–Mitgliedstaaten zum Aufbau von Vertrauen und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen in der EU dient (§ 3 Z 20 NISG).

[35] CSIRT = Computer Security Incident Response Team.
Das CSIRTs–Netzwerk ist ein gemäß Art. 12 NIS–Richtlinie eingerichtetes Gremium, das sich aus Vertreterinnen und Vertretern der Computer–Notfallteams der EU–Mitgliedstaaten und des europäischen Computer–Notfallteams zusammensetzt und zum Aufbau von Vertrauen zwischen den EU–Mitgliedstaaten beitragen sowie eine rasche und wirksame operative Zusammenarbeit fördern soll (§ 3 Z 21 NISG).

[36] Siehe dazu §§ 19 Abs. 5, 21 Abs. 3 und 22 Abs. 4 NISG: Wenn ein Sicherheitsvorfall bei einem Betreiber wesentlicher Dienste, einem Anbieter digitaler Dienste oder einer Einrichtung der öffentlichen Verwaltung einen oder mehrere andere EU–Mitgliedstaaten betrifft, hat der Bundesminister für Inneres oder das zuständige Computer–Notfallteam im Wege der zentralen Anlaufstelle (SPOC) die zentrale Anlaufstelle in diesen Mitgliedstaaten darüber zu unterrichten.

Gemäß den Gesetzesmaterialien ersetzt die zentrale Anlaufstelle (SPOC) nicht die Kommunikation des Bundeskanzlers im Rahmen seiner Aufgaben oder die direkte Kommunikation der Computer–Notfallteams im Rahmen des CSIRTs–Netzwerks. Sie stellt vielmehr sicher, dass es immer einen Kommunikationsweg zwischen den Koordinierungsstrukturen in Österreich und anderen EU–Mitgliedstaaten gibt.[37]

(2) Nach Auskunft des Innenministeriums fand nur ein sehr geringer Teil des Austausches wichtiger Informationen zur Cyber–Sicherheitslage zwischen Österreich und anderen EU–Mitgliedstaaten über diese zentrale Anlaufstelle (SPOC) statt. Tatsächlich enthielt nur ein kleiner Teil der im Zeitraum 2019 und 2020 ausgetauschten Informationen Meldungen über Sicherheitsvorfälle. Der größere Teil umfasste Organisatorisches, Personalia, Newsletter und Ähnliches. Die Anzahl der über die E–Mail–Adresse der zentralen Anlaufstelle (SPOC) ein– und ausgehenden Meldungen und Anfragen stellte sich wie folgt dar:

Tabelle 6: Zentrale Anlaufstelle (SPOC) für den europäischen Informationsaustausch

Anzahl der Meldungen und Anfragen	2019	2020
eingehend	8	22
ausgehend	13	21
gesamt	**21**	**43**

Quelle: BMI

Der Großteil der Meldungen über Sicherheitsvorfälle mit grenzüberschreitender Bedeutung ging nicht über die zentrale Anlaufstelle, sondern über andere Informationskanäle ein (TZ 21).

(3) Nach Mitteilung des Innenministeriums war die Rolle der zentralen Anlaufstelle (SPOC) auf operativer Ebene im Rahmen der EU–Kooperation noch nicht zur Gänze geklärt, wodurch die internationale Kommunikation über diese Einrichtungen nicht entsprechend etabliert war. Dies wurde auch 2019 bei einer Cyber–Übung zur Weiterentwicklung des Cyber–Krisenmanagementsystems in der EU festgestellt. In der Folge befand sich zur Zeit der Gebarungsüberprüfung ein neues europaweites Netzwerk (CyCLONe: Cyber Crises Liaison Organisation Network) im Aufbau, welches die Einführung und Sicherstellung einer effizienten Vorgehensweise bei großflächigen Cyber–Sicherheitsvorfällen und –krisen innerhalb der EU zum Ziel hat. Auch eine Integration der zentralen Anlaufstellen der EU–Mitgliedstaaten in dieses Netzwerk wurde diskutiert und wäre nach Ansicht des Innenministeriums, das an den Arbeiten für das Netzwerk teilnahm, sinnvoll. Das EU–weite Netzwerk (CyCLONe) soll darüber hinaus die politische mit der technischen Ebene operativ verknüpfen,

[37] ErlRV 369 BlgNR XXVI. GP, S. 8

wobei die politische Ebene durch den Krisenreaktionsmechanismus der EU (IPCR: Integrated Political Crisis Response) und die technische Ebene durch das CSIRTs–Netzwerk repräsentiert wird. Nach den Plänen der Europäischen Kommission soll dieses Netzwerk (CyCLONe) zukünftig im Rahmen der Überarbeitung der NIS–Richtlinie rechtlich verankert werden.

(4) Auch die Aufgaben der zentralen Anlaufstelle (SPOC) als operative Verbindungsstelle zur EU–Kooperationsgruppe und zum CSIRTs–Netzwerk waren weitgehend ungeklärt. Die Beziehungen zu diesen internationalen Einrichtungen nahmen in erster Linie andere inländische Stellen wahr. So vertrat grundsätzlich und vorwiegend das Bundeskanzleramt Österreich in der EU–Kooperationsgruppe; am CSIRTs–Netzwerk nahmen die drei Computer–Notfallteams GovCERT, Austrian Energy CERT sowie das nationale CERT.at teil, nicht jedoch die zentrale Anlaufstelle (SPOC).

(5) Art. 10 der NIS–Richtlinie sah eine jährliche Berichtspflicht der zentralen Anlaufstellen der EU–Mitgliedstaaten an die EU–Kooperationsgruppe über die eingegangenen Meldungen vor. Die österreichische zentrale Anlaufstelle (SPOC) im Innenministerium war dieser Verpflichtung nachgekommen und hatte der EU–Kooperationsgruppe die Berichte für die Jahre 2019 und 2020 vorgelegt.

17.2 Der RH betonte, dass gemäß NISG – in Umsetzung unionsrechtlicher Vorschriften – die zentrale Anlaufstelle (SPOC) im Innenministerium eingerichtet und in Betrieb war und damit ein Kommunikationsweg zwischen den EU–Mitgliedstaaten und den Koordinierungsstrukturen in Österreich zu jeder Zeit sichergestellt war. Der RH stellte allerdings fest, dass der zentralen Anlaufstelle (SPOC) trotz unionsrechtlicher Verankerung bislang aufgrund des Bestehens anderer, paralleler und durch die bisherige Praxis besser etablierter Meldewege zwischen den EU–Mitgliedstaaten nur geringe Bedeutung zukam. Der RH hielt daher den Aufbau des neuen europaweiten Netzwerks CyCLONe und Überlegungen, die zentralen Anlaufstellen in dieses einzubinden, für sinnvoll.

Er empfahl dem Innenministerium, als Vertreter Österreichs beim Aufbau dieses neuen EU–weiten Netzwerks CyCLONe mitzuwirken.

17.3 Das Innenministerium merkte in seiner Stellungnahme an, dass die Empfehlung bereits umgesetzt werde.

Computer–Notfallteams

18 (1) Zur Gewährleistung der Sicherheit von Netz– und Informationssystemen sah das NISG die Einrichtung eines nationalen Computer–Notfallteams (Computer Emergency Response Team (CERT[38,39])) und eines Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) vor. Darüber hinaus konnten auch sektorspezifische Computer–Notfallteams eingerichtet werden (§ 14 Abs. 1 NISG).

Die Hauptaufgaben dieser Computer–Notfallteams waren gemäß § 14 Abs. 2 NISG:

- Entgegennahme von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle und Weiterleitung dieser Meldungen an den Bundesminister für Inneres (TZ 21),
- Beobachtung und Analyse von Risiken, Vorfällen oder Sicherheitsvorfällen, Ausgabe bzw. Verbreitung diesbezüglicher Informationen, von Frühwarnungen, Alarmmeldungen und Handlungsempfehlungen sowie Lagebeurteilung,
- erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall. Dies waren „konkrete Handlungsanweisungen und Informationen, um den aktuellen Sicherheitsvorfall abzuwehren“, nicht jedoch die Wiederherstellung des betroffenen Systems. Eine Unterstützung vor Ort sollte daher nur in Ausnahmefällen erbracht werden.[40]

Diese Computer–Notfallteams unterlagen bestimmten gesetzlichen Anforderungen (§ 15 Abs. 1 NISG), insbesondere hinsichtlich der von ihnen genutzten technischen und räumlichen Infrastruktur, ihrer Betriebskontinuität und der Sicherheit ihrer Kommunikationskanäle. Das dort beschäftigte Personal hatte außerdem sicherheitsüberprüft zu sein. Bezüglich des nationalen Computer–Notfallteams und allfälliger sektorspezifischer Computer–Notfallteams hatte der Bundeskanzler die Erfüllung dieser Anforderungen bescheidmäßig festzustellen.

38 Oft wird dafür auch der Begriff Computer Security Incident Response Team (CSIRT) verwendet.

39 Der Begriff CERT (Computer Emergency Response Team) ist seit 1997 eine eingetragene Marke der Carnegie Mellon University. Unternehmen können eine Genehmigung zur Verwendung der CERT–Marke beantragen. Das nationale Computer–Notfallteam (CERT.at) wird von CERT–CC der Carnegie Mellon University als legitimes Computer Emergency Response Team anerkannt und darf daher den Markennamen CERT nutzen.

40 vgl. dazu *Heußler* in Anderl/Heußler/Mayer/Müller, NISG § 14 Rz 5 (2019)

(2) Computer–Notfallteams ließen sich daher hinsichtlich ihres Wirkungsbereichs wie folgt untergliedern:

- nationales Computer–Notfallteam (CERT.at):

  Das nationale Computer–Notfallteam (CERT.at) stellte eine Drehscheibe für technische Informationen dar. Es gab Warnungen über kritische Schwachstellen und Sicherheitslücken in Software und Computernetzen heraus und unterstützte allgemein bei der Vermeidung von Angriffen; es musste daher auch über keine unternehmensspezifischen Detailkenntnisse verfügen. CERT.at nahm 2008 seinen Betrieb als Computer–Notfallteam auf und ist eine Initiative des Unternehmens A. Im März 2019 stellte der Bundeskanzler per Bescheid die Eignung des Unternehmens A zur Wahrnehmung der Aufgaben des nationalen Computer–Notfallteams gemäß NISG fest.

- sektorspezifische Computer–Notfallteams (GovCERT; Austrian Energy CERT):

  Die Zielgruppe eines sektorspezifischen Computer–Notfallteams umfasst grundsätzlich sämtliche Unternehmen bzw. Organisationen eines Sektors. Diese Computer–Notfallteams verfügen über sektorspezifisches Wissen verbunden mit Expertenwissen im Bereich IT– und Cyber–Sicherheit. Detailkenntnisse der IT–Infrastrukturen der einzelnen Unternehmen bzw. Organisationen des Sektors liegen nicht vor, so dass keine unmittelbaren technischen oder organisatorischen Maßnahmen gesetzt werden können. In Österreich bestanden das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) als (besonderes) sektorspezifisches Computer–Notfallteam (TZ 19) und das Austrian Energy CERT (AEC) als Computer–Notfallteam für den österreichischen Energiesektor; auch diese Computer–Notfallteams wurden durch das Unternehmen A betrieben.

- Unternehmen–Computer–Notfallteam:

  Für Unternehmen und sonstige Organisationen (z.B. auch öffentliche Einrichtungen) bestand die Möglichkeit, ein Computer–Notfallteam für die jeweils eigene IT–Infrastruktur einzurichten. In diesem Fall waren die konkreten Aufgaben, Anforderungen sowie die personelle Ausstattung von der Leitung des Unternehmens bzw. der jeweiligen Organisation festzulegen. Gesetzliche Anforderungen bestanden dazu nicht. Einzelne Computer–Notfallteams konnten sich im Umfang ihrer Aufgaben und damit auch bezüglich ihrer personellen Ausstattung deutlich unterscheiden, z.B. dahingehend, ob eine 24–Stunden–7–Tage–Verfügbarkeit bestand bzw. in welchem Umfang präventive IT–Sicherheitsmaßnahmen oder auch Ausbildungsmaßnahmen angeboten wurden.

- CERT–Verbund Austria:

Im CERT–Verbund Austria erfolgte seit November 2011 etwa sechsmal jährlich ein freiwilliges Treffen von österreichischen Computer–Notfallteams zum Informationsaustausch und Networking. Im Mai 2021 bestand dieser Verbund aus 16 Computer–Notfallteams von Organisationen bzw. Unternehmen. Die Administration des CERT–Verbunds nahm das Bundeskanzleramt bzw. das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) wahr.

Computer–Notfallteam der öffentlichen Verwaltung

19.1 (1) Das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) wird seit 2008 vom Bundeskanzleramt gemeinsam mit dem nationalen Computer–Notfallteam (CERT.at) betrieben. Das NISG (§ 14 Abs. 4) legte ab 2018 auch gesetzlich fest, dass das GovCERT beim Bundeskanzler eingerichtet ist. Die strategische Leitung des GovCERT nahm daher das Bundeskanzleramt wahr. Da laut Angabe des Bundeskanzleramts das erforderliche hochspezialisierte Personal für den Bund unter den vorgegebenen Rahmenbedingungen kaum verfügbar war, schrieb es 2020 die „operativen Unterstützungsleistungen für das GovCERT“ – im Sinne aller dem GovCERT gesetzlich zukommenden Aufgaben – öffentlich aus. Den Zuschlag erhielt das Unternehmen A, das auch bereits das nationale Computer–Notfallteam (CERT.at) betrieb. Daher bestand in diesen beiden Computer–Notfallteams weitgehende Personenidentität. Die Eckpunkte des Vertrags mit dem Unternehmen A stellten sich wie folgt dar:

Tabelle 7: Vertrag GovCERT

Vertragsinhalt	
zentrale Aufgaben	**Anmerkung**
24–Stunden–7–Tage–Hotline und sichere Kommunikationskanäle	durch Personalpool, Rufbereitschaft (außerhalb der Regelarbeitszeiten)
Sammlung, Sichtung, Bewertung von Warnungen, Verteilungen von Frühwarnungen und Alarmmeldungen	–
Unterstützung bei der Reaktion auf einen Sicherheitsvorfall	Umfang: Initiale Triage, Forensik, Beratung, Wiederherstellung, (Remediation), Öffentlichkeitsarbeit Vor–Ort–Unterstützung abhängig von Vorfallspriorität und Einsatzort

Quelle: BKA

(2) Obwohl das NISG die „erste allgemeine Unterstützung bei der Reaktion auf einen Sicherheitsvorfall“ als Aufgabe des GovCERT gegenüber allen Einrichtungen der öffentlichen Verwaltung vorsah (TZ 18), war diese Leistung im abgeschlossenen Vertrag nicht weiter konkretisiert. Dieser sah jedoch eine weitergehende Vor–Ort–Unterstützung exklusiv für das Bundeskanzleramt vor.

(3) Teilnahmeberechtigt an der Informationsdrehscheibe des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) waren Vertreterinnen und Vertreter von IKT–Nutzern aus dem Behördenbereich mit der Domänenzuordnung „gv.at“ (Bundesministerien, Landesverwaltungen, Städte– und Gemeindeverwaltungen) sowie Einrichtungen aus dem Bereich der kritischen Infrastruktur. Im März 2021 nahmen 75 Institutionen, darunter sieben Länder[41] und 21 Städte bzw. Gemeinden, an dieser Informationsdrehscheibe teil.

19.2 (1) Der RH hielt fest, dass das nationale Computer–Notfallteam (CERT.at) und das der öffentlichen Verwaltung (GovCERT) weitgehend personenident waren und die Leistungen von einem externen, privaten Dienstleister erbracht wurden, obwohl Sicherheit eine staatliche Kernaufgabe ist.

Der RH empfahl dem Bundeskanzleramt, die Erbringung der Aufgaben des Computer–Notfallteams der öffentlichen Verwaltung langfristig durch eigene Bedienstete des Bundes in Erwägung zu ziehen.

(2) Der RH wies darauf hin, dass im NISG eine erste allgemeine Unterstützung bei der Reaktion auf einen Sicherheitsvorfall durch das GovCERT gegenüber allen Einrichtungen der öffentlichen Verwaltung gesetzlich vorgesehen war; dies beinhaltete eine Unterstützung vor Ort jedoch nur in Ausnahmefällen. Der RH wies daher kritisch darauf hin, dass die Leistungen im Vertrag mit dem Unternehmen A nicht weiter konkretisiert waren.

Der RH empfahl daher dem Bundeskanzleramt, jene Leistungen, welche das mit der Erbringung der operativen Leistungen des Computer–Notfallteams für die öffentliche Verwaltung (GovCERT) beauftragte Unternehmen im Rahmen der Behandlung eines Sicherheitsvorfalls zu erbringen hat, im Rahmen eines allfälligen nächsten diesbezüglichen Vergabeverfahrens im Sinne des gesetzlichen Auftrags („erste allgemeine Unterstützung“) für alle Dienststellen des Bundes zu definieren.

(3) Der RH hielt fest, dass nicht alle Länder und nur einzelne Städte bzw. Gemeinden an der Informationsdrehscheibe des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) teilnahmen.

[41] Nicht in die Information des GovCERT eingebunden waren Kärnten und die Steiermark.

Er empfahl daher dem Bundeskanzleramt, eine Initiative zu starten, um alle Länder sowie weitere Städte bzw. Gemeinden als Teilnehmer an der Informationsdrehscheibe des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) zu integrieren.

19.3 Das Bundeskanzleramt sagte in seiner Stellungnahme zu, einen Evaluierungsprozess bezüglich der Aufgaben des Computer–Notfallteams der öffentlichen Verwaltung zu starten. Zur Empfehlung, langfristig die Leistungen des Computer–Notfallteams der öffentlichen Verwaltung durch Bedienstete des Bundes zu erbringen, wies das Bundeskanzleramt auf die Ressourcensituation hin (siehe auch TZ 4).

Weiters werde es die Empfehlung berücksichtigen, im Zuge eines allfälligen nächsten Vergabeverfahrens bezüglich der operativen Leistungen des Computer–Notfallteams für die öffentliche Verwaltung den zu erbringenden Leistungsumfang näher zu definieren.

Das Bundeskanzleramt sagte zu, die rechtlichen Möglichkeiten zur Integration der Länder sowie weiterer Städte bzw. Gemeinden als Teilnehmer an der Informationsdrehscheibe des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) prüfen zu wollen. Für öffentlich–rechtliche Gebietskörperschaften sei der freiwillige Einstieg in das Regime des NISG möglich.

19.4 Der RH hielt fest, dass – unabhängig von den Ergebnissen der Prüfung der rechtlichen Möglichkeiten – eine Initiative gestartet werden könnte, um alle Länder sowie weitere Städte bzw. Gemeinden als Teilnehmer an der Informationsdrehscheibe des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) zu integrieren.

Frühwarnsystem (Sensornetzwerk)

20.1 Um etwaigen Sicherheitsvorfällen vorzubeugen, war der Bundesminister für Inneres gemäß § 13 i.V.m. § 5 Abs. 1 Z 4 NISG dazu ermächtigt, IKT–Lösungen zu betreiben, welche die Risiken oder Vorfälle von Netz– und Informationssystemen frühzeitig erkennen. Dabei handelte es sich um ein Frühwarnsystem (Sensornetzwerk), das Indikatoren (Merkmale und Daten) auswertete und erkannte[42], die auf eine Kompromittierung eines Computersystems oder Netzwerks hinwiesen (Indicator of Compromise).

[42] Merkmale konnten beispielsweise Einträge in Logfiles, außergewöhnlicher Netzwerkverkehr, bestimmte Dateien, einzelne Prozesse, Verzeichnis–Einträge oder Aktivitäten unter einer Benutzerkennung sein. Durch entsprechend konfigurierte und vor den Netzwerken von teilnehmenden Organisationen platzierte Sensoren sollten Angriffe bzw. das Vorgehen des Angreifers im Netz der teilnehmenden Organisationen erkannt werden.

Betreiber wesentlicher Dienste, Anbieter digitaler Dienste, Einrichtungen der öffentlichen Verwaltung sowie Betreiber öffentlicher Kommunikationsnetze oder –dienste konnten am Frühwarnsystem (Sensornetzwerk) teilnehmen. Ein zentraler Betrieb für möglichst viele Organisationen diente einerseits dazu, Cyber–Angriffe zu erkennen bzw. deren Auswirkungen so gering wie möglich zu halten, andererseits Muster und Vorgehensweisen bei Cyber–Angriffen zu analysieren.

Laut wirkungsorientierter Folgenabschätzung zum NISG wendet das Innenministerium für das Frühwarnsystem (Sensornetzwerk) ab dem Jahr 2020 jährlich rd. 1,70 Mio. EUR an betrieblichem Sachaufwand sowie für Werkleistungen und Investitionen (Software, Hardware) in den Jahren 2019 bis 2022 in Summe rd. 3,89 Mio. EUR auf:

Tabelle 8: Frühwarnsystem des Innenministeriums (Sensornetzwerk)

Auszahlungen für Frühwarnsystem des Innenministeriums (Sensornetzwerk)					
	2019	2020	2021	2022	Summe
	in EUR				
	Abschätzung gemäß wirkungsorientierter Folgenabschätzung zum NISG				
Betrieb	–	1.700.000	1.700.000	1.700.000	5.100.000
Werkleistungen, Lizenzen	200.000	250.000	450.000	800.000	1.700.000
Software, Hardware	406.000	1.226.000	160.000	400.000	2.192.000
	geplant laut Innenministerium für Frühwarnsystem				
NIS–Umsetzungsprogramm des Innenministeriums	–	–	1.096.000	2.209.000	weitere Auszahlungen 2023 und 2024 geplant: 6.715.000

Rundungsdifferenzen möglich Quelle: BMI

NIS = Netz– und Informationssystemsicherheit
NISG = Netz– und Informationssystemsicherheitsgesetz

Das Innenministerium teilte im Mai 2021 mit, dass sich das Frühwarnsystem (Sensornetzwerk) in der Konzeptionsphase befand und für das Jahr 2021 eine Ausschreibung zur Detailkonzipierung dieses Systems geplant sei, welches ab dem Jahr 2022 umgesetzt bzw. implementiert werden sollte. Für die Umsetzung sah das Innenministerium im Zuge seines Programms zur Umsetzung der Netz– und Informationssicherheit im Jahr 2021 Kosten in der Höhe von rd. 1,10 Mio. EUR und im Jahr 2022 von rd. 2,21 Mio. EUR vor. Bis zum Jahr 2024 sollten so in Summe 6,72 Mio. EUR für die Errichtung und den Betrieb eines Sensornetzwerks als Frühwarnsystem investiert werden.

20.2 Der RH stellte kritisch fest, dass das geplante Frühwarnsystem (Sensornetzwerk) zur Erkennung von Risiken bzw. Vorfällen von Netz– und Informationssystemen im Jahr 2021 erst in einer ersten Konzeptionsphase war, obwohl die wirkungsorientierte Folgenabschätzung zum NISG hierzu schon im Jahr 2019 erste Investitionen und bereits im Jahr 2020 Betriebskosten vorsah.

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

20.3 Das Innenministerium teilte in seiner Stellungnahme mit, dass es die technische und organisatorische Detailkonzeption des Frühwarnsystems ehestmöglich ausschreiben werde. Nach Abschluss des Konzeptionsprojekts werde – nach Besetzung der offenen Arbeitsplätze im zuständigen Referat – zeitnah mit der Umsetzung und Implementierung des IOC (Indicator of Compromise)–basierten Frühwarnsystems begonnen.

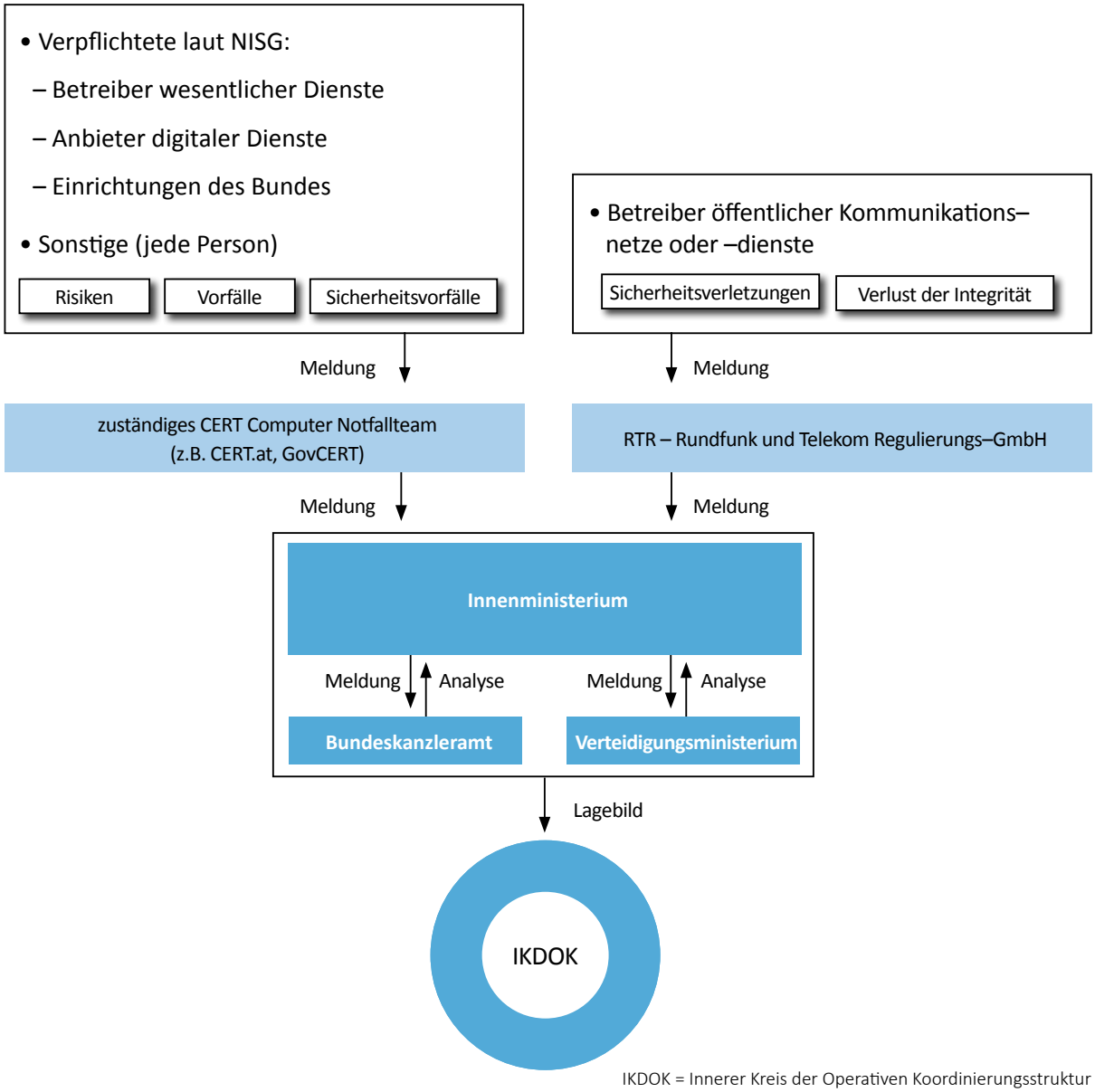
Im Rahmen der vor Kurzem gestarteten europäischen Initiative „Network of SOCs“ (Security Operations Center) würden bereits diesbezügliche Best Practices und Input aus anderen EU–Mitgliedstaaten gesammelt.

Vorfalls– und Krisenmanagement

Grundlagen und Meldestrukturen

21.1 (1) Für die Cyber–Sicherheit relevante Vorfälle (Risiken, Vorfälle, Sicherheitsvorfälle im Sinne des NISG) erreichten die Koordinationsstrukturen[43] über entsprechende Meldungen. Die zur Zeit der Gebarungsüberprüfung etablierten Strukturen zur Meldung von (Sicherheits–)Vorfällen und deren Behandlung stellten sich wie folgt dar:

Abbildung 2: Meldestrukturen



IKDOK = Innerer Kreis der Operativen Koordinierungsstruktur
Quellen: BMI; NISG; Darstellung: RH

[43] Informationen zu Cyber–Sicherheits–Gefährdungen bei Organisationen, die nicht dem NISG unterworfen waren, wurden je nach Informationsstand von den Computer–Notfallteams (TZ 18) verarbeitet und erforderlichenfalls in den Lagebildern (TZ 15) berücksichtigt.

Sicherheitsvorfälle[44] waren von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen des Bundes jedenfalls über das jeweils zuständige Computer–Notfallteam an den Bundesminister für Inneres zu melden. Sonstige Vorfälle[45] und Risiken[46] konnten von den genannten Einrichtungen und auch von jeder Person freiwillig gemeldet werden. Im Sektor Bankwesen und im Sektor digitale Infrastruktur waren Meldungen aufgrund sektorspezifischer Rechtsgrundlagen an die Finanzmarktaufsichtsbehörde bzw. Rundfunk und Telekom Regulierungs–GmbH (RTR) zu erstatten, die diese ihrerseits an den Bundesminister für Inneres weiterleiten mussten.

(2) Der Bundesminister für Inneres war gemäß NISG (§ 5 Abs. 1 Z 3 bzw. § 11 Abs. 1) dazu verpflichtet, diese Meldungen entgegenzunehmen, zu analysieren und daraus regelmäßig ein Lagebild (TZ 15) zu erstellen, um dieses an inländische Behörden oder Stellen weiterzuleiten.[47] Diese Aufgaben nahm die Abteilung Cybersicherheit im damaligen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung als operative NIS–Behörde[48] wahr. Sie erfasste daher sämtliche Meldungen aktenmäßig und speicherte diese in einer Meldungsübersicht. Jede Meldung, die über die im NISG definierten Meldewege gemeldet wurde, wurde unmittelbar auch an das Bundeskanzleramt und Verteidigungsministerium übermittelt (NIS–Meldung). Die einzelnen Meldungen wurden in diesem Stadium noch nicht vertiefend analysiert. Das Bundeskanzleramt, das Innenministerium und das Verteidigungsministerium führten in weiterer Folge jeweils eigene Analysen durch, die wiederum im Kreise dieser drei Bundesministerien ausgetauscht wurden.

(3) Zur Analyse und Bewertung dieser Meldungen sowie der Erkenntnisse aus dem Sensornetzwerk (TZ 20) war der Bundesminister für Inneres außerdem verpflichtet (§ 11 Abs. 1 NISG), ein „NIS–Meldeanalysesystem“ zu betreiben. Dies war eine IKT–Lösung, welche die Erstellung des Lagebildes mittels strategischer und operativer Analyse unterstützen sollte. Eine solche Analyse war eine Methode, das Ausmaß, die Erscheinungsformen und den Charakter (Qualität, Quantität und Struktur) von Angriffen zu erfassen, um Erkenntnisse zu ihren Bewegungen, Entwicklungen und beeinflussbaren Rahmenbedingungen zu gewinnen und darauf aufbauend Präven-

44 Ein „Sicherheitsvorfall“ ist gemäß § 3 Z 6 NISG definiert als eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat.

45 „Vorfälle“ sind gemäß § 3 Z 7 NISG definiert als Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen haben und kein Sicherheitsvorfall sind.

46 „Risiken“ sind gemäß § 3 Z 8 NISG alle Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz– und Informationssystemen haben.

47 Zur Sicherstellung der Information über Sicherheitsvorfälle von internationaler Relevanz, insbesondere für diesbezügliche Meldungen von bzw. an die anderen EU–Mitgliedstaaten, war im Innenministerium eine zentrale Anlaufstelle (Single Point of Contact – SPOC) eingerichtet (TZ 17).

48 Mit der Gründung der Direktion Staatsschutz und Nachrichtendienst wurde diese Aufgabe der Abteilung Netz– und Informationssystemsicherheit in der Sektion IV übertragen.

tions– und Abwehrmaßnahmen zu entwickeln. Das Meldeanalysesystem war auch dem Bundeskanzler und der Bundesministerin für Landesverteidigung bereitzustellen.

Das Innenministerium teilte dazu mit, dass die Meldungsübersicht ab Jahresmitte 2021[49] durch eine neue IT–Anwendung (Meldesammelsystem) unterstützt werden soll, wofür im Jahr 2021 rd. 24.000 EUR budgetiert waren. Darüber hinaus waren keine IKT–Lösungen zur Meldeanalyse implementiert. Die IT–mäßige und vollständige Umsetzung des Meldeanalysesystems war im Rahmen eines eigenen Umsetzungsprojekts geplant. Zur Finanzierung dieses Projekts hatte das Innenministerium auch einen EU CEF–Förderantrag[50] gestellt. Das Innenministerium rechnete mit einer Entscheidung über die Förderung seitens der EU im Sommer 2021.

Das Innenministerium teilte hierzu im September 2021 mit, dass das Meldesammelsystem seit August 2021 in Betrieb gegangen und der Förderantrag bewilligt worden sei.

21.2 Der RH stellte fest, dass zwar die nach dem NISG eingehenden Meldungen im Innenministerium aktenmäßig erfasst, in einer Meldungsübersicht eingetragen und an das Bundeskanzleramt sowie das Verteidigungsministerium weitergeleitet wurden. Er wies jedoch kritisch darauf hin, dass rund zweieinhalb Jahre nach dem Inkrafttreten des NISG noch keine IKT–Lösung zur Umsetzung des im NISG vorgesehenen NIS–Meldeanalysesystems in Betrieb war.

Er empfahl dem Innenministerium, das Meldesammelsystem rasch umzusetzen; die Erfahrungen aus dem Betrieb sollen dafür genutzt werden, die im NISG vorgesehene IKT–Lösung für ein NIS–Meldeanalysesystem umzusetzen.

21.3 Laut Stellungnahme des Innenministeriums sei das Meldesammelsystem bereits implementiert und seit dem dritten Quartal 2021 produktiv im Einsatz. Das Meldeanalysesystem würde zur Zeit der Stellungnahme im Rahmen eines von der EU geförderten Projekts gemeinsam mit dem Bundeskanzleramt und dem nationalen Computer–Notfallteam konzipiert und implementiert.

[49] Gemäß einem Fortschritts– und Risikobericht des Innenministeriums zur Umsetzung des NISG vom Jänner 2021 sollte die IKT–Anwendung für die Meldesammelstelle im September 2021 in Betrieb genommen werden und nach einer Evaluierung im Oktober 2021 in den Echtbetrieb gehen.

[50] Connecting Europe Facility (CEF) ist das europäische Finanzinstrument zur Förderung wichtiger transeuropäischer Infrastrukturvorhaben im Energie–, Transport– und Telekommunikationssektor. In den Jahren 2021 bis 2027 hat die CEF die Schwerpunkte „Verkehr“, „Energie“ und „Digitales“.

Klassifizierung von Risiken und Vorfällen

22.1 (1) Im Zeitraum Jänner 2019 bis Dezember 2020 wurden von der operativen NIS–Behörde im Innenministerium insgesamt 107 Meldungen[51] zu Risiken und Sicherheitsvorfällen gemäß NISG erfasst. Darin waren 42 Meldungen zu Sicherheitsvorfällen im Sinne des NISG enthalten; dazu zählten auch die 18 Meldungen durch Computer–Notfallteams (GovCERT, CERT.at, Austrian Energy CERT).

Die operative NIS–Behörde im Innenministerium klassifizierte die Vorfälle anlassbezogen, aber nicht nach einer standardisierten Taxonomie (Klassifikationsschema). Laut Angaben des Innenministeriums soll künftig die Klassifizierung gemäß der „Cybersecurity Incident Taxonomy“ durchgeführt werden.

Die Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) und für den Sektor Energie (Austrian Energy CERT) sowie das nationale Computer–Notfallteam (CERT.at) verwendeten zur Klassifizierung von Vorfällen die „Reference Security Incident Taxonomy“. Das geplante Computer–Notfallteam des Innenministeriums sah hingegen eine andere Klassifizierung vor; das Computer–Notfallteam des Verteidigungsministeriums (**MilCERT**) setzte wiederum eine andere Klassifizierung ein – das für diesen Bereich besser geeignete „MITRE Adversarial Tactics, Techniques & Common Knowledge Framework“.

(2) Der RH überprüfte stichprobenartig das System der Vorfallbehandlung anhand eines Einzelfalls (anonyme Meldung eines Hackerangriffs vom Juni 2020). Dabei überprüfte er die dazu erstellte Dokumentation sowie die Relevanz der Daten, die zu den eingegangenen Meldungen erfasst wurden, für die im NISG vorgesehene strategische und operative Analyse (z.B. Kategorie, Schweregrad oder Priorisierung des Vorfalls).

Die (dokumentierten) Eckdaten des Falls stellten sich wie folgt dar:

Tabelle 9: Analyse eines Cyber–Sicherheit Einzelfalls

Zeitpunkt	Meldung durch	Meldung an	Gegenstand des Vorfalls	Vorfalls-akt	weitere Ermittlungs-maßnahmen	Behand-lung IKDOK	Behand-lung OpKoord	Aufnahme ins Lagebild
Juni 2020	anonym	operative NIS–Behörde	Ablage Spam auf Server durch Hacker	ja	nein	ja	ja	nein

IKDOK = Innerer Kreis der Operativen Koordinierungsstruktur
NIS = Netz– und Informationssystemsicherheit
OpKoord = Operative Koordinierungsstruktur

Quelle: BMI

[51] Informationen zu Cyber–Sicherheits–Gefährdungen bei Organisationen, die nicht dem NISG unterworfen waren, wurden je nach Informationsstand von den Computer–Notfallteams (TZ 18) verarbeitet und erforderlichenfalls in den Lagebildern (TZ 15) berücksichtigt.

Zum Umfang der Vorfalldokumentation war festzuhalten:

- Der Schweregrad des Vorfalls wurde im System nicht erfasst.
- Eine Kategorisierung des Vorfalls in standardisierter Form – wie eine Erfassung von standardisierten Merkmalen, die einen Hinweis auf die technische Ausgestaltung, die Regionalität oder etwa die Art des Vorfalls geben konnten – kam ebenfalls nicht zum Einsatz.
- Klare Kriterien, wann der Vorfall zur Behandlung in den IKDOK bzw. die OpKoord gelangen sollte, waren nicht festgelegt.
- Eine Priorisierung des Vorfalls wurde nicht dokumentiert.
- Angaben über die tatsächliche Dauer bzw. Zeitspanne des Vorfalls fehlten.
- Der für die Vorfallbehandlung geleistete Aufwand (z.B. zeitlich, monetär) wurde nicht erfasst.

Das Innenministerium teilte dazu mit, dass im neuen Meldesammelsystem (TZ 21) die systematische Erfassung des Schweregrades, einer Kategorisierung sowie einer Priorisierung vorgesehen sei.

22.2 (1) Der RH kritisierte, dass die operative NIS–Behörde im Innenministerium bisher keine Klassifizierung von Sicherheitsvorfällen im Sinne einer standardisierten Taxonomie eingerichtet hatte.

Er empfahl dem Innenministerium, eine standardisierte Taxonomie zur Klassifizierung von Sicherheitsvorfällen für die operative NIS–Behörde, unter Berücksichtigung einheitlich abgestimmter europäischer Lösungen für den Behördenbereich, einzurichten.

Der RH hielt kritisch fest, dass die (geplante) Klassifizierung in der NIS–Behörde und jene in den Computer–Notfallteams unterschiedliche Taxonomien nutzten und damit nicht vergleichbar waren.

Er empfahl den überprüften Stellen, im Rahmen des IKDOK eine Empfehlung für eine einheitliche Taxonomie für österreichische Computer–Notfallteams unter Bezug auf europäische Lösungen auszuarbeiten. Diese sollte bestmöglich auf die Taxonomie der NIS–Behörde im Innenministerium abgestimmt sein, um so den Meldeprozess zu optimieren. Das Ergebnis wäre im Wege der OpKoord bzw. des CERT.at den in Österreich tätigen Computer–Notfallteams bekannt zu geben.

(2) Der RH hielt kritisch fest, dass in der Vorfalldokumentation des stichprobenartig überprüften Beispiels (anonyme Meldung eines Hackerangriffs vom Juni 2020) wichtige Informationen fehlten, beispielsweise zur Kategorisierung, zum Schweregrad, zur Dauer des Vorfalls, zum geleisteten Aufwand und zu Priorisierungen.

Der RH anerkannte, dass das Innenministerium bereits zur Zeit der Gebarungsüberprüfung an der Verbesserung des Systems zur Vorfalldokumentation im Wege des Meldesammelsystems arbeitete und wesentliche Kriterien wie den Schweregrad, eine Kategorisierung sowie eine Priorisierung berücksichtigte. Er wies in diesem Zusammenhang aber darauf hin, dass weiterhin klare Kriterien fehlten, unter welchen Umständen bzw. wann die Befassung von weiteren Gremien wie des IKDOK bzw. der OpKoord notwendig wären. Auch die Angaben über die tatsächliche Dauer bzw. Zeitspanne des Vorfalls sowie über den für die Vorfallbehandlung geleisteten Aufwand (z.B. zeitlich, monetär) waren für eine Dokumentation nicht vorgesehen.

Der RH empfahl daher dem Innenministerium, in der Vorfalldokumentation jedenfalls klare Kriterien zur Befassung weiterer Gremien wie IKDOK bzw. OpKoord festzulegen sowie zu evaluieren, ob auch Informationen zur Dauer des Vorfalls und zum geleisteten Aufwand ergänzt werden sollten.

22.3 (1) Das Bundeskanzleramt sagte in seiner Stellungnahme zu, im Rahmen seiner Zuständigkeiten an der Erarbeitung einer für Computer–Notfallteams einheitlichen Taxonomie und der Verteilung der Ergebnisse mitzuarbeiten.

(2) Das Innenministerium teilte in seiner Stellungnahme mit, dass eine standardisierte Taxonomie zur Klassifizierung von Sicherheitsvorfällen für die operative NIS–Behörde bereits eingerichtet sei. Im Meldesammelsystem der operativen NIS–Behörde werde die Taxonomie der Europäischen NIS–Kooperationsgruppe (NIS–CG) verwendet.

Zur Ausarbeitung einer einheitlichen Taxonomie für Computer–Notfallteams habe bereits ein erster Workshop zwischen den IKDOK–Teilnehmerorganisationen und den gemäß NISG ernannten Computer–Notfallteams im dritten Quartal 2021 stattgefunden. Weitere Arbeiten zur Vereinheitlichung bzw. zur Vergleichbarkeit der eingesetzten Taxonomien würden mit Beginn 2022 fortgeführt.

Innerhalb der Systeme des Innenministeriums solle für die Klassifizierung von Security Events die europäische Computer Security Incident Response Team II Taxonomy zum Einsatz kommen, um so einen einheitlichen Informationsaustausch auch mit anderen externen Stellen in geeigneter Form gewährleisten zu können.

Die Empfehlung zur Vorfalldokumentation bei der geplanten Überarbeitung der NIS–spezifischen Prozesse werde in der seit Dezember 2021 eingerichteten Abteilung Netz– und Informationssystemsicherheit berücksichtigt und eingearbeitet.

(3) Das Verteidigungsministerium sagte in seiner Stellungnahme zu, die Ausarbeitung einer auf Basis von EU–Vorgaben vereinheitlichten Taxonomie für die Kommunikation mit den Computer–Notfallteams zu unterstützen.

Auch wolle es eine Ergänzung der Vorfalldokumentation um alle Daten, die einen Lessons–Learned–Prozess berücksichtigen, unterstützen.

Sicherheitsschwachstelle „Groupware und E–Mail“

23.1 (1) Im März 2021 wurden Sicherheitsschwachstellen in einer welt– und österreichweit verbreiteten Groupware– und E–Mail–Server–Software bekannt. Da diese Sicherheitsschwachstellen[52] bei Cyber–Angriffen ein hohes Risiko darstellten, erhob der RH im Rahmen der Gebarungsüberprüfung, wie die österreichische Koordination zur Abwehr dieses Cyber–Risikos erfolgte.

Sicherheitsschwachstellen von Softwareprodukten sind grundsätzlich nichts Außergewöhnliches, deren Handhabung ist für Computer–Notfallteams Teil des Alltagsgeschäfts. Diese waren für Beobachtung, Analyse, Verteilung von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken bzw. Handlungsempfehlungen zu deren Behebung zuständig.

Die Beobachtung von Schwachstellen in Software oder von Vorfällen und deren Meldungen erfolgten grundsätzlich durch jede IKDOK–Teilnehmerorganisation autonom in ihrem Aufgabenbereich. Die Erörterung des Lagebildes, die Verarbeitung der verfügbaren Informationen und auch der Austausch mit nationalen und internationalen Cyber–Sicherheits–Organisationen oblagen den jeweils verantwortlichen Gremien und Organisationen (IKDOK/OpKoord, SPOC, GovCERT).

[52] Grundsätzlich ist es aufgrund der Schwachstellen möglich, dass Angreifer darüber einen eigenen Programmcode auf den betroffenen Servern ausführen und die Kontrolle über diese Server erlangen. Erfolgreiche Attacken sind u.a. deshalb so gefährlich, weil die Angreifer auch Hintertüren („Backdoors“) hinterlassen können, die einen späteren Fernzugriff auf diese Server ermöglichen.

(2) Der zeitliche Ablauf der Aktivitäten ab Bekanntwerden der Sicherheitsschwachstellen stellte sich wie folgt dar:

Tabelle 10: Eckdaten Sicherheitsschwachstellen „Groupware– und E–Mail–Server–Software“

Datum	Beschreibung
2. März 2021	Der Softwarehersteller informiert über die Sicherheitsschwachstellen und stellt entsprechende Software–Aktualisierungen zur Behebung der Schwachstellen zur Verfügung. Computer–Notfallteams CERT.at und GovCERT werden unmittelbar danach aktiv.
3. März 2021	Das nationale Computer–Notfallteam (CERT.at) übernimmt die führende Rolle und informiert im Wege der entsprechenden Verteiler sowie der Homepage über die Schwachstellen sowie die notwendigen Gegenmaßnahmen; auch alle relevanten Gremien (Mitglieder von CSP, Steuerungsgruppe–CSS, GovCERT, CERT) werden informiert.
4. März 2021	Es findet eine IKDOK–Besprechung statt, ein Lagebild wird erarbeitet. Das nationale Computer–Notfallteam (CERT.at) sowie das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) führen eine gesamtstaatliche Lageerhebung inklusive Risikoeinschätzung durch. Das nationale Computer–Notfallteam (CERT.at) aktualisiert die Warnmeldungen. An die von den Sicherheitsschwachstellen betroffenen Organisationen, welche das nationale Computer–Notfallteam (CERT.at) ermittelt hatte, werden Warnungen samt Empfehlungen proaktiv übermittelt.
11. März 2021	Ein IKDOK–Sonderlagebild zu den Sicherheitsschwachstellen mit zusätzlichen Hinweisen wird erstellt und verteilt.
17. März 2021	Die Sicherheitsschwachstellen werden in einem regulären Lagebild dargestellt. Es wird darin auch auf eine mit den Schwachstellen zusammenhängende Bedrohung durch Ransomware hingewiesen (Schadprogramme, die den Zugriff auf Daten und Systeme einschränken oder verhindern).

CERT = Computer Emergency Response Team (Computer–Notfallteam)
CSP = Cyber Sicherheit Plattform
CSS = Cyber Sicherheit Steuerungsgruppe
GovCERT = Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung)
IKDOK = Innerer Kreis der Operativen Koordinierungsstruktur

Quellen: BKA; BMI

Informationen über die österreichische Lage wurden mit EU–Partnern geteilt (CyCLONe und CSIRTs–Netzwerk). Insgesamt gab es drei freiwillige Meldungen an die operative NIS–Behörde im Innenministerium.

Laut Auskunft des Bundeskanzleramts, des Innen–, Verteidigungs– und Außenministeriums seien die ressorteigenen Groupware– und E–Mail–Server nicht von den gegenständlichen Problemen betroffen gewesen; darüber hinaus seien die erforderlichen Software–Aktualisierungen zeitnah eingespielt worden.

Bei den Einrichtungen der öffentlichen Verwaltung (Bund, Länder) seien laut Auskunft des Bundeskanzleramts bzw. des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) sowie des Innenministeriums die notwendigen Maßnahmen zeitnah durchgeführt worden, so dass nach ihrem Wissensstand keine IT–Systeme

der öffentlichen Verwaltung mehr von den Sicherheitsschwachstellen betroffen seien.

23.2 Der RH anerkannte, dass das Bundeskanzleramt, das Innenministerium, das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) und der IKDOK anlässlich der aufgezeigten Sicherheitsschwachstellen von Groupware– und E–Mail–Server–Software die erforderlichen Maßnahmen zur Koordination der Cyber–Sicherheit zeitnah und angemessen durchführten. Die öffentliche Verwaltung konnte darauf aufbauend die entsprechenden Sicherheitsvorkehrungen effektiv umsetzen.

Der RH verwies jedoch auf das außerhalb der öffentlichen Verwaltung noch bestehende Risiko, dass die entsprechenden Software–Aktualisierungen zur Behebung der Sicherheitsschwachstellen noch nicht installiert waren bzw. in den Systemen bereits Zugänge für die externe Manipulation der Systeme („Backdoors“) aktiviert waren.

Er empfahl daher dem Bundeskanzleramt (Leitung des GovCERT), dem Innenministerium, dem Verteidigungsministerium und dem Außenministerium, im Rahmen des IKDOK vorbeugende Maßnahmen für die noch bestehenden Risiken von mit Schadsoftware infizierten externen Groupware– und E–Mail–Servern zu evaluieren.

23.3 (1) In seiner Stellungnahme teilte das Bundeskanzleramt mit, dass die Empfehlung des RH evaluiert werde.

(2) Laut Stellungnahme des Innenministeriums werde diese Thematik laufend in den IKDOK–Lagesitzungen und in darauffolgenden Initiativen (seitens des nationalen Computer–Notfallteams sowie der NIS–Behörden) behandelt und beobachtet.

(3) Das Verteidigungsministerium sagte in seiner Stellungnahme zu, eine Evaluierung von bestehenden Risiken bei externen Groupware– und E–Mail–Servern, die mit Schadsoftware infiziert bzw. mit Schwachstellen behaftet sind, zu unterstützen.

Cyber–Angriff auf das Außenministerium

Zeitlicher Ablauf und Strukturen des Krisenmanagements

24.1 (1) Im Dezember 2019 erfolgte ein verdeckter Cyber–Angriff auf die Systeme des Außenministeriums, der in weiterer Folge erstmals zur Feststellung einer Cyber–Krise und damit auch zur Aktivierung der dafür vorgesehenen Strukturen führte (TZ 11). In ihrem zeitlichen Ablauf stellten sich dieser Cyber–Angriff bzw. die Cyber–Krise wie folgt dar:

Tabelle 11: Eckdaten zum Ablauf der Cyber–Krise

Datum	Beschreibung
Dezember 2019	rekonstruierter Beginn des Cyber–Angriffs
	Hinweis auf den Cyber–Angriff an GovCERT und Innenministerium; umgehende Weiterleitung der Informationen an das Außenministerium
	operative NIS–Behörde (Innenministerium) legt Vorfallsakt an (TZ 21 und TZ 22)
	laufende Beobachtung des Angreifers im System und Durchführung von technischen Gegenmaßnahmen
Jänner 2020	Ausmaß des Cyber–Angriffs wird erkennbar; IKDOK und Cyberkrisenmanagement–Koordinationsausschuss tagen; Bundesminister für Inneres stellt Cyber–Krise fest; Öffentlichkeit und Datenschutzbehörde werden informiert
	Innenministerium und Außenministerium bereiten Einsatzstruktur vor (TZ 25); technische Erstinformation aller Bundesministerien durch GovCERT
	Einsatzstruktur geht operativ (TZ 25)
	technische Risikowarnung der BRZ GmbH betreffend Aktenverwaltungs–, Haushaltsverrechnungs– und Personalmanagementsystem des Bundes (TZ 25)
	Assistenzeinsatz des Bundesheers wird angefordert; Notbeschaffung des Außenministeriums betreffend Software und Dienstleistungen zur Bewältigung der Cyber–Krise (Gesamtvolumen 1,69 Mio. EUR brutto) (TZ 26)
	Ende der IKDOK–Unterstützungsleistungen und Übergabe an das Außenministerium
Februar 2020	Möglichkeit der Kommunikation des Angreifers mit den kompromittierten Systemen des Außenministeriums wird durch Bereinigung endgültig unterbunden und sämtliche Schadsoftware aus dem System entfernt: „Brand aus“ nach Analysephase und Durchführung aller Gegenmaßnahmen; Beginn „Brandwache“ (bis Juni 2021)
März 2020	Beendigung der Cyber–Krise durch Bundesminister für Inneres

BRZ GmbH = Bundesrechenzentrum Gesellschaft mit beschränkter Haftung
GovCERT = Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung)
IKDOK = Innerer Kreis der Operativen Koordinierungsstruktur

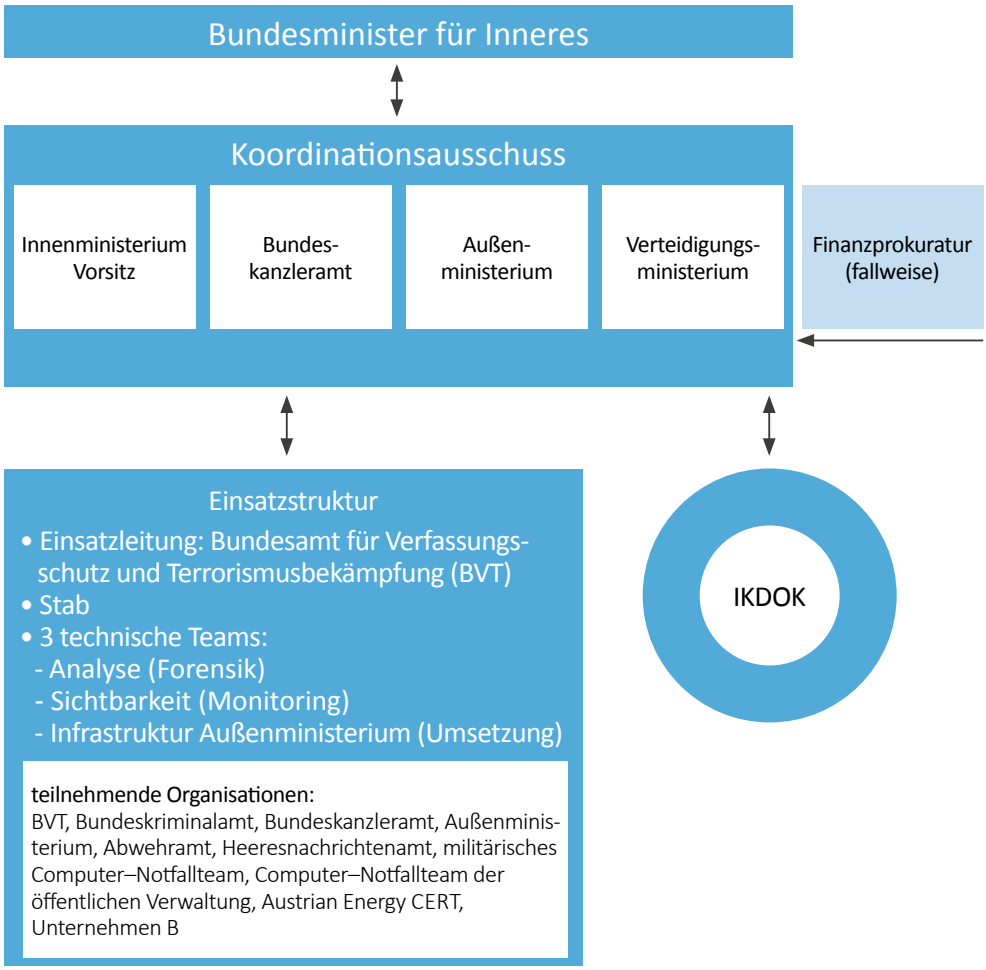
Quellen: BMI; BMEIA

Das Außenministerium erlangte vom Cyber–Angriff am 21. Dezember 2019 Kenntnis und wurde ab diesem Zeitpunkt durch Personal des Innenministeriums sowie des GovCERT unterstützt. Die Cyber–Krise wurde durch den Bundesminister für Inneres am 4. Jänner 2020 festgestellt.

(2) Aufgrund der Weihnachtsfeiertage und der Feiertage rund um den Jahreswechsel standen dem Innen– und Außenministerium insbesondere die personellen Ressourcen nicht im üblichen Ausmaß zur Verfügung. Die jeweils im Bundeskanzleramt, im Innenministerium und im Verteidigungsministerium bestehenden Strukturen zur Cyber–Sicherheit waren vor der Cyber–Krise bzw. vor Aktivierung der Einsatzstrukturen nicht auf einen 24–Stunden–7–Tage–Betrieb an 365 Tagen im Jahr ausgelegt.

(3) Nachdem das Ausmaß des Cyber–Angriffs auf die Systeme des Außenministeriums erkennbar wurde, tagte am 4. Jänner 2020 erstmals der Koordinationsausschuss unter Teilnahme des (damaligen) Bundesministers für Inneres. In dieser Sitzung stellte dieser auch gemäß § 24 NISG das Vorliegen einer Cyber–Krise förmlich fest. In weiterer Folge wurde zur Bekämpfung der Krise eine eigene Einsatzstruktur (neben dem IKDOK) etabliert. Diese Strukturen zum Cyber–Krisenmanagement stellten sich in Summe wie folgt dar:

Abbildung 3: Strukturen des Cyber–Krisenmanagements



IKDOK = Innerer Kreis der Operativen Koordinierungsstruktur
Quellen: BMI; NISG; Darstellung: RH

Zwischen dem 4. Jänner und dem 13. Februar 2020 tagte der Koordinationsausschuss insgesamt neunmal. Wie in § 25 Abs. 2 NISG vorgesehen, führte der Generaldirektor für die öffentliche Sicherheit den Vorsitz und nahmen der Chef des

Generalstabs und der jeweilige Generalsekretär des Außenministeriums[53] regelmäßig an den Sitzungen teil. Zur rechtlichen Beratung nahm auch der Präsident der Finanzprokuratur regelmäßig an den Sitzungen des Koordinationsausschusses teil.

Im Bundeskanzleramt war die Funktion des Generalsekretärs bis 6. Jänner 2020 nicht besetzt. Der mit 7. Jänner 2020 betraute Generalsekretär des Bundeskanzleramts nahm an den Sitzungen des Koordinationsausschusses nicht teil.

(4) Die Einsatzstruktur bestand aus einer Einsatzleitung, einem Einsatzstab sowie aus drei technischen Teams für die Forensik, das Monitoring (Beobachtung im Netzwerk bzw. auf Systemebene) und für die Umsetzung von Maßnahmen. Dazu mussten im Rahmen der Einsatzvorbereitung (am 5. und 6. Jänner 2020) unter Federführung des Innenministeriums die Infrastruktur (Räumlichkeiten) und sonstige Ausstattung (Hardware, Software, Büroausstattung) erst organisiert und beschafft werden, um die Einsatzbereitschaft herstellen zu können. Am 7. Jänner 2020 konnte die Einsatzstruktur ihre Tätigkeiten operativ aufnehmen.

(5) Zentrales Thema der Sitzung des Koordinationsausschusses am 8. Jänner 2020 war eine Risikowarnung der Bundesrechenzentrum Gesellschaft mit beschränkter Haftung (in der Folge: **BRZ GmbH**). Diese betraf die von der BRZ GmbH betriebenen bundesweiten Anwendungen zur Aktenverwaltung (ELAK im Bund), zur Haushaltsverrechnung (HV–SAP) und zum Personalmanagement (PM–SAP). Auf Basis einer technischen Risikoeinschätzung empfahl die BRZ GmbH den für diese Systeme führend verantwortlichen Bundesministerien (Digitalisierungsministerium, Bundesministerium für Finanzen (in der Folge: **Finanzministerium**) und Bundeskanzleramt), die Benutzerkonten des Außenministeriums aufgrund der möglichen Kompromittierung dieser zu trennen. Diese Vorgehensweise war vorab weder mit dem Koordinationsausschuss noch mit dem IKDOK abgestimmt. An dieser Sitzung des Koordinationsausschusses nahmen zwar Vertreter der BRZ GmbH teil, das Finanz– und das Digitalisierungsministerium waren jedoch (zu diesem Zeitpunkt) nicht formell in die Strukturen zur Bewältigung der Cyber–Krise eingebunden. Erst am 24. Jänner 2020 fand ein Briefing des Finanzministeriums und der BRZ GmbH durch den IKDOK statt. Nachdem das Finanzministerium als für das Haushaltsverrechnungssystem verantwortliches Ministerium entschieden hatte, die Benutzerkonten des Außenministeriums in diesem System zu deaktivieren, war die Haushaltsverrechnung im Außenministerium inklusive seiner Auslandsvertretungen unmittelbar nicht mehr verfügbar; sie musste mittelfristig durch Ersatzlösungen sichergestellt werden.

[53] Mit 7. Jänner 2020 erfolgte im Außenministerium ein personeller Wechsel in der Funktion des Generalsekretärs.

24.2 (1) Zu den Sitzungen des Koordinationsausschusses verwies der RH auf seine Feststellungen in TZ 11, wonach vor allem die personelle Zusammensetzung dieses Ausschusses mit den höchsten Funktionsträgern die unmittelbare Information der verantwortlichen Regierungsmitglieder und die effiziente Umsetzung der beschlossenen Maßnahmen in den jeweiligen Ressortbereichen sicherstellen sollte. Er wies daher kritisch darauf hin, dass der Generalsekretär des Bundeskanzleramts an keiner Sitzung des Koordinationsausschusses teilgenommen hatte, obwohl dies in § 25 NISG explizit vorgesehen war. Der RH verwies in diesem Zusammenhang auch auf seinen Bericht „Generalsekretariate in den Bundesministerien“ (Reihe Bund 2021/12): Darin hatte er (in TZ 11 und TZ 31) u.a. festgestellt, dass unklar war, welche konkreten Geschäfte in den Aufgabenbereich einer Generalsekretärin bzw. eines Generalsekretärs fallen und dass auch die Geschäftsordnung des Bundeskanzleramts eine ausreichende Konkretisierung der Befugnisse dieser Funktion vermissen ließ.

Der RH empfahl daher dem Bundeskanzleramt, im Falle einer Cyber–Krise die Teilnahme der Generalsekretärin bzw. des Generalsekretärs des Bundeskanzleramts – soweit diese Funktion im Bundeskanzleramt eingerichtet ist – an den Sitzungen des Koordinationsausschusses sicherzustellen.

(2) Der RH hielt kritisch fest, dass bei der gegenständlichen Cyber–Krise die notwendige Infrastruktur (Räumlichkeiten) und sonstige Ausstattung (Hardware, Software, Büroausstattung) erst organisiert und beschafft werden mussten, um die Einsatzbereitschaft herstellen zu können. Dazu verwies der RH auf seine Empfehlungen zur Cyber–Sicherheitsleitstelle mit Einsatzzentrale in TZ 26 und zu einem permanenten Lagezentrum in TZ 14.

(3) Der RH wies kritisch darauf hin, dass die von der BRZ GmbH ausgesprochene technische Risikoeinschätzung zu den bundesweiten Systemen Aktenverwaltung (ELAK im Bund), Haushaltsverrechnung (HV–SAP) und Personalmanagement (PM–SAP) nicht mit dem IKDOK bzw. dem Koordinationsausschuss abgestimmt war. Aus Sicht des RH trug nicht nur die fehlende formelle Einbindung des Finanzministeriums in die Strukturen zur Bewältigung der Cyber–Krise, sondern auch das Fehlen übergeordneter Krisen–, Kontinuitäts– und Einsatzpläne (TZ 9, TZ 26) dazu bei, dass die Entscheidung des für die Haushaltsverrechnung verantwortlichen Finanzministeriums – zur Deaktivierung der Benutzerkonten des Außenministeriums – ohne Abstimmung mit dem IKDOK bzw. dem Koordinationsausschuss erfolgte.

Der RH wies in diesem Zusammenhang darauf hin, dass

- das Finanzministerium und das Digitalisierungsministerium jeweils die applikationsverantwortlichen Bundesministerien für wichtige bundesweite Systeme – wie die Haushaltsverrechnung des Bundes und den ELAK im Bund – waren und der BRZ GmbH die Rolle als zentraler IT–Dienstleister des Bundes zukam, und
- § 25 Abs. 2 NISG die allfällig erforderliche Erweiterung des Koordinationsausschusses u.a. um weitere Bundesbehörden und Computer–Notfallteams ermöglichte.

Er hielt daher kritisch fest, dass das Finanzministerium, das Digitalisierungsministerium und die BRZ GmbH im Rahmen ihrer jeweiligen Verantwortung für wichtige bundesweite IT–Systeme nicht bereits ab Feststellung der Cyber–Krise im Koordinationsausschuss eingebunden waren.

Der RH empfahl dem Innenministerium, im Falle einer Cyber–Krise, die Systeme des Bundes bzw. von Bundesministerien betrifft, den Koordinationsausschuss auch um entscheidungsbefugte Vertreterinnen und Vertreter des Finanzministeriums, des Digitalisierungsministeriums und der BRZ GmbH zu erweitern, um eine abgestimmte Vorgangsweise hinsichtlich der wichtigen bundesweiten IT–Systeme zu gewährleisten.

24.3 (1) In seiner Stellungnahme teilte das Bundeskanzleramt mit, dass es die Empfehlung evaluieren werde, im Falle einer Cyber–Krise die Teilnahme der Generalsekretärin bzw. des Generalsekretärs des Bundeskanzleramts an den Sitzungen des Koordinationsausschusses sicherzustellen.

(2) Laut Stellungnahme des Innenministeriums werde die Empfehlung zur Erweiterung des Koordinationsausschusses um entscheidungsbefugte Vertreterinnen und Vertreter im Falle einer neuerlichen Cyber–Krise unter der Evaluierung der konkreten krisenhaften Umstände und ihrer potenziellen Auswirkungen berücksichtigt.

24.4 Der RH entgegnete dem Bundeskanzleramt, dass die Teilnahme der Generalsekretärin bzw. des Generalsekretärs des Bundeskanzleramts an den Sitzungen des Koordinationsausschusses gesetzlich (§ 25 NISG) klar festgelegt ist.

Kosten der Cyber–Krise

25.1 (1) Für die Bewältigung der Cyber–Krise entstanden bei den beteiligten Bundesministerien unmittelbar Aufwendungen, die diese jeweils selbst trugen. Diese in den Bundesministerien nicht eigens unter dem Titel Cyber–Krise dokumentierten, sondern erst vom RH erhobenen Aufwendungen bestanden aus externen Aufwendungen für Beschaffungen sowie aus internen Aufwendungen für Personal– und eventuell weiterem Sachaufwand. Die folgende Tabelle zeigt die vom RH erhobenen Aufwendungen:

Tabelle 12: Aufwendungen im Zuge der Cyber–Krise

Art der Aufwendungen	Außen-ministerium	Innen-ministerium	Verteidigungs-ministerium	Bundeskanzleramt (inklusive GovCERT)
Personalaufwand (in Personenstunden)	2.664	2.644	3.824	1.600
	in EUR			
externer Aufwand/ Beschaffungen	1.690.800	20.547,08	–	–
sonstiger Sachaufwand	4.000	–	–	–
Absicherung eigener IT–Systeme	–	–	37.993,20	50.400

GovCERT = Government Computer Emergency Response Team (Computer–Notfallteam der öffentlichen Verwaltung)

Quellen: BKA; BMI; BMLV; BMEIA

In Summe wendeten die zur Bewältigung der Cyber–Krise tätigen Bundesministerien (einschließlich GovCERT) rd. 10.732 Arbeitsstunden auf, das entsprach rd. 67 Personenmonaten.

(2) Das Außenministerium musste aufgrund der Dringlichkeit und Unvorhersehbarkeit für wichtige fehlende Software und Expertise eine Notfallbeschaffung von rd. 1,69 Mio. EUR durchführen. Diesen Betrag vereinbarte es pauschal mit dem externen Unternehmen B für die Bewältigung der Krise. Die vertraglich vereinbarten Leistungen basierten auf dem bei Vertragsabschluss bestehenden Kenntnisstand über den kompromittierten Zustand der Systeme im Außenministerium. Die vertragliche Vereinbarung sah deswegen auch vor, dass bei massiver Überschreitung der notwendigen Leistungen eine Verpflichtung des externen Unternehmens bestand, das Außenministerium darüber zu informieren und eine einvernehmliche Lösung für die weitere Vorgehensweise zu finden. Wenn allerdings geplante Leistungsstunden nicht verbraucht würden, so könnten diese innerhalb von 18 Monaten – im Sinne einer Gutschrift – für weitere Leistungen verwendet werden. Der Vertrag enthielt für jede Teilleistung eine Aufstellung der geschätzten Leistungsstunden. Die Abnahme der vereinbarten Teilleistungen bzw. Leistungsstunden regelte der Vertrag nicht. Im Außenministerium lagen – abseits der als sachlich und rechnerisch richtig

bestätigten Rechnungen des Auftragnehmers – keine weiteren Leistungs– oder Stundennachweise vor. Das Außenministerium übermittelte dem RH eine von Ende Mai 2021 stammende und damit zur Zeit der Gebarungsüberprüfung erstellte Unterlage des Auftragnehmers, die u.a. Angaben zu den erbrachten Leistungen und den bisherigen Gutschriften enthielt.

Die darüber hinausgehenden Aufwendungen der Cyber–Krise beliefen sich auf 2.664 intern geleistete Personenstunden sowie 4.000 EUR an weiteren Sachaufwendungen. Nicht enthalten waren die aufgrund der Cyber–Krise beschlossenen und nachfolgend durchgeführten technischen Neuerungen der IT–Systeme des Außenministeriums.

(3) Das Innenministerium trug die Aufwendungen für die Grundausstattung der Einsatzstruktur von 20.547,08 EUR sowie der eigenen geleisteten 2.644 Personenstunden.

(4) Das Bundeskanzleramt (inklusive GovCERT) wendete rd. 1.600 Personenstunden für die Cyber–Krise auf. Für die Absicherung der eigenen IT–Systeme beschaffte es Software um 50.400 EUR.

(5) Das Verteidigungsministerium trug die Aufwendungen für den Assistenzeinsatz (beim Innenministerium) selbst. Dafür fielen 3.824 Personenstunden an. Darüber hinaus beschaffte das Verteidigungsministerium Software und Dienstleistungen um 37.993,20 EUR zur Absicherung der eigenen Systeme.

25.2 Der RH hielt fest, dass das für die Bewältigung der Cyber–Krise erforderliche Personal durch das Außenministerium (2.664 Stunden) sowie durch umfassende Unterstützung des Innenministeriums (2.644 Stunden), Assistenzleistung des Verteidigungsministeriums (3.824 Stunden) und des Bundeskanzleramts (inklusive GovCERT, 1.600 Stunden) beigebracht wurde. Darüber hinaus war die rasche Verfügbarkeit des externen Unternehmens B für die Bewältigung der Cyber–Krise erforderlich.

Der RH empfahl dem Bundeskanzleramt, dem Innenministerium, dem Verteidigungsministerium und dem Außenministerium als Mitglieder des IKDOK, in Ergänzung zur Schaffung des permanenten Cyber–Lagezentrums im Innenministerium (TZ 14) auch ein permanent verfügbares Cyber–Einsatzteam (Rapid Response Team) zu schaffen; dies in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam (TZ 28).

Der RH wies darauf hin, dass das Außenministerium im Rahmen der Notfallbeschaffung eine Pauschalpreisgestaltung mit einer zusätzlichen Regelung bei massiver Überschreitung (neuerliche Vereinbarung erforderlich) bzw. Unterschreitung (Gutschrift) der kalkulierten und zugrunde gelegten Leistungen vereinbarte. Er hielt

jedoch kritisch fest, dass der abgeschlossene Vertrag keine Regelungen zur Abnahme der vereinbarten Teilleistungen bzw. Leistungsstunden enthielt und im Außenministerium daher auch keine weiteren Leistungs– oder Stundennachweise vorlagen.

Der RH empfahl daher dem Außenministerium, angepasst an die Erfordernisse eines Krisenfalls beim Abschluss von Verträgen über Hardware, Software und IT–Dienstleistungen ein Verfahren zur Leistungsabnahme zu vereinbaren, Zahlungsverpflichtungen an diese förmlichen Leistungsabnahmen zu knüpfen und diese Leistungsabnahmen auch tatsächlich durchzuführen und zu dokumentieren.

Der RH hielt fest, dass keine zusammenfassende Betrachtung der für die Bewältigung der Cyber–Krise insgesamt angefallenen Kosten vorlag. Damit fehlte eine Grundlage für die Weiterentwicklung des Cyber–Krisenmanagements.

25.3 (1) Das Bundeskanzleramt sagte in seiner Stellungnahme zu, die Bestrebungen zur Schaffung eines permanent verfügbaren Cyber–Einsatzteams des Verteidigungsministeriums zu unterstützen.

(2) In seiner Stellungnahme hielt das Innenministerium fest, dass ein weiterer Aufbau der personellen Kapazitäten im Bereich Cyber–Sicherheit geplant und teilweise bereits in Umsetzung sei. Dieser personelle Aufbau sei die Voraussetzung zur Sicherstellung einer erweiterten Einsatzfähigkeit im Sinne von Rapid Response Teams.

(3) Laut Stellungnahme des Verteidigungsministeriums werde es die Aufstellung eines Rapid Response Teams unterstützen. Im Verteidigungsministerium selbst seien seit Herbst 2020 die Grundlagen für ein eigenes Rapid Response Team, mit Schwergewicht für Einsätze bei den Auslandskontingenten, erarbeitet und die Planungs– und Vorhabensabsicht abgeschlossen worden. Zwei Rapid Response Teams sollten bis Anfang 2023 eine erste Einsatzbereitschaft erreichen (siehe auch TZ 28). In der Vorbereitung auf künftige Cyberkrisenfälle sei ein Beschaffungsprozess zu erarbeiten, der im Anlassfall rasche Beschaffungen von Hard– und Software sowie den Zukauf von IT–Dienstleistungen ermögliche.

(4) Das Außenministerium teilte in seiner Stellungnahme mit, dass die Empfehlung zu Leistungsabnahmen nach Maßgabe der Möglichkeiten berücksichtigt werde.

25.4 (1) Der RH begrüßte den vom Innenministerium geplanten bzw. den schon in Umsetzung befindlichen Aufbau der personellen Kapazitäten im Bereich der Cyber–Sicherheit als Voraussetzung zur Sicherstellung einer erweiterten Einsatzfähigkeit im Sinne von Rapid Response Teams. Er verwies hierzu auf seine Empfehlung in dieser TZ, ein permanent verfügbares Cyber–Einsatzteam in Abstimmung mit jenem des Verteidigungsministeriums zu schaffen.

(2) Der RH entgegnete dem Außenministerium, dass seine Empfehlung betreffend Leistungsabnahmen wesentliche Kriterien für eine zweckmäßige, sparsame und auch rechtmäßige Abwicklung von externen Vergaben beinhaltete. Diese Empfehlung wäre daher jedenfalls umzusetzen und nicht lediglich „nach Maßgabe der Möglichkeiten“ zu berücksichtigen.

Cyber–Krisenmanagement

26.1 (1) Die Cyber–Krise im Außenministerium führte zu einer Nachbetrachtung des Kriseneinsatzes unter Federführung des Bundeskanzleramts. Dieses erstellte im April 2020 den Bericht „Lessons Identified“ mit insgesamt 32 Empfehlungen. Die Empfehlungen betrafen sowohl kurzfristig wie auch mittel– und langfristig umsetzbare Maßnahmen. Ein Teil der Maßnahmen war direkt aus den Erfahrungen bei der Bewältigung der Cyber–Krise ableitbar, ein Teil war bereits vor der Cyber–Krise im Regierungsprogramm 2017–2022 oder in der Cyber–Sicherheitsstrategie aus 2013 vorgesehen.

(2) Im Zusammenhang mit dem zeitlichen Ablauf und den vorhandenen Strukturen zur Bewältigung der Cyber–Krise hielt der Bericht fest, dass die Feiertage und die damit einhergehende reduzierte Belegschaft zu Zeitverzögerungen geführt hätten und dass ein Einsatz eines ständig verfügbaren Einsatzteams (Rapid Response Team)[54] und eines Cyber Security Operations Centers (**SOC**)[55] bereits zu Beginn des Angriffs zu einer rascheren Behebung der Cyber–Krise beigetragen hätte. Dazu wäre auch das Vorhalten einer geeigneten Infrastruktur notwendig, welche durch die Schaffung eines staatlichen Cyber–Sicherheitszentrums[56] – wie auch im Regierungsprogramm 2020–2024 vorgesehen – mitberücksichtigt werden könnte.

26.2 (1) Der RH hielt fest, dass die Cyber–Krise grundsätzlich erfolgreich bewältigt werden konnte. Mit der Feststellung der Cyber–Krise am 4. Jänner 2020 wurden die Krisenmechanismen und Krisenstrukturen aktiviert; unter der Federführung des Innenministeriums übernahm eine Einsatzstruktur – bestehend aus den gebündelten Cyber–Sicherheitskräften der verantwortlichen Bundesministerien (Bundeskanzleramt, Innenministerium, Verteidigungsministerium, Außenministerium) und dem externen Unternehmen B – die operativen Aufgaben zur Bewältigung der Krise.

[54] Ein Rapid Response Team ist 24 Stunden am Tag, sieben Tage die Woche, 365 Tage im Jahr (24/7/365) verfügbar und kann bei Cyber–Vorfällen zeitlich unmittelbar und vor Ort wirksam werden („schnelle Eingreiftruppe“).

[55] Security Operations Center (SOC) ist eine Sicherheitsleitstelle, welche sich um den Schutz der IT–Infrastruktur eines Unternehmens oder einer Organisation kümmert.

[56] Ein Cyber–Sicherheitszentrum bietet Cyber–Einsatzkräften eine vorbereitete Infrastruktur, inklusive netzwerktechnischer Anbindungen an die österreichische Ministerienlandschaft. Es verfügt über ein umfassendes Sicherheitskonzept, IKT–Infrastruktur und über ein Lagezentrum.

Damit konnten aus Sicht des RH die grundsätzlichen personellen und zeitlichen Anforderungen für die Dauer der Krisenbewältigung abgedeckt werden (TZ 25).

Der RH anerkannte, dass das Bundeskanzleramt eine umfassende Nachbetrachtung des Kriseneinsatzes durchführte und der dazu erstellte Bericht auch die Probleme im Zusammenhang mit dem zeitlichen Ablauf und den vorhandenen Strukturen zur Bewältigung der Cyber–Krise aufgriff.

(2) Zusammenfassend hielt der RH in Bezug auf das Cyber–Krisenmanagement fest:

- Der Angreifer wählte als Angriffszeitraum die Weihnachtsfeiertage 2019 und den Jahreswechsel 2019/20 (TZ 24).
- Aus Sicht des RH sind übergeordnete Krisen–, Kontinuitäts– und Einsatzpläne für ein funktionierendes Cyber–Krisenmanagement wesentlich. Diese sollten nicht nur die grundlegende Einsatzstruktur behandeln, sondern auch aufbauend auf den Notfall– und Kontinuitätsplänen der Bundesministerien im Rahmen des staatlichen Krisen– und Katastrophenmanagements eine koordinierte und effiziente Krisenbewältigung sicherstellen. Solche Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement lagen jedoch nicht vor, obwohl die Steuerungsgruppe–CSS die Ausarbeitung solcher Pläne bereits 2014 (und 2019) beschlossen hatte (TZ 9).

  Der RH empfahl dem Innenministerium und dem in der Steuerungsgruppe–CSS vorsitzführenden Bundeskanzleramt, konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement auszuarbeiten.

- Eine Cyber–Krisen–Infrastruktur lag nicht vor; deshalb mussten diese (Räumlichkeiten) und sonstige Ausstattung (Hardware, Software, Büroausstattung) erst unmittelbar in der Cyber–Krise organisiert und beschafft werden, um eine Einsatzbereitschaft herzustellen (TZ 25).

  Der RH verwies daher auf seine Empfehlung in TZ 14, ein permanentes Cyber–Lagezentrum für den IKDOK zu schaffen.

- Ein ständig verfügbares Einsatzteam (Rapid Response Team) stand nicht zur Verfügung.

  Der RH verwies daher auf seine Empfehlung in TZ 25, ein ständig verfügbares Cyber–Einsatzteam (Rapid Response Team) einzurichten.

- Ein Cyber Security Operations Center (SOC) – im Sinne einer staatlichen Cyber–Sicherheitsleitstelle mit Einsatzzentrale und einsatzbereitem Personal – stand nicht zur Verfügung.

Der RH empfahl dem Bundeskanzleramt, dem Innenministerium, dem Verteidigungsministerium und dem Außenministerium als Mitglieder des IKDOK, eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale einzurichten und das Cyber–Einsatzteam (Rapid Response Team) dort zu integrieren.

Darüber hinaus verwies der RH auf seine Empfehlung an das Innenministerium zur Umsetzung des Frühwarnsystems (Sensornetzwerk; TZ 20) und auf seine Empfehlungen an das Verteidigungsministerium zur Erweiterung der Einsatzmöglichkeiten des MilCERT durch ein Cyber–Lagezentrum sowie zur Schaffung eines Cyber–Einsatzteams (Rapid Response Team) des Verteidigungsministeriums mit einer teilweisen Ausrichtung auf die Erbringung von Unterstützungsleistungen für den Bund (TZ 28).

Die genannten Maßnahmen sollen aufeinander abgestimmt in den betreffenden Bundesministerien umgesetzt werden; alternativ können diese Maßnahmen in einem nationalen Cyber–Sicherheitszentrum mit entsprechenden Cyber–Sicherheitsstrukturen unter Nutzung vorhandener interministerieller Synergien (Ressourcen) zusammengefasst werden.

26.3 (1) Das Bundeskanzleramt teilte in seiner Stellungnahme mit, dass es im Rahmen seiner Zuständigkeit als vorsitzführende Stelle in der Steuerungsgruppe–CSS auf die Erarbeitung von Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement gemeinsam mit dem Innenministerium und dem Verteidigungsministerium hinwirken werde.

Die Empfehlung, eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale einzurichten, werde es evaluieren.

(2) Laut Stellungnahme des Innenministeriums sei ein Handbuch zum Umgang mit einer Cyber–Krise anhand der Erfahrungswerte aus der Krise im Außenministerium in Vorbereitung und solle 2022 im Rahmen des IKDOK vorgelegt und konsolidiert werden.

Die Empfehlung zu einer Cyber–Sicherheitsleitstelle solle im Rahmen des geplanten Cyber–Lagezentrums betrachtet werden und in die diesbezüglichen Planungen miteinfließen.

(3) In seiner Stellungnahme sagte das Verteidigungsministerium die Unterstützung der Ausarbeitung von Krisen–, Kontinuitäts– und Einsatzplänen für ein Cyber–Krisenmanagement zu. Aufgrund der Bedeutung dieser Cyber–Sicherheitselemente für die Vorbereitung der Cyber–Landesverteidigung bzw. für den Übergang vom Krisen– in einen Verteidigungsfall solle diese Entwicklung in enger Abstimmung mit dem Verteidigungsministerium erfolgen (siehe auch TZ 28).

Weitere Entwicklung der Cyber–Sicherheit

Personalkapazitäten zur Umsetzung des NISG

27.1 (1) Für die wirkungsorientierte Folgenabschätzung (**WFA**) zum Entwurf des NISG nahmen das Bundeskanzleramt und das Innenministerium 2018 jeweils auch eine Abschätzung der finanziellen und personellen Auswirkungen vor. Sie berücksichtigten dabei auch die notwendigen Personalressourcen für die Einrichtung und den Betrieb der für die Umsetzung des NISG notwendigen neuen Organisationseinheiten. Die folgende Tabelle zeigt diese für die neuen Aufgaben errechneten Personalressourcen und stellt sie den tatsächlich eingesetzten Ressourcen gegenüber:

Tabelle 13: Personalressourcen gemäß wirkungsorientierter Folgenabschätzung (WFA) zum Netz– und Informationssystemsicherheitsgesetz (NISG)

Personalressourcen für die Umsetzung des NISG				
	2019	2020	2021	2022
	in Vollbeschäftigungsäquivalenten (VBÄ)			
Bundeskanzleramt laut WFA	7,00	7,00	7,00	7,00
Bundeskanzleramt tatsächlich	1,70[1]	1,70[1]	1,70[3]	–
Innenministerium laut WFA	26,00	36,00	36,00	36,00
Innenministerium tatsächlich	15,00[2]	16,00[2]	16,00[3]	–

[1] nur bestehendes Personal zum Stand 31. Dezember
[2] bestehendes und neu eingestelltes Personal zum Stand 31. Dezember
[3] Stand Mai 2021

Quellen: BKA; BMI

Der vom Bundeskanzleramt errechnete Bedarf belief sich ab 2019 auf 7 VBÄ[57] (größtenteils Juristinnen und Juristen), der des Innenministeriums auf 26 VBÄ im Jahr 2019 und 36 VBÄ[58] für die Folgejahre (größtenteils IT–Technikerinnen und –Techniker).

Die tatsächlich eingesetzten Personalressourcen für die Umsetzung des NISG und damit auch zur Sicherstellung der Cyber–Sicherheit in den beiden Bundesministerien lagen deutlich unter den 2018 als notwendig festgestellten Werten: im Mai 2021 im Bundeskanzleramt bei 1,7 VBÄ (statt 7), im Innenministerium bei 16 VBÄ (statt 36).

Das Bundeskanzleramt und das Innenministerium hielten dazu fest, dass die zur Zeit der Gebarungsüberprüfung gegebene Ausstattung mit Personalressourcen in den zuständigen Abteilungen für einen optimalen Vollzug des NISG nicht ausreichend war.

57 2 VBÄ Leitung/Stellvertretung, 4 VBÄ Fachreferentinnen bzw. –referenten, 1 VBÄ Teamassistenz

58 2 VBÄ Leitung, 2 VBÄ Exekutivdienst, 30 VBÄ Fachreferentinnen bzw. –referenten, 1 VBÄ juristische Referentin bzw. juristischer Referent, 1 VBÄ Assistenz

(2) Die zwischen 2018 und 2021 geltenden Personalpläne des Bundes räumten dem Bundeskanzleramt (für den gesamten Ressortbereich) die Möglichkeit ein, die im Personalplan festgelegte Anzahl an Planstellen (unabhängig von deren konkreter Wertigkeit) um 65 (im Jahr 2018) bzw. 50 (in den Jahren 2019 bis 2021) zu überschreiten. Dennoch wurden im Bundeskanzleramt die Arbeiten des NIS–Büros lediglich von zwei (1,70 VBÄ) statt – wie in der wirkungsorientierten Folgenabschätzung zum NISG vorgesehen – von sieben Bediensteten erledigt, wodurch sich beispielsweise auch Verzögerungen bei der Feststellung der Betreiber wesentlicher Dienste ergeben hätten (TZ 4).

Das Innenministerium nahm für die Umsetzung des NISG teilweise neues Personal auf, verfügte für diese Aufgabe aber über rd. 20 VBÄ weniger als in der wirkungsorientierten Folgenabschätzung als notwendig definiert. Das Innenministerium betonte, dass die Koordination der Cyber–Sicherheit am Beispiel des IKDOK dennoch bestmöglich erfüllt werde, weil die im NISG festgelegten Aufgaben ergänzend auch von bestehenden Bediensteten der fachzuständigen Abteilung miterledigt würden. Die Umsetzung der im NISG optionalen Funktionen, die durch die Projekte IKDOK–Plattform (TZ 15), Frühwarnsystem (Sensornetzwerk, TZ 20) und Meldeanalysesystem (TZ 21) abgedeckt werden sollen, war jedoch aufgrund des Personalmangels wesentlich verzögert.

Das Innenministerium verwies dazu auch auf die Schwierigkeit, im Bereich der Cyber–Sicherheit spezialisiertes Personal zu rekrutieren. Neben dem Gehaltsschema des Bundes seien auch langwierige Aufnahmeprozesse und mangelnde Möglichkeiten für Quereinsteigende limitierende Elemente. Diese Rahmenbedingungen seien daher für hochqualifizierte IT–Spezialisten der Cyber–Sicherheit kein ausreichender Anreiz.

(3) Im Begutachtungsverfahren zum NISG hatte das damalige Bundesministerium für öffentlichen Dienst und Sport in seiner Stellungnahme festgehalten, dass der in der wirkungsorientierten Folgenabschätzung vom Bundeskanzleramt bzw. vom Innenministerium definierte Personalbedarf durch geeignete personalorganisatorische Maßnahmen jeweils ressortintern auszugleichen ist und es zu keiner personellen Ressourcenvermehrung kommt.

27.2 Der RH stellte fest, dass die in der wirkungsorientierten Folgenabschätzung zur Umsetzung des NISG und damit zur Aufrechterhaltung der Cyber–Sicherheit als notwendig definierten Personalressourcen im Bundeskanzleramt und im Innenministerium im Mai 2021 nicht erreicht wurden. Der Fehlstand an Personal belief sich auf rd. 5 VBÄ bzw. auf rd. 20 VBÄ. Er hielt dazu kritisch fest, dass das Bundeskanzleramt – trotz der in den Personalplänen der Jahre 2018 bis 2021 geregelten Überschreitungsermächtigungen – das dafür notwendige Personal nicht rekrutiert hatte.

Der RH empfahl daher dem Bundeskanzleramt, die für die Aufgabenwahrnehmung erforderlichen Personalressourcen in der Abteilung für Cyber–Sicherheit abzuschätzen und entsprechend sicherzustellen.

Der RH empfahl dem Innenministerium, in Zusammenarbeit mit dem zuständigen Beamtenministerium Rahmenbedingungen im Sinne eines modernen Personalmanagements (Personalrekrutierung, –entwicklung und –bindung) zu schaffen, die es ermöglichen, dass allen mit der Cyber–Sicherheit befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung steht.

Der RH betonte in diesem Zusammenhang, dass die Frage der Cyber–Sicherheit im Rahmen der Erfüllung des NISG nicht nur das jeweilige Bundesministerium betraf, sondern eine zentrale koordinative Aufgabe für die gesamte Bundesverwaltung und die gesamte Infrastruktur (Betreiber wesentlicher Dienste, Anbieter digitaler Dienste, kritische Infrastruktur) der Republik Österreich war. Demzufolge wären die im NISG festgelegten Aufgaben zu erfüllen und dabei auch das dafür notwendige Personal bereitzustellen.

27.3 (1) Laut Stellungnahme des Bundeskanzleramts werde es die Empfehlung des RH zu den Personalressourcen evaluieren.

(2) Das Innenministerium teilte in seiner Stellungnahme mit, dass die Richtverwendungen sowie die Besoldung für die IT–Rollen des Bundes mittlerweile rd. 30 Jahre lang im Einsatz seien. Durch die konstante Weiterentwicklung und die ständig stattfindende Spezialisierung der Berufsbilder und der Karrierepfade innerhalb der IT würden die Richtverwendungen in einigen Rollen nicht mehr den aktuellen Anforderungen entsprechen. Ebenso könnten erst in den letzten Jahren entstandene, aber international übliche IT–Rollen nicht mehr abgebildet werden. Daher seien die Richtverwendungen im Rahmen eines vom Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport geleiteten Projekts modernisiert und erweitert worden. Diese Richtverwendungen seien per 1. Jänner 2022 erlassen worden, so dass noch 2022 eine Umsetzung erwartet werden könne. Mit dieser Maßnahme sollten im öffentlichen Dienst bestehende Personalrekrutierungsprobleme durch ein modernes Personalmanagement gelöst werden können.

27.4 Der RH wies gegenüber dem Bundeskanzleramt und dem Innenministerium darauf hin, dass ein modernes Personalmanagement wesentlich zur Positionierung des Bundes als attraktiver Arbeitgeber für technische oder IT–Berufe beitragen konnte. Aufgrund der zentralen Rolle geeigneten Personals für die Cyber–Sicherheit bekräftigte er seine Empfehlung und wies auf die Notwendigkeit der Umsetzung der per 1. Jänner 2022 neu erlassenen „Richtverwendungen für IT–Sonderverträge des Bundes“ in den einzelnen Ressorts hin.

Verteidigungsministerium

28.1 (1) Das Verteidigungsministerium hatte insbesondere folgende für die Cyber–Sicherheit relevante Aufgaben zu bewältigen:

1. Im Rahmen der militärischen Landesverteidigung war es nach Art. 79 Abs. 1 Bundes–Verfassungsgesetz für die Abwehr von Cyber–Angriffen verantwortlich. Voraussetzung dafür war, dass diese Angriffe

   - gegen militärische Rechtsgüter (Abwehr im Rahmen des Militärbefugnisgesetzes[59], als militärischer Eigenschutz gegen Bedrohungen im Cyber–Raum und im Informationsumfeld) oder
   - gegen Österreich als souveränen Staat gerichtet waren, wobei die Angriffe direkt durch einen anderen Staat oder indirekt durch eine staatlich gelenkte Organisation (z.B. wenn sich ein fremder Staat einer Terrororganisation bedient) ausgeführt wurden (Cyber–Defence–Fall).

2. Gemäß Art. 79 Abs. 2 Z 1 Bundes–Verfassungsgesetz konnte eine Assistenzleistung der Cyber–Ressourcen des Verteidigungsministeriums angefordert und erbracht werden. Die zuständigen Behörden[60] konnten diesen Assistenzeinsatz anfordern, wenn allgemeine Gefahren vorlagen, z.B. für die verfassungsmäßigen Einrichtungen und deren Handlungsfähigkeit sowie für die demokratischen Freiheiten der Bevölkerung oder die Aufrechterhaltung der Ordnung und Sicherheit im Inneren.

   (2) 2021 begann das Verteidigungsministerium wichtige Planungen zur Weiterentwicklung seiner Strukturen und Ressourcen für die Cyber–Abwehr. Dies betraf

   - die Aufstellung eines Rapid Response Teams, welches ein hochverfügbares operatives Element bei Cyber–Vorfällen darstellte und zeitlich unmittelbar und vor Ort wirksam werden sollte,
   - die Schaffung eines Security Operations Centers (SOC), das alle sicherheitsrelevanten Systeme wie Netzwerke, Server oder IT–Services überwachte und analysierte und damit den Schutz der eigenen Einrichtungen, IT–Infrastruktur und IT–Services vor Angriffen und Manipulationen im Cyber–Raum sicherstellen sollte, und
   - ein ressortinternes Cyber–Lagezentrum, das die zur Zeit der Gebarungsüberprüfung bestehenden Organisationselemente zur Erstellung von militärischen Lagebildern um die Cyber–Lage ergänzen sollte.

   (3) Laut Auskunft des Verteidigungsministeriums war die bisherige Strategie der Cyber–Abwehr auf die militärische Landesverteidigung fokussiert. Die aus der

[59] BGBl. I 86/2000 i.d.g.F.

[60] alle Behörden und Organe des Bundes, der Länder und Gemeinden innerhalb ihres jeweiligen Wirkungsbereichs (gemäß § 2 Abs. 5 Wehrgesetz, BGBl. I 146/2001 i.d.g.F.)

Cyber–Krise des Außenministeriums erkennbare notwendige Weiterentwicklung der Cyber–Sicherheits–Koordination des Bundes benötigte auch eine stärkere Einbindung der Ressourcen der Landesverteidigung. Dazu legte das Verteidigungsministerium ein Rechtsgutachten vor, wonach Assistenz– und Unterstützungsleistungen grundsätzlich nicht strukturbegründend sind und damit nicht das Recht einräumen, Personal und Infrastruktur für diese Leistungen vorzuhalten. Dennoch würden die 2021 begonnenen Planungen grundsätzlich auch unter Berücksichtigung der bundesweiten Bestrebungen zur Hebung der Cyber–Sicherheit durchgeführt.

28.2 Der RH erachtete es als zweckmäßig, dass das Verteidigungsministerium Planungen zur Weiterentwicklung seiner Cyber–Abwehr für seine Einsatzkräfte einleitete, die eine schnelle Einsatzbereitschaft durch ein Rapid Response Team sowie ein Cyber–Lagezentrum zum Gegenstand hatten. Weiters bewertete er die Planungen für einen noch umfassenderen Schutz der militärischen IT–Infrastruktur und IT–Services durch ein Security Operations Center positiv.

Er wies darauf hin, dass die bundesweiten Bestrebungen für die Weiterentwicklung der Cyber–Abwehrfähigkeiten – das betraf die Risiko– und Bedrohungsszenarien sowie die entsprechenden Einsatz–, Krisen– und Kontinuitäts– bzw. Notfallpläne (TZ 9, TZ 26) – auch für das Verteidigungsministerium wichtige Informationen für die eigene Planung beinhalteten.

Der RH empfahl dem Verteidigungsministerium, die Planungen sowie die Planungsgrundlagen zur Stärkung der Cyber–Abwehr in Abstimmung mit den und unter Berücksichtigung der Bestrebungen des Bundeskanzleramts und des Innenministeriums zur Stärkung der Cyber–Sicherheit des Bundes durchzuführen.

Er empfahl dem Verteidigungsministerium weiters, sein geplantes Rapid Response Team auch auf die Erbringung von Unterstützungsleistungen für den Bund auszurichten.

28.3 Das Verteidigungsministerium sagte in seiner Stellungnahme die Unterstützung der Ausarbeitung von Krisen–, Kontinuitäts– und Einsatzplänen für ein Cyber–Krisenmanagement zu. Aufgrund der Bedeutung dieser Cyber–Sicherheitselemente für die Vorbereitung der Cyber–Landesverteidigung bzw. für den Übergang vom Krisen– in einen Verteidigungsfall solle diese Entwicklung in enger Abstimmung mit dem Verteidigungsministerium erfolgen (siehe auch TZ 26).

Weiters teilte das Verteidigungsministerium mit, dass seit Herbst 2020 die Grundlagen für ein Rapid Response Team, mit Schwergewicht für Einsätze bei den Auslandskontingenten, erarbeitet und die Planungs– und Vorhabensabsicht abgeschlossen worden seien. Zwei Rapid Response Teams sollten bis Anfang 2023 eine erste Einsatzbereitschaft erreichen.

Einbeziehung der Länder aus Bundessicht

29.1 (1) Das NISG verpflichtete – über den Anwendungsbereich der NIS–Richtlinie hinaus – auch Einrichtungen der öffentlichen Verwaltung des Bundes (insbesondere Bundesministerien) zu Sicherheitsvorkehrungen bei ihren wichtigen Diensten und zur Meldung von Sicherheitsvorfällen (TZ 4).

(2) (a) Die Einrichtungen der Länder waren von den Verpflichtungen des NISG nicht unmittelbar erfasst. Der RH hatte daher bereits im Gesetzesbegutachtungsverfahren zum NISG im Oktober 2018 kritisch angemerkt, dass Einrichtungen der Länder und Gemeinden nicht dem gleichen verpflichtenden Schutzniveau wie die vergleichbaren Einrichtungen des Bundes unterstellt wurden. Die Länder konnten diese Vorschriften für ihren Wirkungsbereich (inklusive Gemeinden) allerdings auf freiwilliger Basis mittels Landesgesetz für anwendbar erklären. Bis Mai 2021 hatte kein Land ein dafür vorgesehenes Landesgesetz erlassen.

(b) Den Ländern waren im NISG keine spezifischen Aufgaben zugeteilt. Das NISG war in unmittelbarer Bundesverwaltung (hauptsächlich durch den Bundeskanzler und den Bundesminister für Inneres) zu vollziehen. Ausgenommen davon war nur die Durchführung von Verwaltungsstrafverfahren gegen Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste, die den Bezirksverwaltungsbehörden in mittelbarer Bundesverwaltung oblag.

(c) Meldungen von Vorfällen konnten die Einrichtungen der Länder als freiwillige Meldungen im Sinne des NISG erstatten. Nach einer Auswertung der operativen NIS–Behörde im Innenministerium stammten 2019 und 2020 insgesamt drei (freiwillige) Meldungen über Cyber–Vorfälle von Einrichtungen der Länder.

(d) Der Vorschlag der Europäischen Kommission von Dezember 2020 zur Weiterentwicklung der NIS–Richtlinie sah noch vor, dass öffentliche Einrichtungen bis zur Länderebene als eigener Sektor künftig in die nationalen NIS–Regelungen einbezogen werden sollen (TZ 30). Der Rat der Europäischen Union beschränkte dies jedoch im laufenden Gesetzgebungsverfahren wiederum auf öffentliche Einrichtungen auf Ebene der Zentralregierungen.[61]

[61] Allgemeine Ausrichtung des Rates der Europäischen Union, Pressemitteilung vom 3. Dezember 2021

(3) Strategische Koordinierung

- Für die strategische Koordinierung ermöglichte die Geschäftsordnung der Steuerungsgruppe–CSS die Anwesenheit von Ländervertreterinnen und –vertretern je nach zu behandelndem Thema. Die Einberufung oblag dem Bundeskanzleramt. Bis zur Gebarungsüberprüfung fanden fünf von 14 Sitzungen unter Beteiligung von Ländervertreterinnen und –vertretern statt.
- Auch der Koordinationsausschuss konnte im Rahmen einer Cyber–Krise um Ländervertreterinnen und –vertreter erweitert werden. Dies war nach Auskunft der NIS–Behörden bis Mai 2021 nicht relevant geworden.

(4) Operative Koordinierung

- In den operativen Koordinierungsgremien IKDOK und OpKoord waren die Länder grundsätzlich nicht als Teilnehmer vorgesehen. Auch waren sie bis Mai 2021 nicht als Empfänger des OpKoord–Lagebildes eingerichtet. Im Bedarfsfall konnten sie als Träger einer Einrichtung der öffentlichen Verwaltung, die von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen war, der OpKoord beigezogen werden. Einen entsprechenden Bedarfsfall gab es bis Mai 2021 nicht.
- Die Computer–Notfallteams des NISG (CERT.at, GovCERT, allenfalls Austrian Energy CERT) konnten ihre Aufgaben (insbesondere Informationsaussendungen, Warnungen und Lagebeurteilung) auch gegenüber nicht vom NISG erfassten Einrichtungen, wie solchen der Länder, die sich den Verpflichtungen des NISG nicht unterwarfen, wahrnehmen (§ 14 Abs. 6 NISG). Sieben Länder (Burgenland, Niederösterreich, Oberösterreich, Salzburg, Tirol, Vorarlberg und Wien) sowie einige Städte nahmen an der Informationsdrehscheibe des GovCERT teil, Kärnten und die Steiermark nicht.
- Weiters stand es den Ländern offen, mit ihren eigenen Computer–Notfallteams am vom Bundeskanzleramt koordinierten CERT–Verbund als Mitglied teilzunehmen. Zur Zeit der Gebarungsüberprüfung machte davon nur die Stadt Wien Gebrauch.

29.2 Der RH stellte kritisch fest, dass die Länder weder in die strategische noch in die operative Koordination der Cyber–Sicherheit regelmäßig eingebunden waren:

- Sie waren weder als Teilnehmer in den operativen Koordinierungsgremien IKDOK und OpKoord vorgesehen noch waren alle Länder Teilnehmer an der Informationsdrehscheibe des GovCERT oder des CERT–Verbunds. Zur verstärkten Teilnahme der Länder an der Steuerungsgruppe–CSS, der OpKoord sowie am Computer–Notfallteam der öffentlichen Verwaltung GovCERT verwies der RH auf seine Empfehlungen in TZ 9, TZ 13, TZ 15 und TZ 19.
- Mangels entsprechender landesgesetzlicher Regelungen waren die Einrichtungen der Länder und Gemeinden nicht dem gleichen verpflichtenden Schutzniveau wie die vergleichbaren Einrichtungen des Bundes unterstellt.

Der RH empfahl dem Bundeskanzleramt als strategischem Koordinator der Cyber–Sicherheit, auf eine wirksame Einbeziehung der Länder in die gesetzlichen Verpflichtungen zur Netz– und Informationssystemsicherheit hinzuwirken.

29.3 Das Bundeskanzleramt teilte in seiner Stellungnahme mit, die rechtlichen Möglichkeiten zur Umsetzung der Empfehlung zu prüfen.

Weitere Entwicklungen

30.1 Im Dezember 2020 legte die Europäische Kommission eine neue Cybersicherheitsstrategie sowie einen Vorschlag für eine Weiterentwicklung der NIS–Richtlinie[62] vor. Im Dezember 2021 erstattete der Rat der Europäischen Union dazu eine abändernde Stellungnahme.[63] Folgende wesentliche Änderungen der NIS–Richtlinie wurden u.a. angestrebt:

- Ausweitung der einbezogenen Sektoren und Subsektoren, z.B. auf die Sektoren Abwasser, Post, Lebensmittel, Abfall, Vertrauensdiensteanbieter, Einrichtungen der öffentlichen Verwaltung auf Ebene der Zentralregierungen,
- Verpflichtung zur Annahme eines nationalen Krisenmanagementplans,
- rechtliche Grundlage für das europäische Netzwerk der Verbindungsorganisationen für Cyber–Krisen (EU–CyCLONe),
- Entfall der Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste sowie Entfall der generellen Pflicht zur Ermittlung der Betreiber wesentlicher Dienste, stattdessen einheitliche Sicherheitsvorkehrungen und Meldepflichten für die erfassten wesentlichen und wichtigen Einrichtungen,
- regelmäßige behördliche Überprüfungen bei wesentlichen Einrichtungen (darunter fielen auch die bisherigen Betreiber wesentlicher Dienste) und Ex–post–Kontrolle im Anlassfall bei wichtigen Einrichtungen (darunter fielen auch die bisherigen Anbieter digitaler Dienste),
- Pflicht der verantwortlichen Führungskräfte zur Genehmigung der Maßnahmen des Risikomanagements und zu Trainings.

Bis zur Annahme der neuen Richtlinie durch den Europäischen Rat und das Europäische Parlament sind im Zuge der Verhandlungen der Mitgliedstaaten jedenfalls kleinere, aber auch umfangreichere inhaltliche Änderungen möglich.

[62] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, SEC(2020) 430 final. Parallel dazu legte die Europäische Kommission auch einen Vorschlag für eine Richtlinie über die Resilienz Kritischer Infrastrukturen vor, SEC(2020) 433 final.

[63] Allgemeine Ausrichtung des Rates der Europäischen Union, Pressemitteilung vom 3. Dezember 2021

30.2 Der RH sah im Vorschlag der Europäischen Kommission für die Weiterentwicklung der NIS–Richtlinie ein wichtiges Potenzial zur Erhöhung der Cyber–Sicherheit. Die nationale Umsetzung dieser Vorschläge würde aufgrund der Erweiterung der zu berücksichtigenden Sektoren – zusätzlich Einrichtungen z.B. aus den Sektoren Abwasser, Post, Lebensmittel, Abfall und Vertrauensdiensteanbieter – eine Vervielfachung der zu betreuenden und auch zu beaufsichtigenden Einrichtungen mit sich bringen. Dies wäre nach Ansicht des RH für die damit betrauten Institutionen – das waren die operative NIS–Behörde im Innenministerium, das GovCERT und der IKDOK – mit den bestehenden Strukturen aufgrund fehlender Personalressourcen nicht bewältigbar. Der RH verwies hierzu auf seine Empfehlungen zur

- Evaluierung der Aufgaben der OpKoord und zu einer geeigneten Integration des Digitalisierungsministeriums und der Länder in TZ 13,
- Schaffung eines eigenen Cyber–Lagezentrums in TZ 14,
- Schaffung eines Rapid Response Teams in TZ 25 und
- Evaluierung der Fragestellung, ob die Aufgaben des Computer–Notfallteams langfristig durch Bedienstete des Bundes zu erbringen sind, in TZ 19.

Alternativ können diese Organisationen (IKDOK, OpKoord, Cyber–Lagezentrum, Rapid Response Team und Computer–Notfallteam der öffentlichen Verwaltung) in einem nationalen Cyber–Sicherheitszentrum zusammengeführt werden.

Schlussempfehlungen

31 Zusammenfassend empfahl der RH:

Bundeskanzleramt (**BKA**)
Bundesministerium für Inneres (**BMI**)
Bundesministerium für Landesverteidigung (**BMLV**)
Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**)

		BKA	BMI	BMLV	BMEIA
(1)	Das Bundeskanzleramt als Koordinator der Strategie sollte die Aktualisierung der Österreichischen Strategie für Cyber Sicherheit ehestmöglich vorantreiben, insbesondere die politische Abstimmung des Fachentwurfs abschließen und die Beschlussfassung durch die Bundesregierung vorbereiten. Da einerseits aufgrund der sich rasch ändernden faktischen Gegebenheiten und andererseits aufgrund europäischer Vorgaben auch in naher Zukunft Änderungsbedarf zu erwarten ist, wäre es zweckmäßig, darin auch flexible Instrumente und vereinfachte Adaptierungen vorzusehen. (TZ 3)	X			
(2)	In Zusammenarbeit mit dem Bundesministerium für Inneres wäre den operativen Gremien Innerer Kreis der Operativen Koordinierungsstruktur (**IKDOK**) und Computer–Notfallteam der öffentlichen Verwaltung (**GovCERT**) ein Gesamtüberblick der wichtigen Dienste des Bundes zur Kenntnis zu bringen; dieser wäre in den Krisen–, Kontinuitäts– und Einsatzplänen für das Cyber–Krisenmanagement zu berücksichtigen. (TZ 4)	X	X		
(3)	Die von den Bundesministerien getroffenen Sicherheitsvorkehrungen insbesondere betreffend die wichtigen Dienste wären regelmäßig, vergleichbar mit den Vorschriften des Netz– und Informationssystemsicherheitsgesetzes für die Betreiber wesentlicher Dienste, zumindest alle drei Jahre zu auditieren. (TZ 4)	X	X	X	X
(4)	Im Gremium Operative Koordinierungsstruktur (**OpKoord**) wären auch die übrigen Bundesministerien und die Länder auf die Bedeutung der regelmäßigen Sicherheitsüberprüfung ihrer wichtigen Dienste hinzuweisen. (TZ 4)	X	X	X	X
(5)	Für die Angaben zur Wirkungsorientierung wären aussagekräftigere Kennzahlen im Hinblick auf die Kernaufgaben bei der Koordination der Cyber–Sicherheit auszuwählen. (TZ 5)		X		

Bundeskanzleramt (**BKA**)
Bundesministerium für Inneres (**BMI**)
Bundesministerium für Landesverteidigung (**BMLV**)
Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**)

		BKA	BMI	BMLV	BMEIA
(6)	Die Aufgaben bei der Koordination der Cyber–Sicherheit wären in den Angaben zur Wirkungsorientierung abzubilden. (TZ 5)				X
(7)	Im Rahmen der Aufgaben der strategischen Koordination der Cyber–Sicherheit wäre verstärkt auf die ressortübergreifende Abstimmung bei den Angaben zur Wirkungsorientierung, die das Querschnittsthema Cyber–Sicherheit betreffen, hinzuwirken. (TZ 5)	X			
(8)	Das Bundeskanzleramt sollte als für die zentrale Koordination in Angelegenheiten der Cyber–Sicherheit zuständiges Bundesministerium der Bundesregierung weitere Beschlüsse bzw. Projekte zur Umsetzung der im Regierungsprogramm 2020–2024 angeführten Schwerpunkte zur Cyber–Sicherheit vorbereiten. Dabei wären insbesondere die regelmäßigen Berichte der Cyber Sicherheit Steuerungsgruppe zu beachten. (TZ 8)	X			
(9)	Es wäre(n) – die Cyber Sicherheit Steuerungsgruppe – wie in ihrer Geschäftsordnung vorgesehen – mindestens zweimal im Jahr einzuberufen, – das Bundesministerium für Digitalisierung und Wirtschaftsstandort und die Länder zu diesen Sitzungen einzuladen und – sicherzustellen, dass regelmäßige Berichte zur Cyber–Sicherheit an die Bundesregierung erfolgen, insbesondere zur Umsetzung und Weiterentwicklung ihrer strategischen Vorgaben sowie der rechtlichen Grundlagen zu Cyber–Sicherheit. (TZ 9)	X			
(10)	Ein gesamtstaatliches Cyber–Übungsprogramm wäre zu etablieren, um einen Überblick über die vergangenen und geplanten Übungsaktivitäten in Österreich zu erhalten und ein auf nationaler Ebene abgestimmtes Vorgehen zu ermöglichen. (TZ 9)	X			
(11)	Als das in der Cyber Sicherheit Steuerungsgruppe vorsitzführende Bundesministerium sollte das Bundeskanzleramt ein Austauschprogramm für Cyber–Sicherheits–Expertinnen und –Experten aus der staatlichen Verwaltung, der Privatwirtschaft und der Wissenschaft erarbeiten. (TZ 10)	X			

Bundeskanzleramt (**BKA**)
Bundesministerium für Inneres (**BMI**)
Bundesministerium für Landesverteidigung (**BMLV**)
Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**)

		BKA	BMI	BMLV	BMEIA
(12)	Die Aufgaben der OpKoord wären zu evaluieren und das Bundesministerium für Digitalisierung und Wirtschaftsstandort sowie die Länder auf geeignete Weise zu integrieren. Hierbei wäre auch festzulegen, ob die OpKoord regelmäßig oder nur im Bedarfsfall einzuberufen wäre. (TZ 13)	X	X	X	X
(13)	Ein Cyber–Lagezentrum wäre mit der für die Zwecke der Erfüllung der Aufgaben erforderlichen Infrastruktur unter Beachtung von Kosten–Nutzen–Aspekten einzurichten und dem IKDOK (und der OpKoord) zur Verfügung zu stellen. Dieses sollte aufgrund der dem Bundesminister für Inneres zukommenden Leitungsaufgaben im IKDOK (und der OpKoord) beim Bundesministerium für Inneres eingerichtet werden. (TZ 14)		X		
(14)	Die Funktionalität der Geschäftsstelle des IKDOK und der OpKoord für die Protokollerstellung wäre sicherzustellen. (TZ 14)		X		
(15)	Eine Geschäftsordnung für das Zusammenwirken der Koordinierungsstrukturen (IKDOK und OpKoord) wäre gemäß der gesetzlichen Ermächtigung in § 7 Abs. 3 Netz– und Informationssystemsicherheitsgesetz aufgrund der hohen Bedeutung dieser Strukturen für die Cyber–Sicherheit in Österreich zu erlassen. In dieser sollte jedenfalls auch der Prozess zur Erstellung des Lagebildes festgelegt werden. (TZ 14)		X		
(16)	Die im Aufbau befindliche „IKDOK–Plattform“ wäre fertigzustellen, zur Lagebilderstellung einzusetzen und auch für eine gesicherte Kommunikation technisch auszugestalten. (TZ 15)		X		
(17)	Es wäre zu prüfen, ob das jeweils aktuelle Cyber–Lagebild (in Form des OpKoord–Lagebildes) auch den verfassungsmäßigen Einrichtungen der Länder zur Kenntnis gebracht werden kann. (TZ 15)		X		
(18)	Das Bundesministerium für Inneres sollte als Vertreter Österreichs beim Aufbau des neuen EU–weiten Netzwerks CyCLONe mitwirken. (TZ 17)		X		
(19)	Es wäre in Erwägung zu ziehen, die Aufgaben des Computer–Notfallteams der öffentlichen Verwaltung langfristig durch eigene Bedienstete des Bundes zu erbringen. (TZ 19)	X			

Bundeskanzleramt (**BKA**)
Bundesministerium für Inneres (**BMI**)
Bundesministerium für Landesverteidigung (**BMLV**)
Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**)

		BKA	BMI	BMLV	BMEIA
(20)	Jene Leistungen, welche das mit der Erbringung der operativen Leistungen des Computer–Notfallteams für die öffentliche Verwaltung (GovCERT) beauftragte Unternehmen im Rahmen der Behandlung eines Sicherheitsvorfalls zu erbringen hat, wären im Rahmen eines allfälligen nächsten diesbezüglichen Vergabeverfahrens im Sinne des gesetzlichen Auftrags („erste allgemeine Unterstützung“) für alle Dienststellen des Bundes zu definieren. (TZ 19)	X			
(21)	Eine Initiative wäre zu starten, um alle Länder sowie weitere Städte bzw. Gemeinden als Teilnehmer an der Informationsdrehscheibe des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) zu integrieren. (TZ 19)	X			
(22)	Das Projekt zur Implementierung des Frühwarnsystems (Sensornetzwerk) wäre verstärkt zu betreiben und umzusetzen. Im Sinne des gesamtstaatlichen und sektorübergreifenden Ziels, Cyber–Angriffe zu erkennen bzw. deren Auswirkungen so gering wie möglich zu halten sowie Muster und Vorgehensweisen bei Cyber–Angriffen zu analysieren, sollten möglichst viele Organisationen an diesem Frühwarnsystem (Sensornetzwerk) teilnehmen, um dadurch eine großflächige Abdeckung der Risiken zu erreichen. (TZ 20)		X		
(23)	Das Meldesammelsystem wäre rasch umzusetzen; die Erfahrungen aus dem Betrieb sollen dafür genutzt werden, die im Netz– und Informationssystemsicherheitsgesetz vorgesehene IKT–Lösung für ein NIS–Meldeanalysesystem umzusetzen. (TZ 21)		X		
(24)	Es wäre eine standardisierte Taxonomie zur Klassifizierung von Sicherheitsvorfällen für die operative NIS–Behörde, unter Berücksichtigung einheitlich abgestimmter europäischer Lösungen für den Behördenbereich, einzurichten. (TZ 22)		X		
(25)	Im Rahmen des IKDOK sollte eine Empfehlung für eine einheitliche Taxonomie für österreichische Computer–Notfallteams unter Bezug auf europäische Lösungen ausgearbeitet werden. Diese sollte bestmöglich auf die Taxonomie der NIS–Behörde im Bundesministerium für Inneres abgestimmt sein, um so den Meldeprozess zu optimieren. Das Ergebnis wäre im Wege der OpKoord bzw. des CERT.at den in Österreich tätigen Computer–Notfallteams bekannt zu geben. (TZ 22)	X	X	X	X

Bundeskanzleramt (**BKA**)
Bundesministerium für Inneres (**BMI**)
Bundesministerium für Landesverteidigung (**BMLV**)
Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**)

		BKA	BMI	BMLV	BMEIA
(26)	In der Vorfalldokumentation wären jedenfalls klare Kriterien zur Befassung weiterer Gremien wie IKDOK bzw. OpKoord festzulegen sowie zu evaluieren, ob auch Informationen zur Dauer des Vorfalls und zum geleisteten Aufwand ergänzt werden sollten. (TZ 22)		X		
(27)	Im Rahmen des IKDOK wären vorbeugende Maßnahmen für die noch bestehenden Risiken von mit Schadsoftware infizierten externen Groupware– und E–Mail–Servern zu evaluieren. (TZ 23)	X	X	X	X
(28)	Im Falle einer Cyber–Krise wäre die Teilnahme der Generalsekretärin bzw. des Generalsekretärs des Bundeskanzleramts – soweit diese Funktion im Bundeskanzleramt eingerichtet ist – an den Sitzungen des Cyberkrisenmanagement–Koordinationsausschusses sicherzustellen. (TZ 24)	X			
(29)	Im Falle einer Cyber–Krise, die Systeme des Bundes bzw. von Bundesministerien betrifft, wäre der Cyberkrisenmanagement–Koordinationsausschuss auch um entscheidungsbefugte Vertreterinnen und Vertreter des Bundesministeriums für Finanzen, des Bundesministeriums für Digitalisierung und Wirtschaftsstandort und der Bundesrechenzentrum Gesellschaft mit beschränkter Haftung zu erweitern, um eine abgestimmte Vorgangsweise hinsichtlich der wichtigen bundesweiten IT–Systeme zu gewährleisten. (TZ 24)		X		
(30)	Ein permanent verfügbares Cyber–Einsatzteam (Rapid Response Team) wäre zu schaffen; dies in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam. (TZ 25)	X	X	X	X
(31)	Angepasst an die Erfordernisse eines Krisenfalls wäre beim Abschluss von Verträgen über Hardware, Software und IT–Dienstleistungen ein Verfahren zur Leistungsabnahme zu vereinbaren, Zahlungsverpflichtungen an diese förmlichen Leistungsabnahmen zu knüpfen und diese Leistungsabnahmen auch tatsächlich durchzuführen und zu dokumentieren. (TZ 25)				X
(32)	Es wären konkrete Krisen–, Kontinuitäts– und Einsatzpläne für das Cyber–Krisenmanagement auszuarbeiten. (TZ 26)	X	X		

Bundeskanzleramt (**BKA**)
Bundesministerium für Inneres (**BMI**)
Bundesministerium für Landesverteidigung (**BMLV**)
Bundesministerium für europäische und internationale Angelegenheiten (**BMEIA**)

		BKA	BMI	BMLV	BMEIA
(33)	Eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale wäre einzurichten und das Cyber–Einsatzteam (Rapid Response Team) dort zu integrieren. (TZ 26)	X	X	X	X
(34)	Die für die Aufgabenwahrnehmung erforderlichen Personalressourcen in der Abteilung für Cyber–Sicherheit wären abzuschätzen und entsprechend sicherzustellen. (TZ 27)	X			
(35)	In Zusammenarbeit mit dem zuständigen Beamtenministerium wären Rahmenbedingungen im Sinne eines modernen Personalmanagements (Personalrekrutierung, –entwicklung und –bindung) zu schaffen, die es ermöglichen, dass allen mit der Cyber–Sicherheit befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung steht. (TZ 27)		X		
(36)	Die Planungen sowie die Planungsgrundlagen zur Stärkung der Cyber–Abwehr wären in Abstimmung mit den und unter Berücksichtigung der Bestrebungen des Bundeskanzleramts und des Bundesministeriums für Inneres zur Stärkung der Cyber–Sicherheit des Bundes durchzuführen. (TZ 28)			X	
(37)	Das geplante Rapid Response Team sollte auch auf die Erbringung von Unterstützungsleistungen für den Bund ausgerichtet werden. (TZ 28)			X	
(38)	Im Rahmen der Aufgaben der strategischen Koordination der Cyber–Sicherheit wäre auf eine wirksame Einbeziehung der Länder in die gesetzlichen Verpflichtungen zur Netz– und Informationssystemsicherheit hinzuwirken. (TZ 29)	X			

Rechnungshof Österreich

Wien, im XXXXXX 2022
Die Präsidentin:

Dr. Margit Kraker

Anhang A

Verzeichnis der Rechtsgrundlagen

in alphabetischer Reihenfolge

vom RH verwendete (Kurz–)Bezeichnung	Bezeichnung Langfassung mit Angabe der Fundstelle
Börsegesetz 2018	Bundesgesetz über die Wertpapier– und allgemeinen Warenbörsen 2018 (BörseG 2018), BGBl. I 107/2017 i.d.g.F.
EECC–Richtlinie	Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl. L 2018/321, 36
eIDAS–Verordnung	Verordnung (EU) 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 2014/257, 73
Finanzmarktrichtlinie 2	Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU, ABl. L 2014/173, 349 i.d.g.F.
NIS–Durchführungsverordnung	Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Jänner 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz– und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, ABl. L 2018/26, 48
NISG	Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz– und Informationssystemen (Netz– und Informationssystemsicherheitsgesetz – NISG), BGBl. I 111/2018 i.d.g.F.
NIS–Richtlinie	Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen in der Union, ABl. L 2016/194, 1
NISV	Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie Sicherheitsvorfällen nach dem Netz– und Informationssystemsicherheitsgesetz (Netz– und Informationssystemsicherheitsverordnung – NISV), BGBl. II 215/2019 i.d.g.F.
Telekommunikationsgesetz 2003	Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I 70/2003 i.d.g.F.
Telekommunikationsgesetz 2021	Telekommunikationsgesetz 2021, BGBl. I 190/2021 (TKG 2021)
Telekom–Netzsicherheits-verordnung 2020	Verordnung der Rundfunk und Telekom Regulierungs–GmbH (RTR–GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G–Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen (TK–NSiV 2020), BGBl. II 301/2020 i.d.g.F.
Telekom–Rahmenrichtlinie	Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste (Rahmenrichtlinie), ABl. L 2002/108, 33 i.d.g.F.
Verordnung über qualifizierte Stellen	Verordnung des Bundesministers für Inneres zur Festlegung der Erfordernisse und besonderer Kriterien für qualifizierte Stellen nach dem Netz– und Informationssystemsicherheitsgesetz (Verordnung über qualifizierte Stellen – QuaSteV), BGBl. II 226/2019 i.d.g.F.
Zahlungsdienstegesetz 2018	Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (ZaDiG 2018), BGBl. I 17/2018 i.d.g.F.
Zahlungsdiensterichtlinie 2	Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl. L 2015/337, 35 i.d.g.F.

Quellen: bezughabende Rechtsquellen; RH

Anhang B

Berührungspunkte mit anderen Rechtsgrundlagen

(1) Die unmittelbar anwendbare Datenschutz–Grundverordnung (**DSGVO**)[64] enthält Verpflichtungen zu technischen und organisatorischen Sicherheitsvorkehrungen betreffend den Schutz von personenbezogenen Daten. Anknüpfungspunkt zu verpflichtenden Meldungen an die Datenschutzbehörde ist die Verletzung des Schutzes personenbezogener Daten.

(2) Anknüpfungspunkt der Meldeplichten nach dem NISG ist dagegen bereits eine Störung der Verfügbarkeit von Netz– und Informationssystemen mit erheblichen Auswirkungen (Sicherheitsvorfall).

(3) Verantwortliche und Auftragsverarbeiter im Sinne der DSGVO, die gleichzeitig Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste im Sinne des NISG sind, hatten daher die Verpflichtungen nach der DSGVO unabhängig von und allenfalls parallel zu den Verpflichtungen aus dem NISG zu erfüllen, wenn infolge eines Sicherheitsvorfalls nach dem NISG auch der Schutz personenbezogener Daten nach der DSGVO verletzt wurde.

(4) Die aus dem NISG verpflichteten Betreiber wesentlicher Dienste waren zum Teil auch Betreiber einer kritischen Infrastruktur im Sinne des Sicherheitspolizeigesetzes.[65] Aber nicht alle kritischen Infrastrukturen stellten einen wesentlichen Dienst im Sinne des NISG dar, weil dieser in bestimmten Sektoren und abhängig von Netz– und Informationssystemen erbracht werden musste.

Im Bereich des Schutzes kritischer Infrastrukturen gab es insbesondere aufgrund des dafür vorgesehenen Schutzes der physischen Sicherheit eigene

- Vorgaben (z.B. Richtlinie der EU über kritische Infrastrukturen),
- Rechtsgrundlagen (z.B. Schutz vor gefährlichen Angriffen nach dem Sicherheitspolizeigesetz bzw. Schutz vor verfassungsgefährdenden Angriffen nach dem Polizeilichen Staatsschutzgesetz[66], Strafverfolgung nach der Strafprozessordnung[67]),

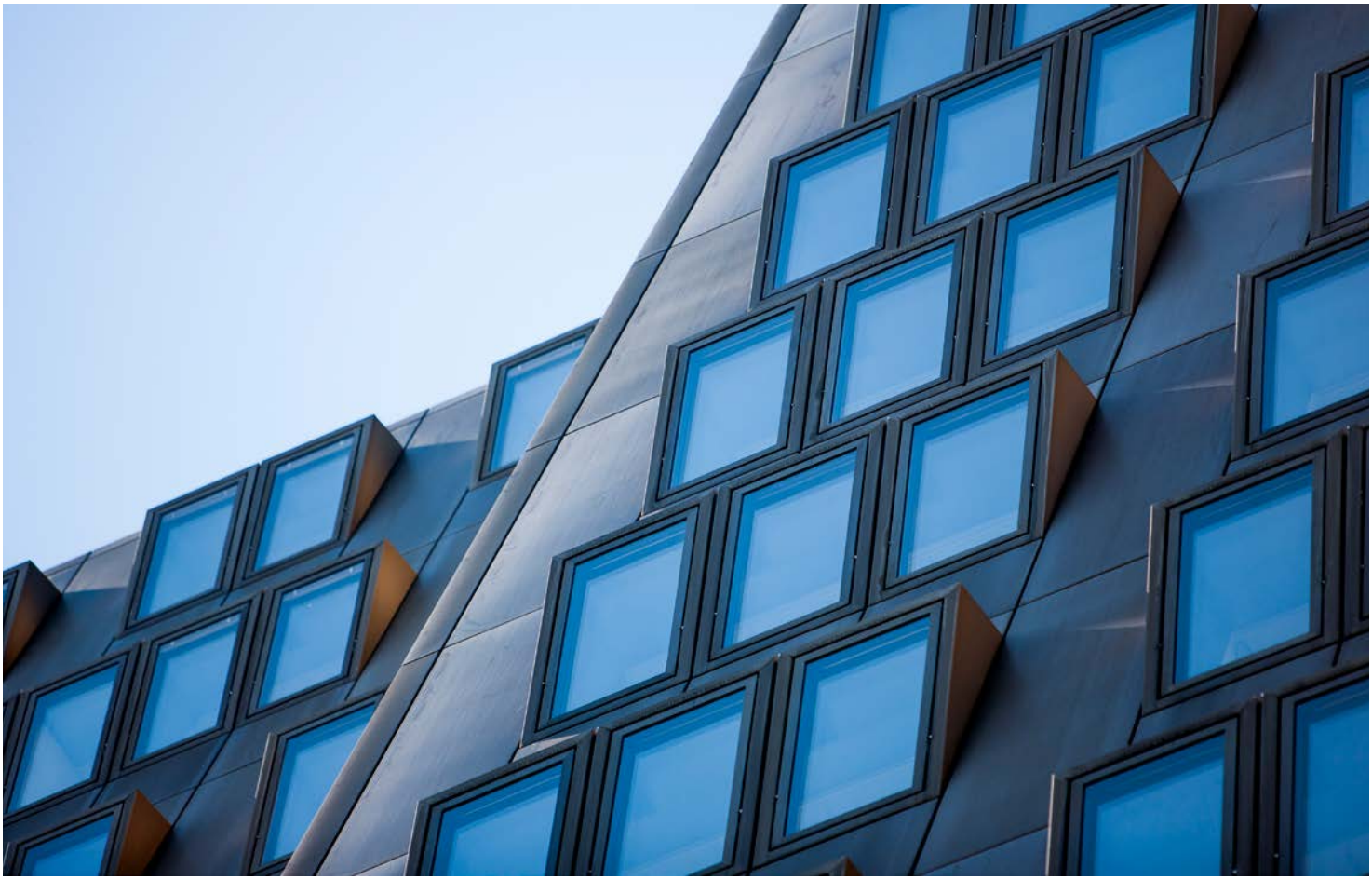
[64] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 2016/119, 1 (insbesondere Art. 32, 33)

[65] § 22 Abs. 1 Z 6 Sicherheitspolizeigesetz definiert die kritische Infrastruktur als „Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations– und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben".

[66] BGBl. I 5/2016 i.d.g.F. (ab Dezember 2021: Staatsschutz– und Nachrichtendienst–Gesetz)

[67] BGBl. 631/1975 i.d.g.F.

- staatliche Initiativen (z.B. Masterplan Österreichisches Programm zum Schutz kritischer Infrastrukturen – APCIP 2014),
- behördliche Einrichtungen (z.B. Koordinierungsstelle für freiwillige Meldungen im Bundesministerium für Inneres, Informationsplattform CIWIN für Betroffene) und
- Maßnahmen (z.B. Objektschutz nach Sicherheitspolizeigesetz, Sicherheitsberatungen, eigene Lagebilder).



REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-04-22T09:19:29+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	