

25 Bundesbehörden bei Informationssicherheit zentral unterstützen und IT-Personal entlasten

Zusammenfassung

Umfangreiche und komplexe Vorgaben zur Informationssicherheit sowie fehlendes IT-Personal führen dazu, dass Bundesbehörden wichtige Sicherheitsmaßnahmen über viele Jahre hinweg unzureichend oder gar nicht umsetzten.

Jede Bundesbehörde ist selbst für die Sicherheit der von ihr verarbeiteten Informationen verantwortlich. Sie muss Sicherheitskonzepte erstellen und geeignete technische sowie organisatorische Maßnahmen umsetzen. Die Vorgehensweise ist im sogenannten IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) festgelegt. Der IT-Grundschutz richtet sich an unterschiedlichste Adressaten aus dem öffentlichen wie privaten Sektor. Er enthält viele umfangreiche und komplexe Vorgaben, Empfehlungen und Maßnahmen.

Der Bundesrechnungshof prüfte seit dem Jahr 2015 die Informationssicherheit in 22 Bundesbehörden. Dabei stellte er wiederholt teilweise gravierende technische und organisatorische Mängel sowie eine unzureichende Personalausstattung fest.

Über die Prüfungsergebnisse unterrichtete er das BMI mehrfach – zuletzt im Jahr 2020.

Der Bundesrechnungshof fragte bei 15 geprüften Behörden nach, ob sie die Mängel inzwischen behoben hatten. Im Ergebnis hatten die Behörden noch nicht einmal alle gravierenden Mängel beseitigt. Rund drei Viertel der befragten Behörden begründeten dies mit fehlendem IT-Personal.

Dem BMI ist seit Jahren bekannt, dass Behörden auch wegen des IT-Personalmangels den IT-Grundschutz unzureichend umsetzen. Um das vorhandene IT-Personal zu entlasten, hätte es den IT-Grundschutz auf die Bedürfnisse der Bundesbehörden hin überprüfen und anpassen müssen. Das BSI hätte beispielsweise speziell auf die Bundesverwaltung zugeschnittene Lösungen erarbeiten können, die musterhaft zur Informationssicherheit beitragen. Das vorhandene IT-Personal in der Bundesverwaltung würde dadurch entlastet und könnte sich darauf konzentrieren, Gefahren und Angriffe zu erkennen sowie Mängel zu beheben.

25.1 Prüfungsfeststellungen

Die Funktionsfähigkeit des Gemeinwesens in Deutschland ist auf zuverlässige und gegen Manipulation geschützte digitale Kommunikation und Datenverarbeitung angewiesen. Sind staatliche IT-Infrastrukturen, z. B. infolge von Cyber-Angriffen, nicht verfügbar oder gestört, kann dies die verfassungsrechtlich garantierte Aufgabenerfüllung des Staates gefährden. Das BMI ist das federführende Ressort im Bereich der Informationssicherheit. Das BSI im Geschäftsbereich des BMI ist die zentrale Informationssicherheitsbehörde des Bundes. Es hat die gesetzliche Aufgabe, die Bundesverwaltung in Fragen der Informationssicherheit zu beraten und zu kontrollieren. In seinem aktuellen Lagebericht schätzt das BSI die Bedrohung durch Cyber-Angriffe so hoch wie nie zuvor ein.

Ungeachtet ihrer spezifischen gesetzlichen Aufgaben haben alle Bundesbehörden vergleichbare Bedarfe und nutzen u. a. Server, IT-Netzwerke sowie E-Mail- und Datenbanksysteme. Sie sind verpflichtet,

- den Schutzbedarf für ihre Geschäftsprozesse zu bestimmen,
- ihre IT entsprechend abzusichern sowie
- sensible Informationen zu schützen.

Dafür müssen die Behörden Sicherheitskonzepte erstellen, fortlaufend pflegen und die darin definierten organisatorischen und technischen Sicherheitsmaßnahmen umsetzen. Sie müssen ein behörden spezifisches Informationssicherheitsmanagement aufbauen, das erforderliche Managementprinzipien, Ressourcen und Sicherheitsprozesse definiert. Die Vorgehensweise ist im sogenannten IT-Grundsatz des BSI festgelegt.

IT-Grundsatz des BSI – umfangreich und komplex

Der IT-Grundsatz richtet sich an unterschiedlichste Adressaten. Behörden und Unternehmen sollen ihn nutzen können – unabhängig von ihrer Größe und ihrem Schutzbedarf. Daher ist der IT-Grundsatz bewusst allgemeingültig und zum Teil sehr abstrakt gehalten. Er soll seine Adressaten systematisch anleiten, Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Der IT-Grundsatz besteht insbesondere aus den BSI-Standards und dem IT-Grundsatz-Kompendium. Er betrachtet neben technischen Aspekten auch organisatorische, personelle und infrastrukturelle Themen. Ferner erklärt er, welche Konzepte erforderlich sind und wie die Adressaten diese erstellen sollen. Er beschreibt Gefährdungen für die Informationssicherheit und listet Anforderungen auf, um diesen zu begegnen.

Jede Behörde der Bundesverwaltung muss zunächst die Empfehlungen des IT-Grundsatzes auf ihre Bedarfe hin anpassen, Vorüberlegungen anstellen und zwischen vielen Handlungsoptionen auswählen. Sie muss dazu bis zu 1 500 Seiten an Vorgaben und Hinweise durcharbeiten, mit ihrem Schutzbedarf abgleichen und bis zu 150 Konzepte, Richtlinien, Leitfäden und Handbücher erstellen. Die Pflichten des IT-Grundsatzes führen damit zu einem erheblichen Aufwand. Zum Teil benötigen die Behörden mehrere Jahre, um alle

notwendigen Konzepte zu erstellen. Diese wiederum ziehen tausende technische und organisatorische Sicherheitsmaßnahmen nach sich, die jede Behörde dann individuell umsetzen und ständig aktualisieren muss.

Auch Behörden, deren IT in der IT-Konsolidierung Bund teilweise zentralisiert wurde, müssen weiterhin die Anforderungen des IT-Grundschutzes beachten.

Mangel an IT-Personal erschwert ausreichende Informationssicherheit

Der Bundesrechnungshof prüfte in den Jahren 2015 bis 2019 die Informationssicherheit in 22 Bundesbehörden. Er stellte wiederkehrend zum Teil gravierende Mängel fest. Dabei handelte es sich einerseits um technische Mängel, wie unzureichend abgesicherte IT-Netzwerke, veraltete oder falsch konfigurierte Software und ungeeignete Werkzeuge zur Administration der IT. Andererseits bestanden Mängel im organisatorisch-konzeptionellen Bereich. Die Behörden sagten zu, die aufgezeigten Sicherheitsmängel zu beheben. Wiederholt stellte der Bundesrechnungshof auch fest, dass das IT-Personal im Bereich der Informationssicherheit nicht ausreichte. Über seine Erkenntnisse unterrichtete er in den Jahren 2019 und 2020 das BMI.

Der Bundesrechnungshof fragte bei 15 geprüften Behörden nach, ob die bei der jeweiligen Prüfung identifizierten Mängel inzwischen behoben waren. Im Ergebnis zeigte sich, dass die Behörden noch nicht einmal alle gravierenden Mängel beseitigt hatten. Rund drei Viertel der Behörden begründeten dies damit, dass

- ihnen zu wenig IT-Personal für die vielfältigen Aufgaben der Informationssicherheit bewilligt worden sei oder
- IT-Personal infolge hoher Abgänge im IT-Bereich fehle und
- neues IT-Personal schwierig zu gewinnen sei.

Die alternative Unterstützung durch externe Auftragnehmer scheitere oft daran, dass auch diese vom Fachkräftemangel betroffen seien. Sie könnten Beratungs- und Unterstützungsaufträge nicht annehmen oder lieferten zum Teil schlechte Arbeitsergebnisse ab.

Eine Umfrage des BMI innerhalb der Bundesverwaltung kam im August 2021 zu folgendem Ergebnis: Der IT-Grundschutz werde wegen fehlenden IT-Personals und fehlender Muster und Vorlagen für Konzepte und Richtlinien nicht vollumfänglich umgesetzt. Weiterhin beklagten die Befragten eine zu komplizierte Struktur und schwer umsetzbare Anforderungen des IT-Grundschutzes.

25.2 Würdigung

Angesichts der Bedrohungslage durch Cyber-Angriffe stellen die Sicherheitsmängel in den Behörden eine erhebliche Gefahr für die gesamte Bundesverwaltung dar. Im Falle eines

gelingenen Cyber-Angriffs trägt die jeweilige Behördenleitung die Verantwortung für Schäden, die abwendbar gewesen wären. Sie muss daher der Informationssicherheit eine hohe Priorität einräumen und festgestellte gravierende Mängel kurzfristig und vollständig beheben. Gleichwohl zeigen die Untersuchungen des Bundesrechnungshofes, dass bekannte Mängel bereits seit Jahren fortbestehen.

Der IT-Grundschutz ist ein wichtiges Rahmenwerk, um die Informationssicherheit in Behörden zu erhöhen und ein ausreichendes Sicherheitsniveau auf Dauer aufrechtzuerhalten. Da er sich an eine große Bandbreite von Adressaten richtet, bedarf es jedoch ausreichenden IT-Personals, um ihn individuell und spezifisch für eine Behörde umzusetzen.

Fehlt IT-Personal, kann eine Behörde nicht die hohen Anforderungen und die Komplexität des IT-Grundschutzes bewältigen und die erforderlichen Sicherheitsmaßnahmen nicht zeitnah umsetzen. Die ständig fortschreitende Digitalisierung der Verwaltung, neue Hard- und Software sowie veränderte Bedrohungslagen führen dazu, dass die Konzepte schnell veralten. Bevor das IT-Personal die letzten Konzepte erarbeitet hat, sind die ersten bereits wieder zu aktualisieren. Damit wird es durch konzeptionelle Aufgaben zunehmend überlastet und kann die Anforderungen des IT-Grundschutzes nicht erfüllen. Die Behörde ist so nicht ausreichend vor Cyber-Bedrohungen geschützt. Gleichzeitig kann sich das so gebundene IT-Personal nicht um die operative Informationssicherheit kümmern.

Dem BMI ist seit Jahren bekannt, dass Behörden den IT-Grundschutz nicht hinreichend umsetzen und der IT-Fachkräftemangel dazu beiträgt. Mit zunehmender Digitalisierung werden die Folgen dieses Mangels für die Informationssicherheit der Behörden immer kritischer. Kurzfristig beheben lässt er sich zudem nicht. Daher hätte das BMI das vorhandene IT-Personal entlasten müssen. Sein Ziel hätte sein müssen, vergleichbare und wiederkehrende Anforderungen zu standardisieren, damit nicht jede Behörde Überlegungen und Arbeiten nur für sich und jeweils neu anstellen muss.

Zum einen hätte das BSI den auf einen breiten Adressatenkreis ausgerichteten IT-Grundschutz auf die Bedürfnisse der Bundesbehörden anpassen müssen. Die umfangreichen Dokumentationspflichten hätte es für die Bundesbehörden näher spezifizieren und gewichten müssen. Es hätte speziell auf die Bundesverwaltung zugeschnittene Vorlagen erarbeiten können, beispielsweise Checklisten, Umsetzungshinweise und Handreichungen sowie Musterkonzepte für verschiedene Schutzbedarfe. Das vorhandene IT-Personal wäre so in hohem Maße von konzeptioneller Arbeit entlastet und könnte sich darauf konzentrieren, Sicherheitsmängel zu identifizieren und abzustellen.

Zum anderen hätte das BMI weitere Konzepte entwickeln müssen, um das vorhandene IT-Personal auch technisch und organisatorisch zu unterstützen. Hierzu könnte das BMI z. B. „schlüsselfertige“ technische Lösungen für die sichere IT-Ausstattung einer Musterbehörde entwickeln oder beschaffen lassen. Durch eine solche Standardausstattung der Behörden könnte das BSI die o. g. Vorlagen zielgerichtet und passgenau formulieren. Der Aufwand des BSI für die Beratung von Behörden und ihre späteren Kontrollen verringerte sich, da es in weiten Teilen auf Vorlagen der Musterbehörde verweisen könnte. Die Bundesbehörden müssten sie lediglich hinsichtlich ihrer spezifischen Besonderheiten ergänzen oder anpassen.

Das BSI müsste regelmäßig überprüfen, ob die Vorlagen noch aktuell sind und die Standardausstattung noch dem Stand der Technik entspricht. Damit würde das BMI den Grad der Standardisierung in der Bundesverwaltung deutlich erhöhen, das IT-Personal entlasten und letztlich die Informationssicherheit stärken.

Bis dahin müssen Behördenleitungen weiterhin die Aufgaben des vorhandenen IT-Personals so gewichten, dass sie zumindest die gravierenden Sicherheitsmängel zeitnah beheben.

25.3 Stellungnahme

Das BMI hat erklärt, die Behörden würden bereits entlastet, um den IT-Grundschutz einfacher umsetzen zu können. So müssten sie das IT-Grundschutz-Kompendium nicht vollständig durcharbeiten. Auch könnten sie Prioritäten setzen und bei fehlendem IT-Personal beispielsweise operative Maßnahmen der Dokumentation vorziehen. Mit Sicherheitsanalysen decke das BSI Mängel in der Informationssicherheit der Rechenzentren auf. Damit unterstütze es die Bundesbehörden. Zudem erhöhe die IT-Konsolidierung Bund die Informationssicherheit. Dabei würden erhebliche Teile der IT aus den Bundesbehörden in das Informationstechnikzentrum Bund verlagert. Dort stünden den Bundesbehörden auch standardisierte und sichere Lösungen bereit.

Außerdem hat das BMI auf weitere geplante Unterstützung für Behörden verwiesen, damit diese den IT-Grundschutz umsetzen. So habe es ein Projekt gestartet, in dem das BSI beispielsweise Arbeitshilfen und Checklisten erstellt und eine Plattform für den Erfahrungsaustausch schafft. Ferner solle ein Kompetenzzentrum für operative Sicherheitsberatung die Bundesbehörden unterstützen. Zudem wolle das BMI das Informationssicherheitsmanagement des Bundes stärker automatisieren.

Das BMI hat dargelegt, ihm sei bewusst, dass Behörden mit dem Informationssicherheitsmanagement überfordert sind. Ihnen fehlten hierfür vor allem IT-Fachkräfte. Das BMI habe wegen der Ressorthoheit jedoch keine Möglichkeiten, die Personalausstattung der Behörden zu beeinflussen. Dem IT-Rat als höchstem Entscheidungs- und Steuerungsgremium für IT habe es einen Beschlussvorschlag zum Personalmangel in der Informationssicherheit vorlegen wollen. Das BMI bedauere, dass es dazu mangels Einvernehmens mit den Ressorts nicht gekommen sei.

25.4 Abschließende Würdigung

Der Bundesrechnungshof erkennt an, dass das BMI den IT-Grundschutz zu vereinfachen plant. Es bleibt abzuwarten, inwieweit die bisherigen Maßnahmen dazu beitragen, die fortbestehenden Sicherheitsmängel zu beseitigen. Die Nachfragen des Bundesrechnungshofes in den von ihm geprüften Bundesbehörden haben jedenfalls gezeigt, dass sich deren Informationssicherheit nicht wesentlich verbesserte.

Eine Behörde kann ohne vollständige Kenntnis des IT-Grundschutz-Kompendiums kaum die für sie relevanten Anforderungen und Handlungshinweise identifizieren. Lückenhafte Konzepte und ein zu niedriges Schutzniveau sind vielfach die Folge. Behörden ziehen operative Maßnahmen immer wieder Dokumentation und Konzeption vor. Infolgedessen gehen sie oft wenig planvoll vor und haben kein vollständiges Bild über Schwachstellen in ihrer Informationssicherheit. Zudem entlastet das BSI die Bundesverwaltung nicht, wenn es seine Erkenntnisse und Handlungsempfehlungen aus einzelnen Sicherheitsanalysen nicht allen bereitstellt.

Das Informationssicherheitsmanagement der IT-Konsolidierung Bund befindet sich erst im Aufbau. Es kann die Informationssicherheit einer stetig komplexeren IT des Bundes nur gewährleisten, wenn es wirksam wird. Nach aktuellen Erkenntnissen werden mindestens 50 % der IT-Verfahren der Bundesverwaltung überhaupt nicht konsolidiert. Auch wird es noch Jahre dauern, bis die IT-Konsolidierung abgeschlossen ist. Daher müssen Bundesbehörden weiterhin ihre verbleibende dezentrale IT nach den Vorgaben des IT-Grundschutzes absichern. Hierfür muss das BMI standardisierte Konzepte, Technik und Prozesse bereitstellen.

Die Ressorts sind zwar selbst für ihr Personal verantwortlich. Dem BMI war aber der IT-Personalmangel in der Bundesverwaltung schon lange bekannt. Es hätte daher als federführendes Ressort sicherstellen müssen, dass sich der IT-Rat mit dem dringenden ressortübergreifenden Problem befasst und Entscheidungen trifft.

Es ist angesichts der verschärften Bedrohungslage besorgniserregend, dass Bundesbehörden Sicherheitsmängel seit Jahren nicht behoben haben. Informationssicherheit ist eine Kernaufgabe des Bundes. Dafür benötigt er ausreichend Fachkräfte. Das BMI muss für alle Bundesbehörden nutzbare „schlüselfertige“ Lösungen entwickeln und diese in einer Bundesbehörde erproben. Das geplante Kompetenzzentrum sollte so bewährte Lösungen bei anderen Bundesbehörden zum Einsatz bringen.