BUNDES
RECHNUNGS
HOF

Prüfungsschwerpunkt

Resilienz der staatlichen Kernfunktionen und ihrer kritischen Infrastruktur

→ *Staat und Verwaltung*

Bericht nach § 88 Absatz 2 BHO
an den Haushaltsausschuss des Deutschen Bundestages

Cybersicherheit

Weichenstellungen für einen sicheren Cyberraum

2. Juli 2025

Geschäftszeichen: VII 4 - 0000583/IV VS-NfD

Dieser Bericht enthält das vom Bundesrechnungshof abschließend im Sinne des § 96 Absatz 4 BHO festgestellte Prüfungsergebnis.

Auf einen Blick

Cybersicherheit bedarf Steuerung und Struktur

Die Informationstechnik (IT) des Bundes ist nicht bedarfsgerecht geschützt. Haushaltsmittel alleine schaffen keine Cybersicherheit. Die Bundesregierung muss die Cybersicherheitsstrategie neu ausrichten, Cybermaßnahmen zentral steuern und die Cybersicherheitsarchitektur reformieren. Dafür benötigt sie überprüfbare Ziele und ein wirksames Controlling. Die Bundesregierung muss ermitteln, was nachgewiesen der Cybersicherheit dient. Nur dies darf sie finanzieren.

→ Worum geht es?

Die Bundesregierung steuert die Cybersicherheit bisher nicht ausreichend. Ihrer Cybersicherheitsstrategie lag keine Analyse der Defizite zugrunde. Die strategischen Ziele hat sie nicht priorisiert. Die Cybersicherheitsarchitektur zeichnet sich durch einen Dschungel von Institutionen und Zuständigkeiten aus. Die IT des Bundes ist nicht auf die aktuellen Bedrohungen vorbereitet. Der Gesetzgeber hat finanzielle Spielräume eröffnet, indem Ausgaben zum Schutz der IT die Verschuldungsmöglichkeiten des Bundes erhöhen können. Die Bundesregierung hat aber noch nicht festgelegt und nachgewiesen, was der Cybersicherheit dient. So wird ein Mehr an Geld kein Mehr an Sicherheit bewirken.

→ Was ist zu tun?

Die Bundesregierung muss ihre strategischen Cybersicherheitsziele so definieren und priorisieren, dass diese überprüfbar und erreichbar sind. Sie muss ein striktes Controlling etablieren und Cybersicherheit steuern. Sie muss prüfen, wie wirksam die Cybersicherheitsarchitektur bei extremen, aber möglichen Krisenszenarien agiert. Erforderlichenfalls muss sie diese reformieren. Die IT des Bundes muss sie so schützen, dass der Staat auch in Krisenfällen handlungsfähig bleibt. Sie muss vorgeben, was unter den Schutz der IT fällt, damit die Verschuldungsmöglichkeiten sachgerecht ermittelt werden.

→ Was ist das Ziel?

Die Bundesregierung hat sich im Cyberraum strategisch neu aufgestellt, die Cybersicherheitsarchitektur geprüft und reformiert und ein wirksames Controlling aufgebaut. Die IT des Bundes ist so abgesichert, dass sie ihre IT-Dienste auch im Krisenfall bedarfsgerecht erbringen kann. Die Bundesregierung hat definiert, was nachweislich dem Schutz der IT des Bundes dient. Sie setzt gezielt und wirkungsvoll zusätzliche Haushaltsmittel für Cybersicherheit ein.

Inhaltsverzeichnis

Abkürzungsverzeichnis

B

BaFin *Bundesanstalt für Finanzdienstleistungsaufsicht*
BBK *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*
BKB *Betriebskonsolidierung Bund*
BKG *Bundesamt für Kartographie und Geodäsie*
BMBF *Bundesministerium für Bildung und Forschung*
BMDS *Bundesministerium für Digitales und Staatsmodernisierung*
BMF *Bundesministerium der Finanzen*
BMI *Bundesministerium des Innern*
BNetzA *Bundesnetzagentur*
BSI *Bundesamt für Sicherheit in der Informationstechnik*
BSIG *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*

C

CER-Richtlinie *Critical Entities Resilience Directive*
Cyber-AZ *Nationales Cyber-Abwehrzentrum*

D

DaaS *Detection-as-a-Service*
DDoS *Distributed Denial of Service*

G

G 115 *Gesetz zur Ausführung von Artikel 115 des Grundgesetzes*

H

Haushaltsausschuss *Haushaltsausschuss des Deutschen Bundestages*
HVB-kompakt *Hochverfügbarkeitsbenchmark kompakt*

I

IT *Informationstechnik*
ITZBund *Informationstechnikzentrum Bund*

K

KI *Künstliche Intelligenz*
KoSi Bund *Kompetenzzentrum für operative Sicherheitsberatung der Bundesverwaltung*
KRITIS *Kritische Infrastruktur*

KRITIS-Betreiber *Betreiber Kritischer Infrastrukturen*
KRITIS-DachG *Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen*

L

LÜKEX *Länderübergreifende Krisenmanagement-Übung/Exercise*

N

NEA *Netzersatzanlage*
NIS-2-Richtlinie *Zweite Netzwerk- und Informationssicherheitsrichtlinie*
NIS2UmsuCG *Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung*

R

Rechnungsprüfungsausschuss *Rechnungsprüfungsausschuss des Haushaltsausschusses des Deutschen Bundestages*
RZ *Rechenzentren*

U

USV *Unterbrechungsfreie Stromversorgung*

0 Zusammenfassung

Der Bundesrechnungshof prüft in einem mehrjährigen Prüfungsschwerpunkt die Resilienz der staatlichen Kernfunktionen und ihrer kritischen Infrastruktur, insbesondere in den Bereichen Verkehr, Energie, Cybersicherheit, Kommunikation, innere- und äußere Sicherheit, Katastrophen- und Zivilschutz, Gesundheit, Wasser, Ernährung und Finanzen.

Resilienz versteht der Bundesrechnungshof insoweit umfassend als die Fähigkeit, staatliche Kernfunktionen und ihre kritische Infrastruktur zu schützen und einen funktionseinschränkenden Vorfall zu verhindern (präventive Komponente) sowie ursachenunabhängig im Falle eines funktionseinschränkenden Vorfalls auf diesen angemessen zu reagieren, diesen abzuwehren, seine negativen Folgen zu begrenzen sowie die Funktionsfähigkeit der betroffenen staatlichen Kernfunktionen und ihrer Infrastruktur möglichst zügig und umfassend wiederherzustellen (reaktive Komponente).

0.1

Die Lage der IT-Sicherheit in Deutschland ist besorgniserregend. Die fortschreitende Digitalisierung, die zunehmende Vernetzung und der verstärkte Einsatz von Künstlicher Intelligenz (KI) vergrößern die Angriffsflächen auf unsere IT-Infrastrukturen erheblich. Cyberkriminelle sowie fremde Staaten nutzen diese in großem Umfang. Die jährlichen Schäden durch Cyberangriffe belaufen sich für die deutsche Wirtschaft auf bald 180 Mrd. Euro. Hinzu kommt das Schadenspotenzial beispielsweise eines Blackouts oder gezielter Sabotageakte. Dieser reale und potenzielle Sicherheitsverlust schwächt das Vertrauen von Bürgerinnen und Bürgern sowie der Wirtschaft in die öffentliche Verwaltung.

Der Bundesrechnungshof hat in der 20. Legislaturperiode zahlreiche Prüfungen zur Informations- und Cybersicherheit der Bundesverwaltung und Kritischer Infrastrukturen (KRITIS) durchgeführt. Dieser Bericht stellt einen Auszug seiner wichtigen Erkenntnisse und Empfehlungen zusammen. Er berücksichtigt zudem die gemeinsame Stellungnahme des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) und des Bundesministeriums des Innern (BMI). Der Bundesrechnungshof will damit der neuen Bundesregierung und dem Gesetzgeber zu Beginn der 21. Legislaturperiode vordringlichen Handlungsbedarf aufzeigen, um die Weichen für einen sicheren Cyberraum zu stellen. (Tz. 1)

0.2

Die Cybersicherheitsstrategie des Bundes bildet den zentralen Handlungsrahmen für die Cyber-Sicherheitspolitik. Seit dem Jahr 2021 ist die dritte Cybersicherheitsstrategie in Kraft. Sie

umfasst 44 nicht priorisierte Ziele. Ihr lag keine Defizitanalyse zugrunde, ihre Finanzierung ist ungeklärt und es fehlt eine zentrale Steuerung sowie ein angemessenes Strategie-Controlling. Entgegen der erklärten Absicht hat die Bundesregierung die Cybersicherheitsstrategie in der 20. Legislaturperiode nicht weiterentwickelt.

Inwieweit die aktuelle Cybersicherheitsstrategie dazu beigetragen hat, die Cybersicherheit Deutschlands zu verbessern, ist unklar. Ohne Defizitanalyse ist offen, welche gravierenden Mängel bestehen und welche Ziele der Cybersicherheitsstrategie in welchem Maße geeignet sind, diese zu adressieren.

Die Bundesregierung muss dafür sorgen, dass ihr vor der Fortentwicklung valide Informationen zur Wirksamkeit und Wirtschaftlichkeit der bisherigen Cybersicherheitsstrategie vorliegen. Auf der Grundlage dieser Evaluation sollte sie dann für die neue Cybersicherheitsstrategie

- → *defizitäre oder fehlende Fähigkeiten in der Cybersicherheit ermitteln,*
- → *überprüfbare defizitbezogene Ziele formulieren und diese priorisieren,*
- → *eine wirksame Steuerung, ein operatives und ein strategisches Controlling etablieren,*
- → *die Umsetzung zentral und nachhaltig finanzieren sowie die Zuweisung von Haushaltsmitteln von nachweislich erreichten Meilensteinen abhängig machen.*

Das BMI hat mitgeteilt, das vorzeitige Ende der Legislaturperiode habe verhindert, die Weiterentwicklung der Cybersicherheitsstrategie abzuschließen. Es werde diese nun bis August 2025 evaluieren. Deren Ziele seien hinreichend überprüfbar, aber aufgrund ihrer jeweils hohen Bedeutung nicht untereinander zu priorisieren. Die im aktuellen Koalitionsvertrag vorgesehene Fortentwicklung werde es danach anstoßen.

Der Bundesrechnungshof bewertet es positiv, dass das BMI nun die Cybersicherheitsstrategie evaluiert. Wie belastbar die Ergebnisse zu den 44 Zielen angesichts weitgehend fehlender und unscharfer Kennzahlen sein werden, bleibt allerdings abzuwarten. Das BMI lässt offen, wie die Bundesregierung eine ausreichende Finanzierung und ein fortlaufendes Controlling der nächsten Cybersicherheitsstrategie sicherstellen soll. Angesichts begrenzter Ressourcen muss diese auch gleichsam hoch relevante Ziele priorisieren. Der Bundesrechnungshof bekräftigt daher seine Empfehlungen vollumfänglich. (Tz. 2)

0.3

Die Cybersicherheitsarchitektur auf Bundesebene weist derzeit 77 Akteure aus, die einen Beitrag zur Cybersicherheit leisten sollen. Die Zahl der staatlichen Akteure steigt seit Jahren. Die Bundesregierung wollte daher die Cybersicherheitsarchitektur überprüfen und diese anpassen. Dies ist bisher unterblieben, obwohl es hierzu konkreten Anlass gibt. So stellte der Bundesrechnungshof bei Prüfungen eine fehlende oder unzureichende Zusammenarbeit der Akteure der Cybersicherheitsarchitektur fest. Inwieweit jeder Akteur, z. B. das Nationale Cyber-

Abwehrzentrum (Cyber-AZ), einen Mehrwert für die Cybersicherheit erbringt, ist nicht nachgewiesen. Verteilte Zuständigkeiten im Bereich KRITIS führen zu bürokratischen Belastungen der Wirtschaft und zu Ineffizienz. Bei Bedrohungslagen könnten die Akteure an einem schnellen und abgestimmten Handeln gehindert sein. Auch sind die neuen europäischen Richtlinien zur Cyber- und zur physischen Sicherheit von KRITIS noch nicht in nationales Recht umgesetzt. Diese werden sich erheblich auf die Cybersicherheitsarchitektur auswirken.

Ohne die längst überfällige Evaluation der Cybersicherheitsarchitektur besteht die Gefahr von Doppelstrukturen und -arbeit. Dadurch könnte die Bundesverwaltung vergeblich Ressourcen vorhalten, die sie an anderer Stelle dringlicher benötigt. Für eine effiziente bürokratiearme Zusammenarbeit fehlt wichtigen Akteuren der Cybersicherheitsarchitektur wie

- *dem Bundesamt für Sicherheit in der Informationstechnik (BSI),*
- *dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK),*
- *der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und*
- *der Bundesnetzagentur (BNetzA)*

eine gemeinsame Datenbasis und ein einheitlicher strukturierter Datenaustausch.

Die Bundesregierung muss die Cybersicherheitsarchitektur evaluieren und schlanker sowie robust gestalten. Insgesamt muss sie die Arbeit von u. a. BSI, BBK, BaFin und BNetzA spätestens mit der Umsetzung der neuen europäischen Richtlinien besser strukturieren und koordinieren.

BMI und BMDS haben auf europäische Vorgaben hingewiesen, die vielfach für verteilte Zuständigkeiten in den KRITIS-Sektoren ursächlich seien. Gegenstand deren nationaler Umsetzung sei es, mehrfache Meldepflichten zu vermeiden und dem BSI zu einem vollständigen Lageüberblick zu verhelfen. Das Cyber-AZ sei eine Kooperationsplattform ohne Befugnisse zur Cyberabwehr. Daran beteiligte Behörden würden im Krisenfall entsprechend ihrer gesetzlichen Aufgaben tätig. Die Bundesregierung wolle das Cyber-AZ fortentwickeln und dabei Doppelstrukturen vermeiden.

Auf wesentliche Empfehlungen des Bundesrechnungshofes sind BMDS und BMI nicht eingegangen. Ohne eine umfassende Analyse der Cybersicherheitsarchitektur fehlen der Bundesregierung wichtige Erkenntnisse z. B. für die Umsetzung der EU-Richtlinien und andere Cybersicherheitsvorhaben. Festzuhalten ist, dass das Cyber-AZ der seiner Bezeichnung geschuldeten Erwartung, Cyberangriffe abzuwehren, bisher nicht gerecht wird. Anstatt dessen Bedeutung zu relativieren, sollte die Bundesregierung untersuchen, ob und wie dieses besser zur Cyberabwehr beitragen kann. Der Bundesrechnungshof bleibt bei seinen Empfehlungen. (Tz. 3)

0.4

Das Fundament der IT des Bundes sind über 100 Rechenzentren (RZ). Ohne sie und die sie verbindenden Netze wären die Behörden in wesentlichen Aufgabenbereichen nicht mehr handlungsfähig. Das IT-Sicherheitsniveau der RZ ist unzureichend. Nach Angaben des BSI erfüllten weniger als 10 % der von ihm untersuchten RZ den Mindeststandard. Darüber hinaus fehlen steuerungsrelevante Informationen über den Zustand der RZ des Bundes. Wegen Personalmangels kontrolliert das BSI die IT der Bundesbehörden bislang unzureichend. Auch fehlen Haushaltsmittel für die Hochverfügbarkeit der RZ und die Stärkung der Sabotage-Resilienz von Staat und Wirtschaft. Entgegen der Anforderungen der zunehmenden Zentralisierung der IT des Bundes ist häufig keine Georedundanz kritischer IT-Dienste vorhanden. Die Notstromversorgung ist für Krisenlagen nicht gerüstet. Insbesondere aber gibt es keine ressortübergreifende RZ-Strategie.

Angesichts der besorgniserregenden Sicherheitslage hätten die Steuerungsgremien des Bundes valide ausführlichere Informationen über die Cybersicherheit der IT-Infrastruktur benötigt, um sachgerechte Entscheidungen treffen zu können. Die notwendige Zentralisierung der IT hätte erfordert, dass die Bundesregierung kritische IT-Dienste redundant bereitstellt. Dies ist bisher nicht gewährleistet und gefährdet so die Krisenresilienz der Bundesverwaltung. Derzeit ist nicht einmal deren Weiterbetrieb bei einem längerfristigen Stromausfall sichergestellt. Ohne eine übergreifende RZ-Strategie fehlt die Grundlage für einen gezielten und wirtschaftlichen Aufbau von Fähigkeiten der IT und der erforderlichen Krisenresilienz.

Die Bundesregierung muss sicherstellen, dass die Steuerungsgremien künftig alle entscheidungsrelevanten Informationen erhalten. Das BSI muss sie so aufstellen, dass es seine Kontroll- und Unterstützungsaufgaben angemessen wahrnehmen kann. Die Bundesregierung muss eine übergreifende RZ-Strategie erstellen und diese umsetzen.

BMDS und BMI haben im Wesentlichen der Würdigung und den Empfehlungen des Bundesrechnungshofes zur Krisenresilienz zugestimmt. Allerdings habe das BMI hierfür nur eine koordinierende Rolle. Aufgrund des Ressortprinzips müssten die Behörden eigenständig prüfen, welche ihrer RZ nötig seien, um die Staats- und Regierungsfunktionen auch in Krisenlagen aufrechtzuerhalten. Gleiches gelte für deren Schutz.

Es bleibt offen, wann BMDS und BMI die Empfehlungen des Bundesrechnungshofes umsetzen. Deren Verweis auf das Ressortprinzip wird zudem weder den Herausforderungen noch ihrer federführenden Verantwortung und Koordinierungsfunktion gerecht. Denn das BMDS hat – anders als früher das BMI – einen Zustimmungsvorbehalt für alle wesentlichen IT-Ausgaben erhalten. Diesen sollte es auch nutzen, um geeignete Schutzmaßnahmen für kritische zentrale und dezentrale IT-Dienste durchzusetzen. Deren Ausfälle muss die Bundesregierung unter allen Umständen vermeiden oder zumindest deren Folgen reduzieren. (Tz. 4)

0.5

Das Grundgesetz ermöglicht es, die für die Schuldenregel relevanten Krediteinnahmen in einem bestimmten Umfang u. a. um Ausgaben für die Cybersicherheit zu bereinigen (Bereichsausnahme). Dadurch steigt der Verschuldungsspielraum des Bundes. Das Bundesministerium der Finanzen (BMF) hat den Ressorts technische Hinweise gegeben, wie sie die Ausgaben für Cybersicherheit zu veranschlagen haben. Danach bleibt weiterhin unklar, welche Beschaffungen und Dienstleistungen hierunter im Einzelnen fallen und in welcher Höhe diese Ausgaben im Bundeshaushalt bereits enthalten waren. Es gibt derzeit kein ressortübergreifendes Informationssicherheitscontrolling, welches solche Daten nach einer einheitlichen Definition liefert. Aufgabe der Bundesregierung ist es, ein sachgerechtes Controlling einzurichten sowie die Finanzierung der Informations- und Cybersicherheit geeignet zu organisieren. Beides hat sie dem Haushaltsausschuss des Deutschen Bundestages (Haushaltsausschuss) bereits zugesichert.

Erst wenn die Bundesregierung beziffern kann, in welcher Höhe sie Ausgaben für Cybersicherheit im Haushaltsentwurf veranschlagt hat, ist eine verfassungskonforme Inanspruchnahme der neu geschaffenen Bereichsausnahme möglich. Da sie bisher nicht vorgegeben hat, was die Ressorts genau der Cybersicherheit zurechnen dürfen, ist davon auszugehen, dass sie dies unverändert uneinheitlich bewerten. Fehlsteuerungen der Bundesregierung sind so nicht auszuschließen. Denn ohne gesicherte fortlaufende Informationen über den Ressourceneinsatz und den Status der Informationssicherheit in der Bundesverwaltung können weder Bundesregierung noch Haushaltsgesetzgeber die Wirtschaftlichkeit und die Wirkung der von ihnen verantworteten Cybersicherheitsmaßnahmen übergreifend und umfassend bewerten. Wie die Bundesregierung erforderliche Maßnahmen künftig steuern und finanzieren will, um Synergie- und Skaleneffekte zu erzielen, ist derzeit offen. Angesichts weiterhin begrenzter Haushaltsmittel ist es erforderlich, Einsatzmöglichkeiten, Wirtschaftlichkeit und Organisation eines zentralen Budgets für Cybersicherheit zu untersuchen.

Der Begriff „Ausgaben für Cybersicherheit“ sollte mit dem Ziel konkretisiert werden, dass alle Ressorts auf der Grundlage eines einheitlichen Verständnisses vergleichbare Angaben machen. Den Aufbau des Informationssicherheitscontrollings sollte die Bundesregierung priorisieren. Zudem sollte sie sachgerechte Einsatzbereiche und Finanzierungsmodelle für ein zentrales Cybersicherheitsbudget ausarbeiten und mit den Ressorts abstimmen.

Das BMI hat bestätigt, es sei aufgrund fehlender einheitlicher Kriterien schwierig, von den Ressorts vergleichbare Angaben zu deren Vorhaben für Cybersicherheit zu erhalten. Zudem setze ein zentrales Budget für Cybersicherheit zusätzliche Mittel aus dem Gesamthaushalt voraus. Bisher habe für ein zentrales Budget die Zustimmung aller Ressorts gefehlt. Die Bereichsausnahme für den „Schutz der informationstechnischen Systeme“ eröffne hierfür eine neue Option. Die neu konzipierte IT-Rahmenplanung könne eine übergreifende Transparenz über die IT-Budgets der Bundesbehörden schaffen.

Zwar erkennen BMDS und BMI den vom Bundesrechnungshof aufgezeigten Handlungsbedarf an. Die vorgesehenen Maßnahmen werden dem bestehenden Handlungsdruck allerdings nicht gerecht. Bereits für die Haushaltsplanungen der Jahre 2025 und 2026 müssen die Behörden angeben, welche IT-Ausgaben unter die Bereichsausnahme fallen. Der Bundesrechnungshof erwartet, dass die Bundesregierung ein zentrales Budget für Cybersicherheit nutzt, um Synergie- und Skalenpotenziale zu erschließen und dadurch Mittel für ressortübergreifende Projekte freizusetzen. Zusätzliche Mittel aus dem Gesamthaushalt hält er dafür nicht für erforderlich. Eine vereinheitlichte IT-Budgetplanung ist ein erster wichtiger Schritt zu mehr Transparenz. Von einem wirksamen Informationssicherheitscontrolling ist die Bundesverwaltung jedoch noch weit entfernt. Daher hält der Bundesrechnungshof an seiner Würdigung und seinen Empfehlungen uneingeschränkt fest. (Tz. 5)

0.6

Die neue Bundesregierung steht im Bereich der Cybersicherheit vor wichtigen Aufgaben. Sie muss zügig

- → *die aktuelle europäische Gesetzgebung in nationales Recht umsetzen und dabei die Zusammenarbeit der betroffenen Akteure wie BSI, BBK und BNetzA optimieren,*
- → *die Cybersicherheitsstrategie evaluieren und wirksam neugestalten,*
- → *die Cybersicherheitsarchitektur verschlanken und robust aufstellen,*
- → *die IT des Bundes und dafür insbesondere die RZ und die sie verbindenden Netze wirkungsvoll schützen und*
- → *eine langfristige, wirtschaftliche und nachhaltige Finanzierung, Steuerung und Kontrolle von wirksamen Cybersicherheitsmaßnahmen sicherstellen.*

BMDS und BMI haben zusammenfassend auf die Eigenverantwortung von Ressorts und Behörden für die Informationssicherheit verwiesen. Es sei gleichwohl bereits gelungen, dass u. a. das BSI diese fortlaufend besser berate, unterstütze und praxisorientierte Hilfestellungen anbiete. Die angespannte Haushaltslage habe bisher weitere bedarfsgerechte Maßnahmen nur eingeschränkt ermöglicht. Mit der Gründung des BMDS, der Umsetzung der zweiten Netzwerk- und Informationssicherheitsrichtlinie (NIS-2-Richtlinie) und den geplanten Kontrollen durch das BSI stelle die Bundesregierung das Informationssicherheitsmanagement des Bundes besser auf. Dabei wolle sie die Empfehlungen des Bundesrechnungshofes berücksichtigen.

Der Bundesrechnungshof sieht angesichts der gewaltigen Bedrohungen im Cyberraum die einzelnen Ressorts und Behörden nicht dauerhaft in der Lage, alleine Cybersicherheit auf dem erforderlichen hohen Niveau zu gewährleisten. Eine vereinheitlichte IT-Budgetplanung und der Zustimmungsvorbehalt des BMDS sind erste probate Mittel, um die Steuerung der Cybersicherheit in der Bundesverwaltung zu verbessern. Das BMDS tritt allerdings als weiterer Akteur in die Cybersicherheitsarchitektur ein. Diese darf dadurch nicht komplexer

werden.
Eigenverantwortung der Ressorts steht einer übergreifenden Steuerung und Finanzierung nicht entgegen. Vielmehr erfordert Eigenverantwortung in einem engvernetzten und digitalisierten Staat, eigene Ziele hinter dem übergeordneten Ziel der Aufrechterhaltung der Staats- und Regierungsfunktionen zurückzustellen. (Tz. 6)

1 Einleitung

Der Bundesrechnungshof prüft in einem mehrjährigen Prüfungsschwerpunkt die Resilienz der staatlichen Kernfunktionen und ihrer kritischen Infrastruktur, insbesondere in den Bereichen Verkehr, Energie, Cybersicherheit, Kommunikation, innere- und äußere Sicherheit, Katastrophen- und Zivilschutz, Gesundheit, Wasser, Ernährung und Finanzen.

Resilienz versteht der Bundesrechnungshof insoweit umfassend als die Fähigkeit, staatliche Kernfunktionen und ihre kritische Infrastruktur zu schützen und einen funktionseinschränkenden Vorfall zu verhindern (präventive Komponente) sowie ursachenunabhängig im Falle eines funktionseinschränkenden Vorfalls auf diesen angemessen zu reagieren, diesen abzuwehren, seine negativen Folgen zu begrenzen sowie die Funktionsfähigkeit der betroffenen staatlichen Kernfunktionen und ihrer Infrastruktur möglichst zügig und umfassend wiederherzustellen (reaktive Komponente).

In dem vorliegenden Bericht befasst sich der Bundesrechnungshof mit zentralen Elementen für einen sicheren und resilienten Cyberraum, bei denen es in Deutschland aktuell Handlungsbedarf gibt.

„Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend“ – so das Fazit des BSI in seinem aktuellen Lagebericht.[1] Die fortschreitende Digitalisierung, die zunehmende Vernetzung und der verstärkte Einsatz von KI vergrößern die Angriffsflächen auf die IT-Infrastrukturen erheblich. Cyberkriminelle sowie fremde Staaten nutzen diese in großem Umfang.[2] Der Branchenverband Bitkom e. V. schätzt die Schäden, die die deutsche Wirtschaft allein durch Cyberangriffe erleidet, auf jährlich 179 Mrd. Euro.[3] Hinzu kommt das erhebliche Schadenspotenzial beispielsweise eines Blackouts[4] oder gezielter Sabotageakte.

Abgesehen von dem monetären Verlust ist für die öffentliche Verwaltung das Vertrauen der Bürgerinnen und Bürger sowie der Wirtschaft in einen sicheren und jederzeit handlungsfähigen Staat von enormer Bedeutung:

→ Geopolitische Spannungen nehmen gegenwärtig zu. Deutschland ist verstärkt Ziel hybrider Angriffe.[5] Für die Krisen- und Verteidigungsfähigkeit Deutschlands ist es daher unerlässlich, dass digitale hochsensible staatliche Informationen umfassend geschützt, sicher verarbeitet und übermittelt werden.

[1] Die Lage der IT-Sicherheit in Deutschland 2024, Hrsg.: BSI, Oktober 2024; zuletzt abgerufen am 25. April 2025.
[2] Bundeslagebild Cybercrime 2023, Hrsg. Bundeskriminalamt, Mai 2024; zuletzt abgerufen am 30. April 2025.
[3] bitkom-Presseinformation "Wirtschaftsschutz-2024", zuletzt abgerufen am 25. April 2025.
[4] Nach dem nahezu landesweiten Ausfall der Stromversorgung in Spanien und Portugal am 28. April 2025 sprach die EU-Kommission von einem Blackout von "nie dagewesenem Ausmaß"; zuletzt abgerufen am 30. April 2025.
[5] Z. B. Drohnen über Militärstützpunkten und kritischer Infrastruktur, sabotierte Unterseekabel in der Ostsee; zuletzt abgerufen am 16. Mai 2025.

- → Die Akzeptanz zentraler Verwaltungsdienstleistungen, wie der elektronischen Identifizierung[6] oder der elektronischen Patientenakte[7], stehen und fallen mit deren sicheren Umsetzung.
- → Staatliche Kernfunktionen lassen sich ohne resiliente RZ und sichere Netzinfrastrukturen – erst recht in Krisensituationen – nicht aufrechterhalten. Mit Papier, Stift und Taschenrechner kann der Staat viele seiner Aufgaben (z. B. Sozialleistungen, Grenzkontrollen, Steuerverwaltung) nicht mehr erfüllen.

Prüfungserkenntnisse des Bundesrechnungshofes zeigen seit Jahren erhebliche konzeptionelle und technische Defizite in der Absicherung der IT-Infrastrukturen der Bundesbehörden auf. Die Bundesregierung hat selber eingeräumt, dass viele Einrichtungen der Bundesverwaltung die Anforderungen an die Informationssicherheit unzureichend umsetzten.[8]

Der Haushaltsausschuss hat sich aus Anlass entsprechender Berichte des Bundesrechnungshofes[9] und des BMI in der letzten Legislaturperiode mehrfach mit der Cybersicherheit befasst. Zuletzt forderte er die Bundesregierung im November 2024 auf, die Eigensicherung des Bundes gegenüber Cyberangriffen zu stärken. Hierfür müsse die Bundesregierung

- → ihre Prioritäten zugunsten der Cybersicherheit neu ausrichten,
- → Maßnahmen der Cybersicherheit ressortübergreifend steuern und insbesondere
- → das BSI effizient aufstellen, digitalisieren und bedarfsgerecht ausstatten.

Gleichzeitig bat der Haushaltsausschuss den Bundesrechnungshof, die Umsetzung dieser Forderungen prüfend zu begleiten.

In der neuen Bundesregierung hat das BMDS vom BMI u. a. die Zuständigkeit für die Cybersicherheit der Bundesverwaltung übernommen. Der Bundesrechnungshof hat daher das BMDS um eine mit dem BMI abgestimmte Stellungnahme gebeten. Diese hat er in dem vorliegenden Bericht berücksichtigt.

[6] Personalausweisportal; zuletzt abgerufen am 2. Mai 2025.
[7] Information des Bundesministeriums für Gesundheit zur Elektronischen Patientenakte; zuletzt abgerufen am 2. Mai 2025.
[8] Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Bundestagsdrucksache 20/13184, Seite 138; zuletzt abgerufen am 27. Juni 2025.
[9] Bundesrechnungshof, Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss des Deutschen Bundestages zu Vorhaben der Cybersicherheit vom 16. Oktober 2024 (Gz.: VII 4 - 0000583/III).

2 Deutschland braucht eine wirksame Cybersicherheitsstrategie

Sachverhalt

Defizitanalyse fehlt

Die Cybersicherheitsstrategie bildet den zentralen Handlungsrahmen für die Cyber-Sicherheitspolitik der Bundesregierung. Im Jahr 2021 beschloss sie ihre dritte Cybersicherheitsstrategie.[10] Diese beschreibt in 44 Zielen, wie die Bundesregierung die Cybersicherheit in Deutschland aufrechterhalten oder verbessern will. Die Bundesregierung analysierte im Vorfeld nicht, welche Defizite Deutschland im Bereich der Cybersicherheit hatte. Ebenso priorisierte sie die 44 Ziele nicht.

Die Bundesregierung begründete ihre Ziele mit der Cyberbedrohungslage in Deutschland. Sie zeigte Angriffsvektoren auf, erläuterte Bedrohungen und benannte die bedrohten Güter. In welchem Umfang die jeweiligen Ziele dazu beitragen sollen, die Cyberbedrohungslage zu bewältigen und künftigen Bedrohungen und Risiken vorzubeugen, stellt die Cybersicherheitsstrategie nicht dar.

Finanzierung ungeklärt

Die Bundesregierung beschloss die Cybersicherheitsstrategie, ohne den Ausgaben- und Personalbedarf für ihre Umsetzung ermittelt zu haben. Sie definierte die Strategie als Rahmen für ihr Handeln „vorbehaltlich der Verfügbarkeit entsprechender Haushaltsmittel“. Zentrale Vorsorge, z. B. im Haushalt des BMI, traf sie auch in den Folgejahren nicht. Die 44 Ziele der Strategie verteilen sich bisher auf zwölf Ressorts. Inwieweit diese haushalterische Vorkehrungen getroffen haben, um ihren Beitrag zur Zielerreichung zu leisten, war dem BMI Ende des Jahres 2024 nicht bekannt. Daher forderte der Haushaltsausschuss das BMI auf, sich einen Überblick zu verschaffen und Vorhaben der Cybersicherheit der Ressorts und die dafür veranschlagten Haushaltsmittel bis Ende März 2025 titelscharf zu ermitteln. Das Ergebnis lag im Mai 2025 noch nicht vor.

Steuerung erforderlich

Die Ressorts sind dafür verantwortlich, geeignete Projekte und Maßnahmen auszuwählen und durchzuführen. Die Cybersicherheitsstrategie sieht zwar ein Controlling auf der

[10] Beschluss des Bundeskabinetts der 19. Legislaturperiode vom 8. September 2021.

strategischen Ebene vor. Allerdings fehlen hier einheitliche Vorgaben für das vorgelagerte operative Controlling der Ressorts sowie für deren Maßnahmenauswahl. Die Ziele definierte die Bundesregierung zumeist nicht so, dass diese überprüfbar wären. Stattdessen sah sie insgesamt 180 Indikatoren vor. Deren Ist-Werte zum Zeitpunkt des Beschlusses der Strategie (Ausgangslage) fehlen hier allerdings ebenso wie (angestrebte) Ziel-Werte.

Beispiel

Ziele und Indikatoren in der Cybersicherheitsstrategie 2021

Unter Ziffer 8.3.4 benannte die Bundesregierung das Ziel „Das Cyber-Abwehrzentrum weiterentwickeln“. Ob sie das Ziel erreicht hat, wollte sie u. a. anhand des Indikators „Cybersicherheitsvorfälle und Cyberlagen werden schnell und effektiv bearbeitet“ überprüfen.

Um das Ziel „Strafverfolgung im Cyberraum intensivieren“ (Ziffer 8.3.7) zu bewerten, wollte sie den Indikator „Die Befugnisse aus der Strafprozessordnung entsprechen den Anforderungen der Praxis“ heranziehen.

Ein anderer Indikator (zu Ziffer 8.1.8) sah – ohne Angabe eines Ausgangs- und Zielwertes – vor, dass „entdeckte Sicherheitslücken […] zunehmend gemeldet“ werden.

Keine Weiterentwicklung

Zu Beginn der 20. Legislaturperiode startete die Bundesregierung einen Prozess, um die Cybersicherheitsstrategie weiterzuentwickeln. Anlass waren teilweise abweichende Vorgaben des damaligen Koalitionsvertrages, beispielsweise zum Schwachstellenmanagement und zur Verschlüsselung. Ebenso wollte die Bundesregierung die Konsequenzen aus der verschärften geopolitischen Lage einbeziehen.[11] Bis zum (vorzeitigen) Ende der 20. Legislaturperiode hatte sie keine überarbeitete Fassung der Cybersicherheitsstrategie verabschiedet.

Der Koalitionsvertrag für die 21. Legislaturperiode setzt das Ziel, die Cybersicherheitsstrategie so fortzuentwickeln, dass Rollen und Aufgaben klar verteilt sind.[12]

[11] Koalitionsvertrag 2021-2025 zwischen SPD, BÜNDNIS 90 / DIE GRÜNEN und FDP, Seite 13.
[12] Koalitionsvertrag zwischen CDU, CSU und SPD „Verantwortung für Deutschland“, Zeilen 2676 ff.

Würdigung

Ohne eine Evaluation ist unklar, inwieweit die Cybersicherheitsstrategie dazu beigetragen hat, die Cybersicherheit Deutschlands zu steigern. Da überprüfbare Ziele und ein wirksames Controlling fehlen, ist eine belastbare Antwort auf diese Frage auch kaum zu erwarten. Fehlende übergreifende Vorgaben – verstärkt durch eine ausstehende, überarbeitete Strategie – führten dazu, dass die Ressorts weitgehend isoliert agierten und ihre Aktivitäten nicht bündelten. Das federführende BMI verschaffte sich dazu bis zum Beschluss des Haushaltsausschusses nicht einmal einen ressortübergreifenden Überblick.

Der Cybersicherheitsstrategie hätte nicht nur eine Bedrohungs-, sondern auch eine übergeordnete Defizitanalyse zugrunde liegen müssen. Stattdessen blieb zum Teil offen, welche gravierenden Mängel hinsichtlich der Cybersicherheit bestehen und inwiefern die Ziele geeignet sind, diese zu beheben. Die Definition von 180 Indikatoren erweckt den Eindruck, diese seien die Stellschrauben, über die sich Cybersicherheit definieren und im Wesentlichen beeinflussen ließe. Welche Bedeutung die Ziele und die ihnen zugeordneten Indikatoren für die Bewältigung der aufgezeigten Bedrohungen und Angriffsvektoren haben, bleibt aber weitgehend unklar. Denn diese sind zu vage definiert, da z. B. für Attribute wie „effizient“, „effektiv“ oder „zunehmend“ sowohl Ist- als auch Zielwerte fehlen. Auch erschließt sich nicht, dass genau die vorgesehenen Ziele und Indikatoren den wesentlichen und wichtigsten Beitrag zur Verbesserung der Cybersicherheit liefern. Eine Defizitanalyse hätte dagegen ermöglicht, die 44 Ziele zu priorisieren.

Empfehlung

Die neue Bundesregierung hat die Aufgabe, eine wirksame Cybersicherheitsstrategie zu erarbeiten und zu beschließen. Sie sollte in diesem Prozess Konsequenzen aus den Versäumnissen früherer Strategien ziehen. Sie muss dafür sorgen, dass ihr vor der Fortentwicklung der bisherigen Cybersicherheitsstrategie valide Informationen zu deren Wirksamkeit und Wirtschaftlichkeit vorliegen. Auf der Basis gesicherter Erkenntnisse sollte sie die nächste Strategie zukunftsgerecht ausgestalten und dazu insbesondere

- die defizitären oder fehlenden Fähigkeiten Deutschlands im Bereich der Cybersicherheit ermitteln und deren Ursachen analysieren,
- die Ziele überprüfbar formulieren, ihren konkreten Beitrag zur Steigerung der Cybersicherheit und Behebung erkannter Defizite klar definieren und auf dieser Grundlage priorisieren,

- → von Beginn an eine wirksame Steuerung auf der Grundlage eines mit dem operativen Controlling eng verzahnten strategischen Controllings vorsehen, um auf Abweichungen rechtzeitig reagieren zu können,
- → die Umsetzung zentral finanzieren sowie die stufenweise Vergabe von Haushaltsmitteln an die Ressorts an das Erreichen verbindlicher Quality Gates[13] binden.

Stellungnahme von BMDS und BMI

Das BMI werde die Evaluation der Cybersicherheitsstrategie 2021 voraussichtlich im August 2025 abschließen. Auf der Grundlage der Ergebnisse werde es die Fortentwicklung anstoßen und dabei die Empfehlungen des Bundesrechnungshofes prüfen.

Die Ressorts hätten bis zum vorzeitigen Ende der letzten Legislaturperiode daran gearbeitet, die Cybersicherheitsstrategie weiterzuentwickeln. Sie hätten sich aber nicht in allen Punkten einigen können. Wegen des Dissenses hätten sie auch deren Controlling zurückgestellt. Zudem habe das hierfür notwendige Personal gefehlt. Aus Sicht des BMI seien die Ziele der Cybersicherheitsstrategie hinreichend überprüfbar formuliert. Um deren Ist- und Zielwerte zu bestimmen, könnte man die jeweilige Beschreibung des aktuellen und des beabsichtigten Zustands heranziehen. Sofern die Evaluation hier im Einzelfall Nachbesserungsbedarf aufzeige, werde das BMI dies bei der Fortentwicklung berücksichtigen. Die Ziele zu priorisieren, sei aufgrund ihrer hohen Relevanz allerdings nicht sachgerecht.

Abschließende Würdigung

Positiv zu bewerten ist, dass das BMI mit der eingeleiteten Evaluation eine wesentliche Grundlage schaffen will, um die Cybersicherheitsstrategie fortzuentwickeln. Ob die Abfrage bei den Stakeholdern der Cybersicherheitsstrategie, inwieweit die insgesamt 44 Ziele erreicht wurden, zu belastbaren Ergebnissen führt, ist angesichts deren teilweise ungenauer Formulierung und weitgehend fehlender Kennzahlen zu bezweifeln.

Auch lässt das BMI offen, wie die Bundesregierung die strukturellen Mängel, wie die ungeklärte Finanzierung und die fehlenden Ressourcen für die Steuerung der Cybersicherheitsstrategie, beheben soll. Der Bundesrechnungshof hält an seinen Empfehlungen fest, diese und weitere kritische Erfolgsfaktoren zu klären. Die nächste Cybersicherheitsstrategie sollte mit ausreichenden Haushaltsmitteln unterlegt sein. Auch sollte die Bundesregierung von Beginn an ein fortlaufendes Controlling sicherstellen. Insbesondere muss sie angesichts der großen Anzahl von Zielen klare Prioritäten setzen, selbst wenn alle Ziele eine hohe Relevanz für die Steigerung der Cybersicherheit

[13] Quality Gates sind Punkte im Ablauf einer Maßnahme, bei denen anhand von im Voraus eindeutig bestimmten Qualitätskriterien über die Freigabe und Finanzierung des nächsten Maßnahmenschrittes entschieden wird.

aufweisen. Denn nur dies ermöglicht ihr, ihre begrenzten Ressourcen auf besonders Wichtiges und Dringliches zu konzentrieren. Im Fall von Zielkonflikten kann sie anhand der Prioritäten entscheiden, wo sie welche Ressourcen einsetzt.

3 Deutschland benötigt eine robuste Cybersicherheitsarchitektur

Sachverhalt

Starker Aufwuchs der Cybersicherheitsarchitektur

Die Digitalisierung aller Lebensbereiche schreitet stetig voran und die sicherheitspolitische Bedeutung des Cyberraums nimmt weiter zu. Entsprechend ist die Cybersicherheit zu einem Thema geworden, mit dem sich in Deutschland eine mittlerweile nahezu unüberschaubare Vielzahl an Akteuren auf Ebene der Zivilgesellschaft, der Wissenschaft, der Wirtschaft und des Staates befasst. Der Nationale Pakt Cybersicherheit hat in seinem „Online-Kompendium Cybersicherheit in Deutschland“ bereits im Jahr 2020 über 370 Akteure identifiziert, die einen besonderen Beitrag zur Cybersicherheit leisten.[14] Auf Ebene des Bundes waren dies vor fünf Jahren bereits 20 Einrichtungen. Die aktuelle Übersicht „Deutschlands staatliche Cybersicherheitsarchitektur“ weist für die Bundesebene sogar 77 Einrichtungen aus.[15] Der Koalitionsvertrag für die 21. Legislaturperiode sieht u. a. vor, eine neue spezialisierte Zentralstelle zur Unterstützung der Nachrichtendienste im Cyber- und Informationsraum zu schaffen.[16]

Die Bundesregierung hat sich schon mehrfach das Ziel gesetzt, die nationale Cybersicherheitsarchitektur zu überprüfen und weiterzuentwickeln:

→ Die Cybersicherheitsstrategie 2021[17] sieht ein eigenes Handlungsfeld 3 für eine „leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur“ vor. Die Cybersicherheitsarchitektur sollte permanent überprüft und weiterentwickelt werden. Das Zusammenspiel der staatlichen Institutionen müsse fortlaufend strukturell und prozessual bewertet und gegebenenfalls angepasst werden. Die Bundesregierung wollte u. a. das BSI durch grund- und einfachgesetzliche Änderungen zur Zentralstelle

[14] Online Kompendium Cybersicherheit in Deutschland, Hrsg.: BMI, November 2020; zuletzt abgerufen am 29. April 2025.
[15] Cybersicherheitsarchitektur v1.1.1, Hrsg.: interface – Tech analysis and policy ideas for Europe e. V.; zuletzt abgerufen am 29. April 2025.
[16] Koalitionsvertrag zwischen CDU, CSU und SPD „Verantwortung für Deutschland“, Zeilen 2682 ff.
[17] Cybersicherheitsstrategie 2021, Seite 84; zuletzt abgerufen am 29. April 2025.

im Bund-Länder-Verhältnis ausbauen.[18] Das Cyber-AZ wollte sie als zentrale Kooperations-, Kommunikations- und Koordinationsplattform der relevanten Sicherheitsbehörden fortentwickeln.[19]

→ Auch mit der Nationalen Sicherheitsstrategie aus dem Jahr 2023[20] setzte sich die Bundesregierung das Ziel, die Cybersicherheitsarchitektur weiterzuentwickeln, Deutschland sollte jederzeit auch im Cyberraum reaktionsfähig und wehrhaft sein. Dafür wollte sie das Zusammenwirken der staatlichen Institutionen für Cybersicherheit und Strafverfolgung sowie von Nachrichtendiensten, Diplomatie und Militär bei der Abwehr von Cyberbedrohungen im Sinne der Integrierten Sicherheit verbessern.

→ Die Digitalstrategie[21] sieht vor, das Cyber-AZ als einen Akteur der Cybersicherheitsarchitektur weiterzuentwickeln, um damit die ressortübergreifende und gesamtstaatliche Zusammenarbeit in der Cybersicherheit zu stärken. Dies solle ermöglichen, Informationen zu einem gemeinsamen und umfassenden Lagebild der Cybersicherheit zu verdichten.

Unzureichende Zusammenarbeit von Akteuren der Cybersicherheitsarchitektur

Der Bundesrechnungshof hat die Zusammenarbeit der Behörden bei der Cybersicherheit geprüft. Er stellte dabei u. a. fest, dass die Bundesregierung das Cyber-AZ weiterentwickelte, ohne zuvor analysiert zu haben, inwieweit sich die behördenübergreifende Bewältigung von Cyber-Ereignissen außerhalb des Cyber-AZ optimieren lässt.

Beispiele

Einbindung des Cyber-AZ in das IT-Krisenmanagement

In der LÜKEX[22] 23 übten eine Vielzahl von Akteuren der Cybersicherheitsarchitektur, u. a. auch der Krisenstab des BMI und das Cyber-AZ, die Bewältigung des Szenarios „Cyberangriff auf das Regierungshandeln“. Obwohl das Cyber-AZ bereits zu Beginn der Übung in die sogenannte Lage- und Ereignisstufe 2 übergegangen war und dies dem BMI-Krisenstab mitgeteilt hatte, bezog dieser das Cyber-AZ während der gesamten zweitägigen Übung nicht unmittelbar ein. Damit konnten vorgesehene Prozesse nicht etabliert und die Rolle des Cyber-AZ in der Krise nicht erprobt werden.

[18] Ebd., Seite 89.
[19] Ebd., Seite 90.
[20] Nationale Sicherheitsstrategie, Seite 61; zuletzt abgerufen am 29. April 2025.
[21] Digitalstrategie, Seite 50; zuletzt abgerufen am 29. April 2025.
[22] Länderübergreifende Krisenmanagement-Übung/Exercise.

Nationales Cybersicherheitslagebild

Das BSI hat die Aufgabe, ein Gesamtlagebild der Cyber-Sicherheit in Deutschland zu erstellen.[23] Es arbeitet an einem einheitlichen, kontinuierlich aktualisierten Cybersicherheitslagebild. Dieses soll jederzeit eine fundierte Grundlage für strategische und operative Entscheidungen bieten. Hierfür soll das BSI Daten und Erkenntnisse aus den vier Säulen der Cybersicherheitsarchitektur (militärisch, zivil, nachrichtendienstlich und polizeilich) und aus der Wirtschaft zusammenführen und wieder in diese Strukturen zurückspielen.

Das Cyber-AZ soll ein umfassendes und jederzeit verfügbares, dynamisches, skalierbares Lagebild „Cyber" zentral bereitstellen. Dieses soll sowohl als Information für die politisch-strategische Ebene als auch als Basis für operative Entscheidungen dienen.

Die Bundesregierung hat die Cybersicherheitsarchitektur bislang nicht umfassend überprüft. Auch den bisherigen Planungen, das BSI zu einer Zentralstelle im Bund-Länder-Verhältnis auszubauen, lag keine entsprechende Analyse zugrunde.[24] Sie hat zwar mit LÜKEX 11[25] und LÜKEX 23 zwei Mal Stabsrahmenübungen auf politisch-administrativer Ebene durchgeführt, an denen auf freiwilliger Basis auch Akteure der Cybersicherheitsarchitektur teilgenommen haben. Aber verpflichtende Stresstests[26], wie sie beispielsweise in der Finanzwelt üblich sind, gab es bisher noch nicht.

Die neue Bundesregierung richtet im Bundeskanzleramt mit dem Nationalen Sicherheitsrat einen weiteren Akteur der Cybersicherheitsarchitektur ein.[27]

Verteilte Zuständigkeiten im Bereich der KRITIS

Betreiber kritischer Infrastrukturen (KRITIS-Betreiber) unterliegen hinsichtlich ihrer Cybersicherheit unterschiedlichen gesetzlichen Verpflichtungen. Überwiegend müssen sie Meldungen über Sicherheitsvorfälle sowie Nachweise über ihren Sicherheitsstatus an das BSI richten. Daneben sind aber auch beispielsweise die BaFin sowie die BNetzA Aufsichtsbehörden für KRITIS-Betreiber bestimmter Sektoren.

[23] Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, Bundestagsdrucksache 19/26106, Begründung zu § 4 b BSIG.
[24] Zwischenbericht des BMI zum Thema „Unabhängigere Aufstellung und Ausbau des Bundesamtes für Sicherheit in der Informationstechnik als Zentralstelle für IT-Sicherheit" vom 2. Januar 2024.
[25] Der LÜKEX 11 lag das Szenario zielgerichteter IT-Angriffe auf Schwachstellen bei KRITIS und in Regierungsnetzen zugrunde.
[26] Ein Stresstest für eine Organisation ist eine Prüfung, bei der extreme, aber mögliche Krisenszenarien durchgespielt werden, um zu sehen, wie gut die Organisation solchen Belastungen standhalten kann. Ziel ist es, Schwachstellen frühzeitig zu erkennen und sich besser auf Notfälle oder Ausnahmesituationen vorzubereiten.
[27] Organisationserlass des Bundeskanzlers vom 6. Mai 2025, Abschnitt XVI.

Beispiel

Betreiber von Energieversorgungsnetzen und Energieanlagen

Für die KRITIS-Betreiber im Bereich der Energieversorgungsnetze und Energieanlagen speichern sowohl die BNetzA als auch das BSI Daten und Informationen. Deren Struktur und Ordnungsmerkmale haben sie nicht aufeinander abgestimmt. Wenn sie Daten und Informationen austauschen, erzeugt dies zusätzlichen Aufwand. Für bestimmte KRITIS-Betreiber gelten gleichzeitig die Regelungen des BSI-Gesetzes und des Energiewirtschaftsgesetzes. Sie müssen ihre IT-Sicherheitsvorkehrungen sowohl dem BSI alle zwei Jahre mit einem Nachweis als auch der BNetzA alle drei Jahre mit einem Zertifikat belegen.

Die Europäische Union will mit zwei Richtlinien sowohl den physischen Schutz als auch die Cybersicherheit von KRITIS-Betreibern erstmalig regeln beziehungsweise verbessern:

- → Die Critical Entities Resilience Directive (CER-Richtlinie)[28] verpflichtet die EU-Mitgliedstaaten, die physische Widerstandsfähigkeit der KRITIS-Betreiber gegenüber Bedrohungen wie Naturgefahren, Terroranschläge oder Sabotageakte zu stärken.
- → Mit der NIS-2-Richtlinie [29] will sie die Anfälligkeit der EU-Mitgliedstaaten gegenüber Cyberbedrohungen senken und hierfür einheitliche Vorgaben schaffen.

Die neue Bundesregierung muss beide Richtlinien noch in nationales Recht umsetzen. Mit dem sogenannten KRITIS-DachG[30] sollen dem BBK zentrale Aufgaben, wie die Registrierung oder die Bearbeitung von Sicherheitsvorfällen von KRITIS-Betreibern, übertragen werden. Vergleichbare Aufgaben sah der bisherige Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)[31] für das BSI vor.

Der Bundesrechnungshof hat das BMI und zuletzt den Haushaltsausschuss auf das Erfordernis der Kohärenz von KRITIS-DachG und NIS2UmsuCG hingewiesen. Denn KRITIS-Betreiber und die mit der Aufsicht betrauten Behörden sollten diese Regelungen und Maßgaben möglichst wirtschaftlich und unbürokratisch umsetzen können. In

[28] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen; zuletzt abgerufen am 27. Juni 2025.
[29] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union; zuletzt abgerufen am 27. Juni 2025.
[30] Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, Bundestagsdrucksache 20/13961; zuletzt abgerufen am 27. Juni 2025.
[31] Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Bundestagsdrucksache 20/13184; zuletzt abgerufen am 27. Juni 2025.

die Gesetze sollten insbesondere Regelungen für eine gemeinsame Datenbasis von BSI und BBK aufgenommen werden.[32]

Würdigung

Der Cyberraum und seine Bedrohungen verändern sich schnell und dynamisch. Die Bundesregierung hätte daher – wie in ihrer Cybersicherheitsstrategie ausgewiesen – die Cybersicherheitsarchitektur fortlaufend überprüfen müssen. Nicht nur die spätestens seit dem Jahr 2022 verschärfte geopolitische Bedrohungslage hätte hierzu Anlass gegeben. Gerade weil die Bundesregierung plante, dem BSI eine Zentralstellenfunktion zuzuweisen und die LÜKEX 23 Schwierigkeiten in der Zusammenarbeit der Behörden aufzeigte, hätte sie die Cybersicherheitsarchitektur tiefgehend analysieren müssen. Es hätte umfassender auf die gesamte Cybersicherheitsarchitektur bezogener Stresstests bedurft, um deren Leistungsfähigkeit beurteilen zu können. Stabsrahmenübungen, die die Cybersicherheitsarchitektur nur in Teilen berühren, reichen dafür nicht aus.

Solange die Ergebnisse dieser längst überfälligen Analyse fehlen, bleibt beispielsweise offen, welche Rolle dem Cyber-AZ u. a. bei der Krisenbewältigung oder beim Nationalen Cybersicherheitslagebild zukommt. Die Folge können unnötige Doppelstrukturen und Doppelarbeit, aber auch das vergebliche Vorhalten nicht benötigter Ressourcen sein. Unklarheiten bei der Abgrenzung von Zuständigkeiten können auch dazu führen, dass Aufgaben nicht wahrgenommen werden. Dies kann sich Deutschland angesichts der Bedrohung und der begrenzten Ressourcen nicht leisten.

Das weitere Anwachsen der Akteure in dieser schon sehr komplexen Cybersicherheitsarchitektur kann Unklarheiten hinsichtlich der Ansprechstellen, Kompetenzen und Zuständigkeiten verstärken. Bei Cyberangriffen kann dies zu ineffizienten Melde-, Informations- und Bearbeitungsprozessen führen oder bestehende Defizite vergrößern. Ein gemeinsamer Datenbestand und ein strukturierter Datenaustausch hätten die mehrfache Meldung und Erfassung von Daten vermieden. Beides hätte dazu beitragen können, die Reaktionsfähigkeit der Akteure der Cybersicherheitsarchitektur zu steigern. Z. B. können physische Sicherheitsvorfälle bei kritischen Dienstleistungen unmittelbar die Cybersicherheit beeinflussen oder umgekehrt. Auch sind diese nicht immer trennscharf voneinander abzugrenzen. Daher müssen BSI und BBK sofort und unmittelbar den gleichen Sachstand kennen, um sich abstimmen und handeln zu können. Dies gilt auch für andere Behörden der Cybersicherheitsarchitektur wie BaFin und BNetzA.

[32] Bundesrechnungshof, Bericht nach § 88 Absatz 2 BHO zu dem Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 17. September 2024 (Gz.: VII 4 - 0002698).

Empfehlung

Deutschland benötigt eine robuste Cybersicherheitsarchitektur, um auch bei gravierenden Cyber-Ereignissen schnell und wirksam reagieren zu können. Ziel sollte sein, die Strukturen zu verschlanken und effizienter zu gestalten, um die Schlagkraft zu erhöhen.

Die Bundesregierung muss ihren anstehenden Planungen, u. a.

- → für einen Nationalen Sicherheitsrat,
- → für eine neue Cybersicherheitsstrategie,
- → für eine Zentralstellenfunktion des BSI und
- → vor der Einrichtung möglicher weiterer Institutionen

eine umfassende Analyse der bestehenden Cybersicherheitsarchitektur zugrunde legen. Dazu hat sie das Zusammenwirken der staatlichen Institutionen strukturell und prozessual zu bewerten. Sie muss diese anpassen, um Doppelstrukturen und Barrieren für die Zusammenarbeit abzubauen. Mit auch in der Finanzwelt üblichen Stresstests könnte sie erkennen, inwieweit die Cybersicherheitsarchitektur extremen, aber denkbaren Krisenszenarien standhalten kann.

Diese Bewertungen und Tests betreffen in besonderem Maße das Cyber-AZ, dessen Rolle im Vorfeld und gegebenenfalls bei der Cyberabwehr[33] kritisch zu hinterfragen ist.

Bei der anstehenden Umsetzung der beiden EU-Richtlinien zum Schutz der KRITIS sollte die Bundesregierung bedenken, dass jede weitere Behörde, der sie Aufgaben in der Cybersicherheitsarchitektur zuweist, die Komplexität für alle Beteiligten erhöht. Um diese zumindest abzumildern, sollte sie alle Möglichkeiten der strukturierten, gemeinsamen Datenhaltung nutzen.

Stellungnahme von BMDS und BMI

Die verteilten Zuständigkeiten in den verschiedenen KRITIS-Sektoren ergeben sich vielfach aus europäischen Vorgaben. In deren nationaler Umsetzung sei dafür Sorge getragen, dass mehrfache Meldepflichten vermieden werden und ein vollständiger Lageüberblick beim BSI sichergestellt sei. Mit dem NIS2UmsuCG seien hier weitere Verbesserungen geplant.

Der aktuelle Koalitionsvertrag sehe vor, das Cyber-AZ fortzuentwickeln. Dabei solle auch geklärt werden, welche Rolle ihm bei der Erstellung des Lagebildes „Cyber“ zukommt, um Doppelstrukturen zu vermeiden. Als Plattform für Kooperation und

[33] Dem Bund stehen nach geltendem Verfassungsrecht lediglich in bestimmten Bereichen gefahrenabwehrrechtliche Sonderzuständigkeiten bei Cybergefahrenlagen zu (z. B. in den Bereichen Eigensicherung, internationaler Terrorismus, Grenzschutz oder Sicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes).

Informationsaustausch verfüge das Cyber-AZ über keine Befugnisse für Maßnahmen der Cyberabwehr. Im Krisenfall, wie zuletzt bei der LÜKEX 23, seien die am Cyber-AZ beteiligten Behörden entsprechend ihrer gesetzlich zugewiesenen Aufgaben einbezogen.

Abschließende Würdigung

Abgesehen von punktuellen Hinweisen zu den Aufsichtsbehörden im KRITIS-Bereich sowie zum Cyber-AZ sind BMDS und BMI auf die grundsätzlichen Empfehlungen nicht eingegangen. Der Bundesrechnungshof hält diese uneingeschränkt aufrecht.

Ohne eine vertiefte und umfassende Analyse der bestehenden Cybersicherheitsarchitektur bleiben Handlungsbedarfe, insbesondere infolge deren weitgehend unsystematischen Aufwuchses und verschärfter Bedrohungen im Cyberraum, unerkannt. Dies zeigen auch die aktuellen Erkenntnisse aus der LÜKEX 23. Der Bundesregierung fehlen so wichtige Erkenntnisse für aktuelle Vorhaben. Dazu zählen die überfällige Umsetzung der EU-Richtlinien, die Einrichtung eines Nationalen Sicherheitsrates oder der Ausbau des BSI als dritte Säule einer föderal integrierten Cybersicherheitsarchitektur.

Sobald dem Deutschen Bundestag die neuen Regierungsentwürfe für das NIS2UmsuCG und das KRITIS-DachG vorliegen, beabsichtigt der Bundesrechnungshof daher, die zuständigen Ausschüsse u. a. hinsichtlich etwaiger Anpassungsbedarfe zum Zusammenwirken der betroffenen Behörden zu beraten.

Soweit BMDS und BMI die Bedeutung des Cyber-AZ bei der Bewältigung von Cyberkrisen und bei der Abwehr von Cyberangriffen relativieren, ist dem schon allein die Erwartungshaltung entgegenzuhalten, die sich aus der Bezeichnung „Cyber-Abwehrzentrum“ ergibt. Die Nationale Sicherheitsstrategie definiert das Ziel, dass Deutschland auch im Cyberraum jederzeit reaktionsfähig und wehrhaft sein soll. Der Bundesrechnungshof erwartet, dass die Bundesregierung bei der Weiterentwicklung der Cybersicherheitsarchitektur insbesondere untersucht, ob das Cyber-AZ wirksam zu diesem Ziel beitragen kann und welcher Veränderungen seiner Aufgaben, Kompetenzen und Rechtsstellung es dafür bedarf.

4 Deutschland benötigt sichere Informationstechnik

Sachverhalt

Der Bund betreibt seine IT in über 100 RZ[34]. Auf 17 000 Servern stellen dort 15 000 Fachverfahren große Teile der IT-Dienste der Bundesverwaltung zur Verfügung. Ohne Zugriff auf digital gespeicherte Informationen (beispielsweise Steuer-, Melde- oder Unternehmensdaten) ist die Bundesverwaltung auf Dauer nicht handlungsfähig. Greifen Unbefugte auf die in den RZ gespeicherten schutzbedürftigen Daten zu oder manipulieren deren Verarbeitung, hat dies gravierende Folgen für die Bürgerinnen und Bürger und die Sicherheit Deutschlands.

Unzureichendes IT-Sicherheitsniveau der RZ

Das BSI legt für Einrichtungen des Bundes Mindeststandards für die Sicherheit in der IT fest. Für RZ und die aus ihnen bereitgestellten IT-Dienstleistungen ist dies u. a. der Mindeststandard zum sogenannten komprimierten Hochverfügbarkeitsbenchmark (HVB-kompakt). Der HVB-kompakt definiert 34 Indikatoren, um die Sicherheit von RZ zu bewerten. Das BSI legte für diese 34 Indikatoren Mindestwerte fest, die die RZ für ein gewisses Mindestniveau an Sicherheit erreichen müssen. Je nach individuellem Schutzbedarf eines RZ ist es in der Regel nicht ausreichend, die Mindestwerte lediglich einzuhalten.

Auf Anforderung des Haushaltsausschusses prüft das BSI seit dem Jahr 2015 jährlich bei einer Auswahl von Bundesbehörden, ob deren RZ die Anforderungen des HVB-kompakt erfüllen. Das BSI stellte ein „dramatisches Umsetzungsdefizit in der Cybersicherheit“ fest. Weniger als 10 % der vom BSI untersuchten Behörden erreichten die Mindeststandards.[35]

[34] Im Jahr 2025 betrieb die Bundesverwaltung nach eigenen Angaben 114 RZ selbst und nutzte zusätzlich 21 Fremd-RZ. Vgl. Bundestagsdrucksache 20/15028.

[35] Bericht der Bundesregierung zum Stand der IT-Sicherheit der Rechenzentren der Bundesverwaltung, Analyse der IT-Sicherheit der Rechenzentren der Bundesverwaltung mittels HV-Benchmark - 7. Teilprüfung, Ziffer 3.1.

Notstromversorgung nicht für Krisenlagen gerüstet

Der Blackout[36] auf der Iberischen Halbinsel im April 2025 zeigt das zwingende Erfordernis einer verlässlichen Notstromversorgung. Obwohl die meisten Behörden mit Netzersatzanlagen (NEA) ausgestattet sind, stellte der Bundesrechnungshof fest, dass die Notstromversorgung für kritische IT-gestützte Geschäftsprozesse in Krisenlagen nur unzureichend gesichert ist. Behörden haben keine hinreichenden Vorkehrungen getroffen, um Betrieb, Wartung, Pflege der NEA sowie die Treibstoffversorgung auch außerhalb der Normallage sicherzustellen. Diesen Tatbestand bestätigen auch Untersuchungen des BSI.

Zunehmende Zentralisierung

Die IT-Konsolidierung Bund verfolgt in der Betriebskonsolidierung (BKB) das Ziel, grundsätzlich alle konsolidierungsfähigen IT-Lösungen einer Behörde auf den vom Informationstechnikzentrum Bund (ITZBund) bereitgestellten Standardbetriebsumgebungen in einem zentralen RZ zusammenzuführen. Ungeachtet dessen gibt es eine Vielzahl nicht konsolidierungsfähiger IT-Lösungen. Der Bedarf nach dezentralen RZ besteht weiterhin. Die Bundesverwaltung plant, mindestens 15 neue RZ bis zum Jahr 2026 und darüber hinaus zu bauen.[37]

Das BSI selbst stellte in seinen Prüfberichten wiederholt fest, dass der Hochverfügbarkeit der RZ durch die Zentralisierung vieler Anwendungen und Daten der Bundesverwaltung eine besondere Bedeutung zukomme.

Georedundanz oft nicht vorhanden

Der Bundesrechnungshof befragte elf Behörden, die im Spannungs- und Verteidigungsfall bedeutsame Aufgaben wahrzunehmen haben, um die Staats- und Regierungsfunktionen aufrechtzuerhalten. Danach verfügen deren RZ selbst bei als kritisch bewerteten IT-Diensten über keine Georedundanz[38], in manchen Fällen noch nicht einmal über eine Betriebsredundanz[39].

Für den Fall der Zerstörung eines RZ gaben vier der Behörden an, zwar über keine Betriebs- oder Georedundanz zu verfügen, jedoch regelmäßige Backups anzufertigen.

[36] Unter einem Blackout wird ein unkontrolliertes und unvorhergesehenes Versagen von Netzelementen des europäischen Verbundnetzes verstanden. Das führt in der Folge dazu, dass größere Teile des europäischen Verbundnetzes oder das gesamte Netz ausfallen. Solche Ausfälle der Netzinfrastruktur werden auch „Schwarzfall“ genannt.

[37] Bundestagsdrucksache 20/15028.

[38] Georedundanz bezeichnet die Verteilung von IT-Systemen oder Diensten dieser Systeme auf mehrere geografisch getrennte Standorte (Mindestabstand 200 km), um auch bei großflächigen Störungen (z. B. Naturkatastrophen oder Stromausfällen) den Betrieb aufrechtzuerhalten.

[39] Betriebsredundanz bedeutet, dass IT-Systeme oder Dienste innerhalb eines RZ oder Standorts mehrfach vorhanden sind, um Ausfälle durch Hardware- oder Softwarefehler abzufangen (z. B. doppelte Server, Netzteile oder Speicher).

Keine der Behörden hatte umfänglich getestet, ob sich die in einem RZ betriebenen IT-Dienste basierend auf den angefertigten Backups wiederherstellen lassen.

Beispiele

Ausfall kritischer IT-Dienste der Bundesverwaltung

Im Juli 2023 kam es zu einem Brand der Zuleitung des Energieversorgers in der Mittelspannungsübergabeanlage zu einem RZ des ITZBund. Die Anlagen zur Unterbrechungsfreien Stromversorgung (USV) und die NEA des RZ übernahmen daraufhin die Energieversorgung. Durch einen Fehler der USV konnte das ITZBund die Versorgung nicht vollständig auf die vorgesehene NEA umschalten. Das ITZBund musste die IT-Dienste in dem RZ abschalten. Das ITZBund benötigte 31 Stunden, um den vollen Funktionsumfang des RZ wiederherzustellen. Von dem Ausfall waren auch besonders kritische IT-Dienste betroffen.[40]

Cyberangriff auf Bundesamt für Kartographie und Geodäsie (BKG)

Ein Cyberangriff auf das BKG Ende 2021 verdeutlicht, dass sich längst auch der nachgeordnete Geschäftsbereich im Visier von mutmaßlich staatlichen Angreifern befindet.[41] Die Dienstleistungen des BKG sind u. a. relevant für die Bereiche Verkehr, Katastrophenvorsorge, Innere Sicherheit und Energieversorgung; dies sind ausnahmslos KRITIS-Sektoren oder betrifft staatliche Kernfunktionen.

Distributed Denial of Service (DDoS)-Angriff legt Kommunikationsdienste lahm

Im September 2023 fand ein DDoS-Angriff[42] auf die Bundesverwaltung statt. Aufgrund der gemeinsam genutzten Internet-Infrastruktur waren die Kommunikationsdienste deutlich beeinträchtigt. Beschäftigte der Bundesverwaltung konnten für etwa drei Stunden nur mit massiven Einschränkungen arbeiten.

Das BMI sah in seiner Cybersicherheitsagenda aus dem Jahr 2022 das Ziel vor, die Hochverfügbarkeit der RZ des Bundes zu stärken.[43]

[40] Hierzu gehören insbesondere Dienste mit dem Service Level Gold, für die der jeweilige IT-Dienstleister bei einem Major Incident (Priorität 1) eine maximale Entstörungszeit von 130 Minuten gemäß den Anlagen des Produktkatalogs des Verbunds der IT-Dienstleister Bund zusichert.

[41] Pressemitteilung des BMI zum Cyberangriff auf das BKG, zuletzt abgerufen am 28. April 2025.

[42] Bei einem DDoS-Angriff überlastet ein Angreifer eine Website, einen Server oder eine Netzwerkressource mit Anfragen oder sonstigem Datenverkehr.

[43] Cybersicherheitsagenda des BMI - Ziele und Maßnahmen für die 20. Legislaturperiode, Kapitel 4; zuletzt abgerufen am 19. Mai 2025.

Fehlende finanzielle Mittel

Für die Jahre 2024 bis 2027 meldete das BSI dem BMI einen zusätzlichen Mittelbedarf für den Sondertatbestand „Stärkung der Sabotage-Resilienz von Staat und Wirtschaft" von insgesamt 93 Mio. Euro. Mit diesen Mitteln wollte es u. a.

- → eine Bestandsaufnahme zum Sabotageschutz exponierter IT-Infrastrukturen finanzieren sowie
- → Vorgaben und Handlungsempfehlungen entwickeln, um die Resilienz für IT-Infrastrukturen der öffentlichen Hand zu stärken.

Der Haushaltsvoranschlag des BMI für den Bundeshaushalt 2024 und den Finanzplan bis 2027 sah keine Haushaltsmittel für die Hochverfügbarkeit der RZ oder deren Sabotage-Resilienz vor.

Der Bundesrechnungshof hatte in einem Bericht nach § 88 Absatz 2 BHO bereits im Jahr 2023 empfohlen, die Sicherheit der RZ stärker zu priorisieren. Der Haushaltsausschuss hat sich diesen Forderungen mit seinem Maßgabebeschluss vom 16. November 2023 inhaltlich angeschlossen. In diesem forderte er das BMI auf, angesichts der verschärften Bedrohungslage im Cyberraum und der defizitären IT-Sicherheitssituation in den RZ ihre Prioritäten zugunsten der Cybersicherheit neu auszurichten. Damit die Bundesverwaltung jederzeit handlungsfähig sei, müsse sie die Verfügbarkeit ihrer wesentlichen IT-Infrastrukturen, insbesondere der RZ, sicherstellen.

Keine ressortübergreifende RZ-Strategie

Die IT-Strategie Bund[44] weist übergreifende Ziele und Handlungsfelder für die IT der Bundesverwaltung aus. Ihre Inhalte sind ressortübergreifend für die gesamte IT der Bundesverwaltung verpflichtend. Die IT-Strategie Bund enthält IT-Sicherheitsvorgaben für einzelne RZ.[45] Sie beschreibt keine Ziele oder Vorgaben für die RZ-Landschaft der Bundesverwaltung, mit deren Hilfe die Bundesregierung den Beitrag der bestehenden und neuen RZ zur Hochverfügbarkeit, Kontrollfähigkeit und Souveränität übergreifend steuern will.

Das BMI hat sich für grundlegende Fragen der Krisenresilienz ziviler RZ des Bundes aufgrund des Ressortprinzips nicht zuständig gesehen. In der neuen Bundesregierung hat das BMDS vom BMI auch die Zuständigkeit für die IT-Steuerung, IT-Konsolidierung einschließlich der BKB und damit auch für grundsätzliche Fragen der RZ des Bundes übernommen. Es erhält einen Zustimmungsvorbehalt für alle wesentlichen

[44] IT-Strategie Bund – Leitbild und Ziele, Januar 2023; zuletzt abgerufen am 19. Mai 2025. Bisher ist nur ein Handlungsfeld der IT-Strategie Bund beschrieben, das Handlungsfeld Cloud Computing. Andere wesentliche Handlungsfelder wie Digitale Souveränität, Resilienz und Sicherheit oder Digitale Infrastruktur konkretisierte das BMI bislang nicht.

[45] Die IT-Strategie des Bundes (Leitbild und Ziele) fordert, dass Behörden ihre RZ durch die Methodik des HVB-kompakt bewerten müssen und das jeweils erforderliche IT-Sicherheitsniveau durch IT-Sicherheitszertifizierungen und regelmäßige Audits nachweisen.

IT-Ausgaben der unmittelbaren Bundesverwaltung.[46] Inwieweit es weiterhin den jeweiligen Betreiber in der alleinigen Verantwortung für die Krisenresilienz der RZ sieht, bleibt abzuwarten.

Für flächendeckende Kontrollen und Unterstützung fehlt Personal

Die IT-Steuerungsgremien des Bundes benötigen belastbare Erkenntnisse zur Cybersicherheit, um das ressortübergreifende Informationssicherheitsmanagement des Bundes bewerten und steuern zu können. Seit Dezember 2021 ist das BSI gemäß § 4a BSIG[47] befugt, die IT-Sicherheit in der Bundesverwaltung zu kontrollieren. Für umfassende Kontrollen verfügt das BSI weder über ausreichende personelle noch finanzielle Mittel. Für „flächendeckende" Aussagen zur Informationssicherheit hält es 112 Stellen für erforderlich. Von bislang insgesamt rund 20 zugewiesenen Stellen sind drei mit Beschäftigten besetzt, die flächendeckende Kontrollen durchführen sollen.

Die Bundesverwaltung kann ihre Cybersicherheit nur dann gewährleisten, wenn sie Cyberangriffe rechtzeitig erkennt. Die starke technische Vernetzung der Behörden miteinander macht die Detektion von Cyberangriffen zu einem behördenübergreifenden Erfordernis. Dem BSI kommt dabei neben der Koordinierung auch die operative Umsetzung speziell unter Nutzung der nur ihm gemäß §§ 5 und 5a BSIG zugewiesenen Befugnisse zu. Diese ermöglichen z. B. die Erkennung von Angriffen in den sogenannten Schnittstellendaten. Ziel des BSI ist es auch, möglichst viele Behörden von eigenen Detektionsmaßnahmen zu entlasten.

Beispiel

Potenzial des zentrales Security Operation Center unzureichend ausgeschöpft

Das BSI hat für den Bund ein Security Operation Center aufgebaut, welches gemeinsam mit IT-Dienstleistern des Bundes Cyberangriffe detektieren soll. Gemeinsam mit dem ITZBund bietet das BSI den Dienst Detection-as-a-Service (DaaS) an, an den Behörden ihre Protokollierungsdaten übermitteln können. Das BSI kann diese dann analysieren. Die Zahl der Behörden, die das BSI mit DaaS unterstützen kann, hängt von seinen technischen und personellen Ressourcen ab. Das BSI plant, der gesamten Bundesverwaltung (etwa 200 Behörden) DaaS anzubieten. Bisher nutzen den Service lediglich fünf Behörden. Das BSI gibt an, dass sowohl ihm als auch potenziell nutzenden Behörden die erforderlichen personellen Ressourcen für einen zügigen Ausbau von DaaS fehlen.

[46] Hiervon ausgenommen sind nur der Geschäftsbereich des Bundesministeriums der Verteidigung und der Sicherheits- und Polizeiaufgaben im Geschäftsbereich des BMI, des Bundesnachrichtendienstes sowie der Steuerverwaltung im Geschäftsbereich des BMF.

[47] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

Auch darüber hinaus sind die Bundesbehörden vielfach auf Unterstützung angewiesen, um Defizite in der Informationssicherheit ihrer RZ abstellen zu können. Hierfür sah das BMI in seiner Cybersicherheitsagenda u. a. den Aufbau eines Kompetenzzentrums für operative Sicherheitsberatung der Bundesverwaltung (KoSi Bund) vor. Diesen Sondertatbestand nahm es weder in den Haushalt 2024 noch in den 1. Regierungsentwurf für den Haushalt 2025 auf.

Würdigung

Als für die IT des Bundes federführendes Ressort hätte das BMI mit dem erforderlichen Nachdruck darauf hinwirken müssen, dass die Bundesbehörden angemessene Maßnahmen zur Hochverfügbarkeit der RZ ergreifen und dafür entsprechende Mittel einplanen. Weder waren seine bisherigen Initiativen ausreichend noch erfolgreich.

Auch die verschärfte geopolitische Lage hat erkennbar bislang nicht dazu geführt, die Hochverfügbarkeit der wesentlichen RZ des Bundes verlässlich und nachhaltig zu steigern und somit die Sabotage-Resilienz des Staates zu erhöhen.

Es ist höchst bedenklich, wenn nicht einmal die Notstromversorgung IT-gestützter kritischer Geschäftsprozesse in allen Behörden angemessen sichergestellt ist. Da auch das BSI Mängel in der Notstromversorgung erkannt hat, hätte die Bundesverwaltung schon angesichts der verschärften Bedrohungslage die Mängel mit der erforderlichen Vehemenz beseitigen müssen.

Darüber hinaus sind in weiten Teilen kritische IT-Dienste nicht georedundant abgesichert. Dies birgt für die notwendige Zentralisierung der IT erhebliche Risiken. Die Bundesverwaltung kann dann Staats- und Regierungsfunktionen in Krisenlagen nicht verlässlich aufrechthalten. Dies gilt erst recht im Spannungs- und Verteidigungsfall. Erhebliche Schäden können die Folge sein. Der RZ-Ausfall im ITZBund hat deutlich gemacht, dass dessen bisherige Redundanzmaßnahmen für kritische IT-Dienste nicht ausreichend waren. Hinreichende Redundanzen sind ein wichtiges Instrument, um die Resilienz von IT-Infrastrukturkomponenten wie RZ zu steigern.

Solange das BSI die Kontrollen der IT-Sicherheit in Behörden und RZ des Bundes nicht flächendeckend sowie regelmäßig und in ausreichendem Umfang durchführt, fehlen auch den IT-Steuerungsgremien wichtige Informationen. Sie können den aktuellen Sicherheitszustand der Bundesbehörden nicht vollständig erfassen und entscheiden ohne valide Grundlage. Gleichzeitig fehlt den Bundesbehörden eine kompetente Bewertung ihrer Cybersicherheit. Insbesondere vor dem Hintergrund, dass das BSI in stichprobenartigen Kontrollen bereits erhebliche Defizite bei der IT-Sicherheit der RZ feststellte, ist dieser Zustand beunruhigend.

Ohne eine angemessene personelle Ausstattung der betreffenden Arbeitseinheiten wird das BSI Kontroll- und Detektionsmaßnahmen kaum in dem sachlich gebotenen Umfang durchführen können.

Die Bundesregierung hat bisher keine ressortübergreifende RZ-Strategie erarbeitet. Dadurch kann die Bundesverwaltung nicht gewährleisten, dass ihre RZ-Landschaft die Anforderungen ihrer kritischen Geschäftsprozesse angemessen und hinreichend unterstützt.

In der letzten Legislaturperiode wurde die nicht konsolidierte IT maßgeblich von den jeweiligen Ressorts gesteuert. Sie konnten frei über ihre IT-Mittel verfügen. Das BMI tat sich schwer, seine federführende Verantwortung und Koordinierungsfunktion für das (IT-)Krisenmanagement, die IT-Steuerung des Bundes und die Cybersicherheit angemessen wahrzunehmen. Gleichwohl betrifft der Ausfall von RZ-Kapazitäten in aller Regel längst nicht mehr nur eine einzige Behörde. Ausfälle können die Handlungsfähigkeit der gesamten Bundesverwaltung gefährden. Der neue Ressortzuschnitt in der 21. Legislaturperiode weist dem BMDS eine übergreifende Verantwortung für den Einsatz der IT-Mittel der Ressorts zu. Dies sollte ihm ermöglichen, die erforderlichen Maßnahmen durchzusetzen, um die Resilienz der zentralen und dezentralen IT-Infrastrukturen schnell und umfassend zu stärken.

Empfehlung

Um die Hochverfügbarkeit der RZ des Bundes zu stärken, muss die Bundesregierung geeignete Handlungsoptionen ermitteln und für eine auskömmliche Finanzierung sorgen. Dabei muss sie das Ziel der BKB, den Betrieb der unmittelbaren Bundesverwaltung im ITZBund zusammenzuführen und damit die Anzahl der dezentralen RZ zu reduzieren, angemessen berücksichtigen.

Das künftig für strategische Fragen der IT des Bundes entscheidungsbefugte Gremium muss unter Leitung des BMDS festlegen, wie es die RZ-Landschaft der Bundesverwaltung resilient gestalten kann. Dazu muss es geeignete und alle Behörden bindende strategische Vorgaben erlassen.

Auswirkungen, die die Konsolidierung der IT der Bundesverwaltung auf deren Handlungsfähigkeit im Krisen- und Katastrophenfall haben kann, sollte das BMDS analysieren. Anschließend sollte es darauf hinwirken, dass die Bundesverwaltung geeignete Schutzmaßnahmen ergreift, um die Auswirkungen von Ausfällen kritischer zentraler und dezentraler IT-Dienste zu reduzieren oder zu vermeiden.

Das BMDS sollte Mindestanforderungen an die Notstromversorgung durch NEA in der Bundesverwaltung zur Bewältigung von Krisenlagen erstellen. Es sollte darauf hinwirken, dass alle Behörden diese Mindestanforderungen umsetzen. Alle Behörden sollten

in ihren IT-Sicherheitskonzepten darlegen, wie sie Betrieb und Wartung der NEA unter normalen Bedingungen sowie in Krisenlagen sicherstellen. Das Notfallmanagement sollte das Krisenszenario „Blackout“ berücksichtigen.

Das BSI muss sicherstellen, dass die IT-Steuerungsgremien des Bundes valide und entscheidungsrelevante Informationen über den Zustand der Cybersicherheit des Bundes erhalten. Dazu muss es seine Kontrollen zügig intensivieren und erforderlichenfalls Personal innerhalb des BSI umsetzen. Die Detektion von Cyberangriffen auf die Bundesverwaltung muss es so priorisieren, dass möglichst viele Behörden den DaaS nutzen können.

Stellungnahme von BMDS und BMI

BMDS und BMI haben im Wesentlichen der Würdigung und den Empfehlungen des Bundesrechnungshofes zugestimmt. Die Bundesregierung habe einen partiellen Überblick über den Zustand der Informationssicherheit in der Bundesverwaltung. Die Erkenntnisse aus Prüfungen des BSI seien aber noch unvollständig und nicht tief und aktuell genug, um die Informationssicherheit in der Bundesverwaltung wirksamer steuern zu können. BMDS und BMI wollen DaaS ausbauen und als Standardmaßnahme bei der IT-Konsolidierung Bund integrieren.

Das BMI habe zwar eine koordinierende Rolle in der Zivilen Verteidigung. Für die Krisenresilienz ziviler RZ des Bundes sei es aber aufgrund des Ressortprinzips nicht zuständig. Die Ressorts müssten eigenständig prüfen, welche RZ nötig seien, um die Staats- und Regierungsfunktionen aufrechtzuerhalten, und wie Sie diese RZ (auch in Krisenlagen) schützen können.

Abschließende Würdigung

Auch wenn BMDS und BMI den Empfehlungen im Wesentlichen zustimmen, bleibt unklar, wie und bis wann sie diese umsetzen werden. Dies betrifft vor allem das Vorliegen geeigneter Informationen für die Steuerungsgremien, die anforderungsgerechte Aufgabenwahrnehmung durch das BSI und das Erarbeiten einer ressortübergreifenden RZ-Strategie. Auch lassen BMDS und BMI offen, inwiefern sie dem BSI geeignete personelle Ressourcen für den Ausbau von DaaS bereitstellen wollen.

Der bloße Verweis von BMI und BMDS auf das Ressortprinzip ist angesichts ihrer federführenden Verantwortung und Koordinierungsfunktion für das (IT-)Krisenmanagement, die IT-Steuerung des Bundes und die Cybersicherheit kein hinreichend geeignetes Argument. Dies gilt umso mehr, als es hier um hochkritische IT-Dienste in einzelnen RZ geht, die auch im Spannungs- und Verteidigungsfall im Interesse der gesamten Bundesverwaltung zwingend aufrechterhalten werden müssen. Nicht zuletzt die

LÜKEX 23 hat sehr deutlich gemacht, dass es angesichts der ressortübergreifenden Auswirkungen von potenziellen Angriffen auf IT-Infrastrukturen nicht sachgerecht ist, die Verantwortung für die Krisenresilienz der RZ den Ressorts individuell zu überlassen.

Der Bundesrechnungshof bleibt bei seiner Empfehlung, dass das BMDS gemeinsam mit dem künftig für strategische Fragen der IT des Bundes entscheidungsbefugten Gremium festlegen muss, wie es die RZ-Landschaft der Bundesverwaltung resilient gestalten kann. Dazu muss es geeignete und für alle Behörden bindende strategische Vorgaben festlegen.

Anders als früher das BMI hat das BMDS einen Zustimmungsvorbehalt für alle wesentlichen IT-Ausgaben weiter Teile der unmittelbaren Bundesverwaltung erhalten. Diesen sollte es auch nutzen, um geeignete Schutzmaßnahmen durchzusetzen. Denn die Folgen von Ausfällen kritischer zentraler und dezentraler IT-Dienste muss die Bundesregierung zwingend reduzieren oder vermeiden.

5 Cybersicherheit benötigt angemessene Ressourcen

Sachverhalt

Ausnahmen von der Schuldenbremse

Das Grundgesetz ermöglicht es, die für die Schuldenregel relevanten Krediteinnahmen u. a. um Ausgaben für die Cybersicherheit zu bereinigen. Dies gilt, soweit diese Ausgaben zusammen mit anderen sicherheitsrelevanten Ausgaben 1 % des Bruttoinlandsprodukts überschreiten (Artikel 115 Absatz 2 Satz 4 Grundgesetz; Bereichsausnahme). Dadurch steigt der Verschuldungsspielraum des Bundes. Daneben kann der Bund zusätzliche Investitionen, die u. a. der Cybersicherheit digitaler Infrastrukturen (z. B. Netze des Bundes, Digitalfunk) dienen, aus einem neu geschaffenen Sondervermögen „Infrastruktur“ finanzieren (Artikel 143h Grundgesetz). Diese Ausnahmen von der Schuldenbremse sollen eine Finanzierungsgrundlage der Gesamtverteidigung[48] und sicherheitspolitischer Aufgaben ermöglichen.

[48] Unter Gesamtverteidigung versteht man die Gesamtheit aller militärischen und zivilen Verteidigungsmaßnahmen eines Staates. Vgl. Rahmenrichtlinie für die Gesamtverteidigung.

Für beide Regelungen stellt sich die Frage, was unter den Begriff „Ausgaben für Cybersicherheit“ beziehungsweise „Ausgaben für den Schutz der informationstechnischen Systeme“ fällt und in welcher Höhe diese Ausgaben im Bundeshaushalt derzeit bereits veranschlagt sind. Bislang konnte das BMI diese Frage nicht beantworten. Für die Aufstellung des 2. Regierungsentwurfs des Bundeshaushalts 2025 hat das BMF den Ressorts Hinweise gegeben, wie sie die Ausgaben für den Schutz der informationstechnischen Systeme zu veranschlagen haben.[49] Ziel ist, die Ausgabenansätze, die die sogenannte „Bereichsausnahme gemäß Artikel 109/115 Grundgesetz“ betreffen, eindeutig abgrenzen zu können. Das BMF hat nicht erläutert, was unter diese Ausgaben im Einzelnen fällt. Die Ressorts sollen stattdessen bestätigen, dass die entsprechenden Ausgaben dem in Artikel 115 Grundgesetz vorgegebenen Begriff entsprechen.[50]

Zwischenzeitlich hat das BMF den Entwurf für eine Ergänzung des Gesetzes zur Ausführung von Artikel 115 des Grundgesetzes; G 115 vorgelegt.[51] Danach sollen die Ausgaben, die unter die Bereichsausnahme fallen, auf Ebene der Einzelpläne, Kapitel oder Titel im jährlichen Haushaltsgesetz näher bestimmt werden. Eine inhaltliche Eingrenzung der Ausgaben, die über die Formulierung im Grundgesetz hinausgeht, enthält der Gesetzentwurf nicht.

Cybersicherheit ist vielfach immanenter Bestandteil von Hardware, Software oder IT-Dienstleistungen. Denn Prinzipien wie „Security-by-Default“[52] und „Security-by-Design”[53] sollen dazu führen, dass Cybersicherheit allen Entwicklungs- und Nutzungsphasen von IT und Digitalisierung inhärent ist. Entsprechende Beschaffungen oder Dienstleistungen anteilsmäßig der Cybersicherheit zuzuordnen, ist bisher im Bundeshaushalt nicht vorgesehen.

Personal für Cybersicherheit

Abgesehen von ausreichenden Finanzmitteln benötigt die Bundesverwaltung auch qualifiziertes Personal für Cybersicherheit. Von den hierfür aktuell vorhandenen 4 415 Planstellen und Stellen (im Folgenden: Stellen) waren zuletzt 684 bzw. 15 % nicht besetzt.[54] Um die neuen Anforderungen aus der NIS-2-Richtlinie umzusetzen, gaben die

[49] Rundschreiben und Verfahrenshinweise des BMF für die Aufstellung des Bundeshaushalts 2025 (2. Regierungsentwurf), der Eckwerte 2026 bis 2029, des Regierungsentwurfs 2026 und des Finanzplans bis 2029 vom 19. Mai 2025.

[50] Information des BMF vom 7. Mai 2025 zur „Veranschlagung der Ausgaben der Bereichsausnahme gem. Artikel 109/115 Grundgesetz im Rahmen der Aufstellung des 2. RegE 2025 sowie des RegE 2026 und Fpl. bis 2029“.

[51] Entwurf einer Formulierungshilfe für die Fraktionen der CDU/CSU und SPD zu dem Entwurf eines Haushaltsbegleitgesetzes 2025.

[52] Security-by-Default bedeutet, dass ein System oder eine Software standardmäßig mit sicheren Einstellungen ausgeliefert wird – also so konfiguriert ist, dass Sicherheitsrisiken minimiert werden, ohne dass der Nutzer manuell eingreifen muss. Ziel ist es, Sicherheitslücken durch unsichere Voreinstellungen zu vermeiden.

[53] Security-by-Design bedeutet, dass Sicherheitsaspekte von Anfang an in den Entwicklungsprozess eines Systems oder einer Software integriert werden. Sicherheit ist dabei ein grundlegender Bestandteil der Architektur und kein nachträglich hinzugefügtes Merkmal.

[54] Antwort des BMI auf die Schriftliche Frage 25 der Abgeordneten Domscheit-Berg vom 22. Januar 2025, Bundestagsdrucksache 20/14639.

Bundesbehörden einen zusätzlichen Bedarf von 1 034 Stellen an.[55] Obwohl die Anforderungen für alle Ressorts nahezu identisch sind, wichen die Bedarfsmeldungen vergleichbarer Geschäftsbereiche deutlich voneinander ab.[56]

Beispiel

Angaben der Ressorts zum Personalbedarf für Informationssicherheit

Das bisherige Bundesministerium für Bildung und Forschung (BMBF)[57] – insgesamt rund 1 400 Stellen, keine Geschäftsbereichsbehörde – ging davon aus, dass es 0,5 zusätzliche Stellen benötigt, um die Verpflichtungen aus dem NIS2UmsuCG umzusetzen. Das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung – ebenfalls ohne Geschäftsbereich, mit gut 1 100 Stellen kleiner als das BMBF – wies den zusätzlichen Bedarf hingegen mit zwölf Stellen aus. Anhaltspunkte, warum Ministerien mit ähnlich vielen Beschäftigten bei identischen neuen Anforderungen ihren Personalbedarf so unterschiedlich bezifferten, waren nicht ersichtlich.

Bundesbehörden hatten wiederholt darauf hingewiesen, für die Cybersicherheit stehe ihnen zu wenig Fachpersonal zur Verfügung. Der Bundesrechnungshof empfahl dem BMI u. a., das vorhandene IT-Personal zu entlasten und dadurch Kapazitäten zu schaffen. Es sollte den IT-Grundschutz auf die Bedürfnisse der Behörden hin überprüfen und anpassen. Als Standard für die Informationssicherheit in der Bundesverwaltung sieht dieser vor, dass jede Behörde bis zu 1 500 Seiten an Vorgaben und Hinweisen beachten und bis zu 150 Konzepte und Richtlinien erstellen und fortlaufend aktualisieren muss.[58] Der Rechnungsprüfungsausschuss des Haushaltsausschusses des Deutschen Bundestages (Rechnungsprüfungsausschuss) hat das BMI daraufhin aufgefordert, den IT-Grundschutz zu vereinfachen und zu untersuchen, inwieweit die bisherigen Maßnahmen ausreichend wirksam sind, um den steigenden Bedarf an Fachkräften für die Informationssicherheit zu decken.[59]

Zentrales Budget

Auf Beschluss des Haushaltsausschusses im Jahr 2023 sollte das BMI prüfen, inwieweit ein zentrales Cybersicherheitsbudget eingerichtet werden kann. Dieses sollte sich aus anteiligen – beispielsweise prozentual an den jeweiligen IT-Ausgaben orientierten –

[55] Entwurf eines NIS2UmsuCG, Bundestagsdrucksache 20/13184, Seite 97 ff.
[56] Bundesrechnungshof, Bericht nach § 88 Absatz 2 BHO zu dem Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 17. September 2024 (Gz.: VII 4 - 0002698).
[57] In der 21. Legislaturperiode: Bundesministerium für Technologie und Raumfahrt.
[58] Bemerkungen 2022 zur Haushalts- und Wirtschaftsführung des Bundes - Ergänzungsband, Bundestagsdrucksache 20/6530, Nummer 25 „Bundesbehörden bei Informationssicherheit zentral unterstützen und IT-Personal entlasten“.
[59] 14. Sitzung des Rechnungsprüfungsausschusses am 16. Juni 2023, Top 10.b).

Beiträgen aller Ressorts zusammensetzen. Diesem Auftrag sind das BMI und die übrigen Ressorts bislang nicht mit dem gebotenen Nachdruck nachgekommen. Ein zentrales Budget für Cybersicherheit ist weder im Entwurf der Bundesregierung der 20. Legislaturperiode für den Bundeshaushalt 2025 noch im Finanzplan bis 2028 vorgesehen.

Beispiel

Explizite Ausgaben für Zwecke der IT- oder Cybersicherheit im Haushaltsentwurf 2025

Der Entwurf der Bundesregierung der 20. Legislaturperiode für den Haushalt 2025 enthielt – über sechs Einzelpläne verteilt – insgesamt acht Titel, die in der Zweckbestimmung oder in den Erläuterungen den expliziten Einsatz (auch) für Zwecke der IT- oder Cybersicherheit vorsahen. In der Summe waren hier 233 Mio. Euro an Ausgaben vorgesehen.[60] Ein Titel, aus dem ressortübergreifende Maßnahmen finanziert werden können, gehörte nicht dazu.

Informationssicherheitscontrolling

Daten zum Ressourceneinsatz der Bundesbehörden für die Informationssicherheit liegen den Entscheidungsträgern im IT-Rat derzeit ebenso wenig vor, wie dieser über detaillierte Informationen zum Stand der Informationssicherheit verfügt (vgl. Tz. 4). Einzige Datenquelle ist derzeit die Sachstandserhebung des IT-Planungsrates zur Umsetzung der Leitlinie der Informationssicherheit der öffentlichen Verwaltung. Auf der Basis von 26 Kennzahlen erhält der IT-Rat hier einmal im Jahr eine zusammengefasste Selbsteinschätzung der Ressorts. Der Bundesrechnungshof mahnte daher fehlende, belastbare Informationen für eine wirksame Steuerung an.[61] Der Rechnungsprüfungsausschuss hat das BMI daraufhin aufgefordert, ein Informationssicherheitscontrolling bis Ende des Jahres 2025 aufzubauen, mit dem sich steuerungsrelevante Daten zur Informationssicherheit in der Bundesverwaltung identifizieren, analysieren und interpretieren lassen.[62]

Würdigung

Die aktuellen technischen Hinweise des BMF, wie die Ausgaben für Cybersicherheit zu veranschlagen sind, schaffen eine wichtige formale Voraussetzung, um diese von denjenigen IT-Ausgaben abzugrenzen, die nicht die Ausnahmeregelung des Artikel 115 Grundgesetz betreffen. Die ungleich bedeutsamere Frage, was unter die Ausgaben für

[60] Hinzu kommen Ausgaben von 217 Mio. Euro, die im Kapitel 0623 für das BSI veranschlagt sind.
[61] Bemerkungen 2022 zur Haushalts- und Wirtschaftsführung des Bundes - Ergänzungsband, Bundestagsdrucksache 20/6530, Nummer 24 „Informationssicherheit: IT-Rat bleibt trotz erheblicher Defizite untätig“.
[62] 14. Sitzung des Rechnungsprüfungsausschusses am 16. Juni 2023, Top 10.a).

Cybersicherheit fällt, bleibt allerdings auch nach Vorlage des Entwurfes einer Anpassung des G 115 weiterhin ungeklärt. Wenn das BMF in dem Gesetzentwurf darauf verweist, die Ausgaben würden im jährlichen Haushaltsgesetz näher bestimmt, dann ist das zwar formal – durch den Ausweis in separaten Titeln – zutreffend; inhaltlich und im Hinblick auf eine über mehrere Haushaltsjahre hinweg vergleichbare Veranschlagung der Ausgaben für Cybersicherheit hilft dies aber nicht weiter. Solange die Ressorts dazu keine Vorgaben erhalten, werden sie die Frage, was hierunter fällt, unterschiedlich beantworten. Die zum Teil erheblichen, nicht nachvollziehbaren Differenzen beim Stellenbedarf für das Informationssicherheitspersonal zeigen, dass dies bereits der Fall ist. Wenn das BMF die Ausgaben für Cybersicherheit nicht angemessen eingrenzt, könnten diese den Bundeshaushalt in einem Umfang belasten, der kaum kalkulierbar ist. Die Bereichsausnahme ermöglicht nämlich, diese im Ergebnis prinzipiell unbegrenzt durch Schulden zu finanzieren. Anders als bei den übrigen Bereichsausnahmen fehlen hier jegliche Vergleichsinformationen zur Höhe der bisherigen Ausgaben.

Das BMI hat bereits erkannt, dass das BSI den IT-Grundschutz vereinfachen und untersuchen muss, inwieweit die bisherigen Maßnahmen ausreichend wirksam sind. Dies ist eine wichtige Voraussetzung, um den steigenden Bedarf an Fachkräften für die Informationssicherheit zu decken. Das BMDS ist nun in der Pflicht, dies gemeinsam mit BMI und BSI fortzuführen.

Solange Ergebnisse zu dem Prüfauftrag des Haushaltsausschusses ausstehen, lassen sich die Vor- und Nachteile der Bündelung von Maßnahmen in einem zentralen Cybersicherheitsbudget nicht bewerten. Synergie- und Skaleneffekte, die durch eine Steuerung und Finanzierung von Maßnahmen an zentraler Stelle eröffnet werden würden, sind so derzeit nicht bezifferbar.

Den Entscheidungsträgern in den IT-Steuerungsgremien, aber auch dem Haushaltsgesetzgeber, fehlt das zentrale Instrument, um die Wirtschaftlichkeit und die Wirkung der von ihnen verantworteten Cybersicherheitsmaßnahmen übergreifend und umfassend bewerten zu können. Denn sie haben keine gesicherten fortlaufenden Informationen über den Ressourceneinsatz und den Status der Informationssicherheit in der Bundesverwaltung. Angesichts der Verzögerungen, u. a. bei den Kontrollen des BSI (vgl. Tz. 4), bezweifelt der Bundesrechnungshof, dass es dem BMDS bis Ende des Jahres 2025 gelingen wird, das Informationssicherheitscontrolling, wie vom BMI zugesichert, aufzubauen und mit belastbaren Daten zu befüllen.

Empfehlung

Die Bundesregierung sollte den Begriff „Ausgaben für Cybersicherheit (beziehungsweise den Schutz der informationstechnischen Systeme)“ mit dem Ziel konkretisieren, dass alle Ressorts auf der Grundlage eines einheitlichen Verständnisses vergleichbare Angaben machen. Ungeachtet dessen, dass der Haushaltsgesetzgeber Details im

jährlichen Haushaltsplan regeln kann, sollte der Rahmen für den Geltungsbereich dieser Bereichsausnahme bereits in dem dauerhaft geltenden G 115 näher vorgegeben werden.

Angesichts der hohen Anzahl unbesetzter Stellen sollte das BMI gemeinsam mit dem BMDS prüfen, inwieweit zusätzliche Maßnahmen zu ergreifen sind, um Fachkräfte für die Bundesverwaltung zu gewinnen. Denn die anstehende Umsetzung der NIS-2-Richtlinie führt zu einem weiter steigenden Bedarf an Fachkräften für die Informationssicherheit. Das BSI muss seine Bemühungen zum Erfolg führen, um den IT-Grundschutz in der Umsetzung zu vereinfachen und praxisgerechter zu gestalten.

Das BMDS sollte zeitnah, möglichst noch im Haushaltsaufstellungsverfahren für das Jahr 2026, sachgerechte Einsatzbereiche und Finanzierungsmodelle für ein zentrales Cybersicherheitsbudget ausarbeiten und mit den Ressorts, insbesondere aber mit dem BMF, abstimmen.

Die Bundesregierung sollte geeignete Steuerungsstrukturen schaffen, die es ihr ermöglichen, knappe Haushaltsmittel effektiv für die Cybersicherheit einzusetzen. Hierzu sollte sie das Informationssicherheitscontrolling zügig etablieren.

Stellungnahme von BMDS und BMI

Das BMI hat auf die Schwierigkeit verwiesen, vergleichbare Angaben zu den Ausgaben der Ressorts für Vorhaben der Cybersicherheit zu erheben. Eine entsprechende Abfrage habe deutlich gemacht, dass es hier bislang an einheitlichen Kriterien fehle, um beispielsweise Ausgaben für die IT-Sicherheit von denen des IT-Betriebs eindeutig abzugrenzen. Gemeinsam mit den Ressorts solle in der aktuellen Legislaturperiode ein Verfahren entwickelt werden, wie Ausgaben für die Cybersicherheit einheitlicher und damit vergleichbarer erhoben werden können.

Um die Behörden zu entlasten, habe das BMI das KoSi Bund konzipiert, aber in Ermangelung von Haushaltsmitteln nicht umsetzen können. Demselben Ziel diene der neue sogenannte „IT-Grundschutz ++“, den das BSI derzeit entwickele.

Nach Ansicht des BMI setze ein zentrales Budget für Cybersicherheit zusätzliche Mittel aus dem Gesamthaushalt voraus. Je nach Ausgestaltung bedürfe dies der Zustimmung aller Ressorts. Diese habe sich bislang nicht abgezeichnet. Möglicherweise eröffne jedoch die Bereichsausnahme für den „Schutz der informationstechnischen Systeme“ neue Optionen.

Derzeit setze die Bundesregierung die neu konzipierte IT-Rahmenplanung um. Diese schaffe im Ergebnis eine übergreifende Transparenz über die vereinheitlichte IT-Budget-Planung der Bundesbehörden.

Abschließende Würdigung

BMDS und BMI erkennen den vom Bundesrechnungshof aufgezeigten Handlungsbedarf an; ihre vorgesehenen Maßnahmen sind jedoch nicht ausreichend ambitioniert und greifen zum Teil zu kurz. Die Haushaltsplanungen für die Jahre 2025 (2. Regierungsentwurf) und 2026 sind weit fortgeschritten. Es ist daher sehr zeitnah – und nicht erst im Laufe der aktuellen Legislaturperiode – notwendig, den Bundesbehörden einheitliche Vorgaben zu machen, welche IT-Ausgaben sie zukünftig innerhalb der Bereichsausnahme gemäß Artikel 109 Grundgesetz und Artikel 115 Grundgesetz veranschlagen dürfen.

BMI und BMDS haben für das KoSi Bund auch im 2. Regierungsentwurf 2025 keine Haushaltsmittel angemeldet. Sie bleiben damit erneut den Nachweis schuldig, die Bundesbehörden tatsächlich entlasten zu wollen. Inwieweit der „IT-Grundschutz ++“ dies zu leisten vermag, bleibt abzuwarten.

Der Bundesrechnungshof teilt nicht die Auffassung, dass ein zentrales Budget für Cybersicherheit „on top“ finanziert werden müsse. Ganz im Gegenteil könnte ein solches ressortübergreifendes Budget ein wirksames Instrument sein, um Synergie- und Skalenpotenziale zu erschließen. Dadurch bedingte Einsparungen würden Freiräume für Projekte von ressortübergreifender Relevanz schaffen, ohne dass hierfür zusätzliche Mittel aus dem Gesamthaushalt erforderlich wären.

Eine vereinheitlichte IT-Budgetplanung ist ein erster wichtiger Schritt zu mehr Transparenz. Ein wirksames Controlling setzt jedoch voraus, dass diese Plandaten fortlaufend mit den Ist-Daten zum Ressourceneinsatz und zum aktuellen Status der Informationssicherheit abgeglichen werden. Davon ist die Bundesverwaltung noch weit entfernt. Der Bundesrechnungshof hält daher an seiner Würdigung und seinen Empfehlungen uneingeschränkt fest.

6 Fazit

Die neue Bundesregierung steht im Bereich der Cybersicherheit vor wichtigen Aufgaben. Sie muss die **NIS-2-Richtlinie** der Europäischen Union zügig in nationales Recht umsetzen. Da die Frist hierfür im Oktober 2024 abgelaufen ist, läuft bereits ein Vertragsverletzungsverfahren der EU-Kommission. Gleiches gilt für die ebenfalls überfällige Umsetzung der **CER-Richtlinie** der Europäischen Union durch das sogenannte KRITIS-DachG. Die Regelungen zum Schutz der physischen und der Cybersicherheit

kritischer Infrastrukturen (einschließlich der Bundesverwaltung) muss die Bundesregierung eng aufeinander abstimmen.

Die Cybersicherheitsstrategie bedarf der dringenden Überarbeitung und Anpassung an die verschärfte Bedrohungslage. Hierzu muss die Bundesregierung

- → zunächst die Defizite der Fähigkeiten Deutschlands im Bereich der Cybersicherheit ermitteln und deren Ursachen analysieren,
- → daraus überprüfbare Ziele ableiten und diese priorisieren,
- → die Umsetzung der erforderlichen Maßnahmen von Beginn an zentral steuern, überwachen und kontrollieren sowie
- → Vorsorge für deren angemessene Finanzierung, beispielsweise durch ein Zentralbudget, treffen.

Zusammen mit der Cybersicherheitsstrategie muss die Bundesregierung die **Cybersicherheitsarchitektur** auf den Prüfstand stellen. Unklare Zuständigkeiten und Doppelarbeit kann und darf sich Deutschland nicht länger leisten. Deutschland benötigt eine robuste Cybersicherheitsarchitektur, um auch bei gravierenden Cyber-Ereignissen schnell und wirksam reagieren zu können. Hierzu sollte die Bundesregierung die Cybersicherheitsarchitektur insbesondere Stresstests unterziehen und auf der Grundlage der dabei gewonnenen Erkenntnisse mit dem Ziel einer Verschlankung reformieren. Mit einer gemeinsamen Datenbank und einem strukturierten Datenaustausch lassen sich Mehrfacherfassungen und Bürokratie vermeiden. Außerdem verbessert dies die Zusammenarbeit der für die KRITIS-Betreiber zuständigen Behörden.

Insbesondere die **Rechenzentren** und die sie verbindenden Netze sind die Achillesferse für die staatliche IT. Es kommt daher entscheidend darauf an, dass

- → das BSI auf der Grundlage seiner gesetzlichen Kontrollbefugnisse den IT-Steuerungsgremien des Bundes valide und entscheidungsrelevante Informationen über den Zustand der Cybersicherheit des Bundes bereitstellt,
- → die Bundesregierung auf der Grundlage einer ressortübergreifenden RZ-Strategie geeignete Handlungsoptionen ermittelt und für eine auskömmliche Finanzierung sorgt, um die Hochverfügbarkeit der RZ des Bundes zu stärken,
- → die Bundesregierung den Auswirkungen, die sich durch die Zentralisierung der IT des Bundes bereits in der Normallage, erst recht aber im Spannungs- und Verteidigungsfall ergeben, entgegenwirkt, indem sie geeignete Schutzmaßnahmen ergreift, um die Folgen von Ausfällen kritischer zentraler und dezentraler IT-Dienste zu reduzieren oder zu vermeiden,
- → das BMDS Mindestanforderungen für den Einsatz von NEA in der Bundesverwaltung zur Bewältigung von Krisenlagen erarbeitet und darauf hinwirkt, dass alle Behörden diese umsetzen.

Mit den aktuellen Grundgesetzänderungen rückt auch die **Finanzierung von Cybersicherheitsmaßnahmen** in den Fokus. Hierzu fehlen bislang aber wesentliche Grundlagen. Die Bundesregierung muss daher

- → zügig, zweckmäßigerweise anlässlich des aktuellen Entwurfs zur Änderung des G 115, konkret festlegen, was unter den Begriff „Ausgaben für Cybersicherheit" fällt (und was nicht),
- → die Anwendung des IT-Grundschutzes vereinfachen, um das Personal zu entlasten,
- → sachgerechte Einsatzbereiche und Finanzierungsmodelle für ein zentrales Cybersicherheitsbudget ausarbeiten und abstimmen und
- → ein geeignetes Informationssicherheitscontrolling etablieren, das es ihr ermöglicht, den effektiven Einsatz der Haushaltsmittel für Zwecke der Cybersicherheit zu planen, zu steuern und zu überwachen.

BMDS und BMI haben zusammenfassend auf die Eigenverantwortung von Ressorts und Behörden für die Informationssicherheit verwiesen. Es sei gleichwohl gelungen, dass u. a. das BSI diese fortlaufend besser berate, unterstütze und praxisorientierte Hilfestellungen anbiete. Die angespannte Haushaltslage habe bisher weitere bedarfsgerechte Maßnahmen nur eingeschränkt ermöglicht. Mit der Gründung des BMDS, der Umsetzung der NIS-2-Richtlinie und den geplanten Kontrollen durch das BSI stelle die Bundesregierung das Informationssicherheitsmanagement des Bundes besser auf. Dabei wolle sie die Empfehlungen des Bundesrechnungshofes berücksichtigen.

Der Bundesrechnungshof sieht angesichts der gewaltigen Bedrohungen im Cyberraum die einzelnen Ressorts und Behörden überfordert, alleine Cybersicherheit dauerhaft auf dem erforderlich hohen Niveau zu gewährleisten. Anders als in den zurückliegenden Jahrzehnten muss es der Bundesregierung daher gelingen, die Kräfte der Ressorts zu bündeln und Synergien zu erzeugen. Es stehen auch weiterhin nur eingeschränkt Ressourcen zur Verfügung. Diese gilt es effektiv und effizient mit größtmöglicher Wirkung einzusetzen. Hierfür kann die vorgesehene vereinheitlichte Budgetplanung und der Zustimmungsvorbehalt des BMDS für alle wesentlichen IT-Ausgaben einen wichtigen Beitrag leisten. Die Eigenverantwortung der Ressorts steht einer übergreifenden Steuerung und Finanzierung nicht entgegen. Denn Eigenverantwortung erfordert in einem engvernetzten und digitalisierten Staat, eigene Ziele hinter dem übergeordneten Ziel der Aufrechterhaltung von Staats- und Regierungsfunktionen zurückzustellen.

Essers Scherwa

Beglaubigt: Trimborn, Amtsinspektorin
Wegen elektronischer Bearbeitung ohne Unterschrift und Dienstsiegelabdruck.