75 Jahre
Demokratie
lebendig

Deutscher Bundestag
Wissenschaftliche Dienste

Sachstand

Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik

© 2024 Deutscher Bundestag

Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik

Aktenzeichen:	WD 3 - 3000 - 075/24
Abschluss der Arbeit:	07.08.2024
Fachbereich:	WD 3: Verwaltung und Verfassung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1. Einführung

Dieser Sachstand zeigt zunächst übersichtsartig **die gesetzlichen Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)** auf und geht danach gesondert auf die Frage ein, inwieweit die Entwicklung von Authentifizierungs- und Identifikationssystemen i.S.d. **unionsrechtlichen eIDAS-Verordnung** (eIDAS-VO)[1] zu seinem Aufgabenkreis gehört.

Die Aufgaben und Befugnisse des 1991 als nachgeordnete Behörde im **Geschäftsbereich des Bundesministeriums des Innern und für Heimat (BMI)** gegründeten BSI werden im BSI-Gesetz (BSIG)[2] geregelt.[3] Zusammenfassend lässt sich der Auftrag des BSI dahingehend beschreiben, dass es durch die Bereitstellung technischer Vorgaben, das Sammeln und Auswerten von Informationen über Angriffsmuster und die Warnung betroffener Stellen zur **Gewährleistung der Cybersicherheit in Deutschland** beitragen soll.

2. Gesetzliche Aufgaben des BSI

Die Aufgaben des BSI sind im Wesentlichen in **§ 3 BSIG** geregelt. Ergänzende Bestimmungen finden sich in **§§ 4a ff. BSIG**. Da die Vorschriften teils sehr detailliert formuliert sind, werden die verschiedenen Aufgaben zwecks besserer Übersichtlichkeit im Folgenden jeweils zusammenfassend als Teil eines von insgesamt sechs Aufgabenbereichen dargestellt.

2.1. Allgemeine Maßnahmen zur Gewährleistung der Sicherheit in der Informationstechnik

Das BSI fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten.[4] Daher hat es die Aufgabe, **Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren**.[5] Zur **Abwehr von Schadprogrammen** und **Gefahren für die Kommunikationstechnik des Bundes** darf das BSI die erforderlichen Daten auswerten.[6] Außerdem sammelt es **Informationen über**

---

1 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28. August 2014, S. 73-114), zuletzt geändert durch die Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (ABl. L, 2024/1183, 30. April 2024).

2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982).

3 Vgl. hierzu und zur weiteren Historie des BSI: Wissenschaftliche Dienste des Deutschen Bundestages, „Möglichkeit der Einstufung des BSI als Nachrichtendienst“, Ausarbeitung vom 17. Dezember 2021, WD 3 - 3000 - 200/21, S. 4 f.

4 Vgl. § 3 Abs. 1 Satz 1 BSIG.

5 § 3 Abs. 1 Satz 2 Nr. 1 BSIG.

6 § 5 BSIG.

Sicherheitsrisiken und Sicherheitsvorkehrungen und wertet diese aus.[7] Das BSI prüft, **untersucht und bewertet die Sicherheit informationstechnischer Systeme** und Komponenten und darf auch selbst **Sicherheitsvorkehrungen entwickeln.**[8] Es ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten zu kontrollieren.[9] Im Übrigen legt es die **Mindeststandards** für die Sicherheit der Informationstechnik des Bundes fest.[10]

2.2. Unterstützungsleistungen

Darüber hinaus wird das BSI weitestgehend unterstützend tätig.[11] So **unterstützt** es etwa hinsichtlich der Sicherheit in der Informationstechnik den **Bundesbeauftragten für den Datenschutz und die Informationsfreiheit** (BfDI) bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz,[12] ferner **Polizeien, Strafverfolgungsbehörden und Nachrichtendienste** bei der Erfüllung ihrer gesetzlichen Aufgaben.[13] Das BSI unterstützt außerdem die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik zuständigen **Landesbehörden** auf deren Ersuchen hin.[14]

2.3. Kritische Infrastrukturen

Weitere Kompetenzen bestehen auf dem Gebiet der **Kritischen Infrastrukturen.**[15] Das BSI fungiert als **zentrale Stelle** für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen.[16] Dazu **koordiniert** es die **Zusammenarbeit** zum Schutz der Sicherheit in der Informationstechnik Kritischer Infrastrukturen im Verbund mit der **Privatwirtschaft.**[17] Es ist berechtigt, Betreibern Kritischer Infrastrukturen den **Einsatz kritischer Komponenten** zu **untersagen**.[18]

---

7 § 3 Abs. 1 Satz Nr. 2 BSIG.

8 Etwa nach § 3 Abs. 1 Satz Nr. 3, 4, 5 -7, 10 BSIG.

9 § 4a BSIG.

10 § 8 BSIG.

11 Vgl. etwa § 3 Abs. 1 Satz 2 Nr. 9, 12-13a, 18 BSIG.

12 § 3 Abs. 1 Satz 2 Nr. 12 BSIG.

13 § 3 Abs. 1 Satz 2 Nr. 13 BSIG.

14 § 3 Abs. 1 Satz 2 Nr. 13a BSIG, darüber hinaus auch im Rahmen von § 3 Abs. 2 BSIG.

15 Siehe etwa § 3 Abs. 1 Satz 2 Nr. 15, 17, Abs. 3, §§ 8a, 8b, 9b BSIG.

16 § 3 Abs. 1 Satz 2 Nr. 17, § 8b BSIG.

17 § 3 Abs. 1 Satz 2 Nr. 15 BSIG.

18 § 9b BSIG.

2.4. Warnungen

Das BSI ist berechtigt, in Fragen der Sicherheit in der Informationstechnik **Warnungen** gegenüber **staatlichen Stellen, Herstellern, Vertreibern, Anwendern und Verbrauchern** auszusprechen.[19] Dies gilt insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen.[20]

2.5. Maßnahmen zur Wiederherstellung

Liegt eine **Beeinträchtigung der Sicherheit** oder Funktionsfähigkeit eines **informationstechnischen Systems** vor, so kann das BSI auf Ersuchen der betroffenen Stelle in herausgehobenen Fällen bei der **Wiederherstellung der Sicherheit oder Funktionsfähigkeit** unterstützend tätig werden.[21] Ein herausgehobener Fall liegt insbesondere dann vor, wenn es um **einen Angriff von besonderer technischer Qualität** geht oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von **besonderem öffentlichem Interesse** ist.[22]

2.6. Weitere Zuständigkeiten

Darüber hinaus dient das BSI auch als **zentrale Stelle** im Bereich der Sicherheit in der Informationstechnik für die zuständigen **Stellen im Ausland**,[23] als **nationale Zertifizierungsstelle** der Bundesverwaltung für IT-Sicherheit[24] und als nationale Behörde für die **Cybersicherheitszertifizierung**.[25]

3. Entwicklung von Authentifizierungs- und Identifikationssystemen

Als Anknüpfungspunkte für eine Zuständigkeit des BSI für die Entwicklung von Authentifizierungs- und Identifikationssystemen i.S.d. eIDAS-VO kommen, wie im Folgenden näher dargelegt, zwar grundsätzlich verschiedene Vorschriften des BSIG in Betracht, eindeutig lässt sich eine Kompetenz derzeit jedoch nicht bestimmen (siehe unten 3.1 und 3.2). Dies gilt jedenfalls für die

19 Siehe hierzu § 3 Abs. 1 Satz 2 Nr. 14, 14a, § 7 BSIG.

20 § 3 Abs. 1 Satz 2 Nr. 14, 14a BSIG.

21 § 3 Abs. 1 Satz 2 Nr. 18, § 5b BSIG.

22 § 5b Abs. 2 BSIG.

23 § 3 Abs. 1 Satz 2 Nr. 16 BSIG.

24 § 9 BSIG.

25 § 3 Abs. 1 Satz 2 Nr. 5a, § 9a BSIG.

Entwicklung von elektronischen **Authentifizierungs- und Identifikationsverfahren zur Anwendung in der Breite**, also insbesondere zwischen privaten Rechtsträgern.[26]

3.1. § 3 Abs. 1 Satz 2 Nr. 19 BSIG: Empfehlungen und Bewertungen von Verfahren

Das BSI hat gemäß § 3 Abs. 1 Satz 2 Nr. 19 BSIG die Aufgabe, **Empfehlungen für Identifizierungs- und Authentifizierungsverfahren** zu geben und diese **Verfahren** im Hinblick auf die Informationssicherheit zu **bewerten**. Diese Kompetenznorm wurde durch Art. 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme[27] in das BSIG eingefügt. Wie der Begründung des Gesetzentwurfs zu entnehmen ist, wurde diese Norm jedenfalls auch zwecks Ausführung der eIDAS-VO geschaffen. Dort heißt es:

> Mit der neu eingefügten Nummer 19 in § 3 Absatz 1 Satz 2 BSIG wird die Zuständigkeit des BSI für die Entwicklung von Vorgaben sowie die abschließende Bewertung von Identifizierungs- und Authentisierungsverfahren unter dem Gesichtspunkt der Informationssicherheit gesetzlich klargestellt. Diese sicherheitstechnisch relevanten Verfahren bedürfen gerade mit Blick auf die Vorgaben der eIDAS-VO auf EU-Ebene einer Konkretisierung sowie abschließenden Bewertung im nationalen Kontext, um eine sichere, nutzerfreundliche und insbesondere einheitliche Ausgestaltung zu gewährleisten. Das BSI ist Kraft seines gesetzlichen Auftrags innerhalb der Bundesverwaltung für diesen Bereich zuständig, da der Gesetzgeber mit der Bündelung der Fachkompetenz des Bundes im Bereich der Informationssicherheit beim BSI (§ 1 Satz 2 BSIG) gerade das Ziel verfolgt hat, eine einheitliche Bewertung für sicherheitstechnisch relevante Verfahren und Maßnahmen zu erzielen. Darüber hinaus verfügt das BSI über eine besondere technische Kompetenz, die für eine abschließende Bewertung solcher Verfahren erforderlich ist. Die neu eingefügte Klarstellung in Nummer 19 stellt daher sicher, dass das gesetzgeberische Ziel erreicht wird.[28]

Der **Hinweis auf die eIDAS-VO** macht deutlich, dass das BSI nach dem Willen des Gesetzgebers auch und gerade im Hinblick auf Identifizierungs- und Authentifizierungsverfahren i.S.d. eIDAS-VO **Empfehlungen und Bewertungen** aussprechen soll. Zur Frage, ob damit auch gemeint ist, dass das BSI **eigene Softwarelösungen für solche Verfahren entwickeln** darf, haben sich bislang weder Rechtsprechung noch juristisches Schrifttum geäußert. Allerdings legen die Begriffe „Empfehlung“ und „Bewertung“ nach **allgemeinem Verständnis** nahe, dass das BSI die Aufgabe hat, in Bezug auf Authentifizierungs- und Identifikationsverfahren **Informationen** in Gestalt von **Untersuchungsergebnissen, Ratschlägen und Hinweisen** bereitzustellen. Ferner ist in der Begründung des Gesetzentwurfs die Rede davon, dass der Gesetzgeber mit der Bündelung der Fachkompetenz des Bundes im Bereich der Informationssicherheit beim BSI gerade das Ziel verfolgt habe, eine

---

26 Anm.: Soweit es dagegen um die Entwicklung von Authentifizierungs- und Identifikationsverfahren geht, die spezifisch dem Schutz der Informationstechnik des Bundes dienen, lässt sich eine Zuständigkeit des BSI über die Auffangaufgabe des § 3 Abs. 1 Satz 2 Nr. 1 BSIG (Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes) und § 3 Abs. 1 Satz 2 Nr. 11 BSIG (Bereitstellung von IT-Sicherheitsprodukten für Stellen des Bundes) begründen.

27 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021, BGBl. 2021 Teil I Nr. 25, ausgegeben zu Bonn am 27. Mai 2021.

28 Gesetzentwurf der Bundesregierung, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, vom 25. Januar 2021, BT-Drs. 19/26106, S. 61.

einheitliche Bewertung für sicherheitstechnisch relevante Verfahren und Maßnahmen zu erzielen, und dass die neu eingefügte Klarstellung in Nummer 19 sicherstelle, dass dieses gesetzgeberische Ziel erreicht werde. Auch diese Ausführung spricht dafür, dass die Kompetenz aus § 3 Abs. 1 Satz 2 Nr. 19 BSIG in erster Linie die Bereitstellung von Informationen zu Authentifizierungs- und Identifikationsverfahren durch das BSI, nicht hingegen die Entwicklung eigener Softwarelösungen umfasst.

3.2. § 3 Abs. 1 Satz 2 Nr. 3 BSIG: Entwicklung von Sicherheitsvorkehrungen

Allerdings gehört, wie bereits oben unter 2.1. erwähnt, gemäß **§ 3 Abs. 1 Satz 2 Nr. 3 BSIG** auch die „**Entwicklung von Sicherheitsvorkehrungen**“ zu den Aufgaben des BSI. Beispielhaft ist in der Vorschrift insoweit die Rede von „**informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte)**“. Identifizierungs- und Authentifizierungsverfahren gewährleisten, dass nur die jeweils befugten Personen Zugriff auf geschützte Informationen, Konten und Systeme erhalten, und erhöhen auf diese Weise die Sicherheit in der Informationstechnik. Diese Verfahren können daher als IT-Sicherheitsprodukte, mithin als Sicherheitsvorkehrungen i.S.d. § 3 Abs. 1 Satz 2 Nr. 3 BSIG angesehen werden.

Die Kompetenz zur Entwicklung von Sicherheitsvorkehrungen gilt jedoch nicht uneingeschränkt, sondern gemäß § 3 Abs. 1 Satz 2 Nr. 3 BSIG nur, „**soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist**“.

3.2.1. Aufgabe des Bundes

Gemäß **Art. 30 GG** ist die Ausübung der staatlichen Befugnisse und die **Erfüllung der staatlichen Aufgaben** grundsätzlich **Sache der Länder**, soweit das GG keine andere Regelung trifft oder zulässt. Diese Regelung gilt für jegliches Handeln staatlicher Organe, einschließlich der sog. gesetzesfreien Verwaltung, dem staatlichen Handeln in Privatrechtsform, der fiskalischen oder erwerbswirtschaftlichen Teilnahme am Marktgeschehen oder der Vergabe von Fördermitteln.[29]

Eine **Aufgabe des Bundes** liegt daher nur vor, soweit der **Bund** sich für eine **staatliche Aufgabe** auf eine ausdrückliche oder stillschweigende **Kompetenzzuweisung im Grundgesetz** berufen kann.[30]

3.2.1.1. Vollzug der eIDAS-VO

Der Vollzug der eIDAS-VO scheidet als Anknüpfungspunkt für eine Aufgabe des Bundes vorliegend bereits deshalb aus, weil die VO, wie **Erwägungsgrund 13** verdeutlicht, es der **freien Entscheidung der Mitgliedstaaten** überlässt, eigene Identifikations- und Authentifizierungsverfahren zu entwickeln:

> Den Mitgliedstaaten sollte es freigestellt bleiben, zwecks elektronischer Identifizierung eigene Mittel für den Zugang zu Online-Diensten einzuführen oder zu verwenden. Sie sollten auch

29 Wittreck, in: Dreier, GG, 3. Auflage 2015, Art. 3 Rn. 17 f.

30 Hellermann, in: Epping/Hillgruber, GG, 58. Edition Stand 15.Juni 2024, Art. 30 Rn. 14 f.

selbst entscheiden können, ob sie den Privatsektor in die Bereitstellung solcher Mittel einbeziehen. Die Mitgliedstaaten sollten nicht verpflichtet sein, ihre elektronischen Identifizierungssysteme der Kommission zu notifizieren. Die Entscheidung, alle, einige oder keines der elektronischen Identifizierungssysteme der Kommission zu notifizieren, die auf nationaler Ebene zumindest für den Zugang zu öffentlichen Online-Diensten oder bestimmten Diensten verwendet werden, ist Sache der Mitgliedstaaten.[31]

Die **Entwicklung von Softwarelösungen** für Identifikations- und Authentifizierungsverfahren gehört daher **gerade nicht** zu den **Aufgaben nach der eIDAS-VO**. Unter diesem Gesichtspunkt kann die Kompetenz des BSI zur Entwicklung eigener Softwarelösungen also nicht begründet werden.

3.2.1.2. Grundrechtliche Schutzpflicht

Die Entwicklung von Sicherheitsvorkehrungen könnte jedoch dann zu den Aufgaben des Bundes gehören, wenn es für den Bund aufgrund einer grundrechtlichen Schutzpflicht geboten wäre, solche Vorkehrungen zu entwickeln. Das Bundesverfassungsgericht leitet eine **Schutzpflicht des Staates**, **elektronische Kommunikation und informationstechnische Systeme vor Angriffen Dritter zu schützen**, aus der objektiven Wertordnung der Grundrechte her.[32] Die immer breitere Nutzung informationstechnischer Systeme führe dazu, dass Einzelne von ihren grundrechtlichen Freiheiten ohne die Nutzung solcher Systeme immer weniger Gebrauch machen könnten und immer weniger die Möglichkeit hätten, sich den Gefahren der Nutzung dadurch zu entziehen, dass sie auf diese Nutzung verzichteten.[33] Vor diesem Hintergrund treffe den Staat auch die **Pflicht**, **aktiv** dazu **beizutragen**, dass die **Integrität und Vertraulichkeit informationstechnischer Systeme** gegen Angriffe durch Dritte **geschützt** werden.[34]

Die Wahrnehmung dieser staatlichen Schutzpflicht weist das Grundgesetz dem Bund **nicht ausdrücklich** als Aufgabe zu. Der Bund könnte jedoch aufgrund einer **ungeschriebenen Verwaltungskompetenz kraft Natur der Sache** dafür zuständig sein, Integrität und Vertraulichkeit informationstechnischer Systeme zu schützen. Eine Kompetenz kraft Natur der Sache setzt voraus, dass eine Aufgabe **aufgrund ihrer Eigenart nur durch den Bund** wahrgenommen werden kann.[35] Dazu reicht es allerdings nicht aus, dass die Aufgabenwahrnehmung durch den Bund zweckmäßig erscheint, um gleichwertige Lebensverhältnisse im Bund herzustellen, oder dass die Aufgabe faktisch überregionaler Natur ist; Voraussetzung ist vielmehr, dass die Aufgabe **durch die Länder überhaupt nicht effektiv wahrgenommen** werden kann.[36]

Inwieweit Stellen der Länder tatsächlich in der Lage wären, im Rahmen der Wahrnehmung der staatlichen Schutzpflicht Authentifizierungs- und Identifikationssysteme zu entwickeln, kann

---

31 Erwägungsgrund 13, eIDAS-VO.

32 BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18, Rn. 33.

33 BVerfG, a.a.O.

34 BVerfG, a.a.O.

35 F. Kirchhof, in: Dürig/Herzog/Scholz, GG, 103. EL Januar 2024, Art. 83 Rn. 63.

36 F. Kirchhof, a.a.O.

vorliegend nicht abschließend beurteilt werden. Zwar liegt die Annahme nahe, dass ein bundesweit einheitliches Verfahren zur Authentifizierung und Identifikation von Personen Vorteile im Hinblick auf Kompatibilität und Praktikabilität bieten könnte. Würden solche Verfahren auf Landesebene entwickelt, bestünde jedoch zumindest grundsätzlich die Möglichkeit, die bundesweite Einheitlichkeit über **Koordinationsgremien** wie die Innenministerkonferenz herzustellen. Inwieweit die Entwicklung von Authentifizierungs- und Identifikationsverfahren eine **Aufgabe des Bundes** darstellt, muss daher im Rahmen dieser Bearbeitung als **offen** betrachtet werden.

3.2.2. Erforderlichkeit

Mangels eindeutig zu identifizierender Aufgabe des Bundes kann auch **dahinstehen**, ob die Entwicklung von Sicherheitsvorkehrungen zur Erfüllung solcher Aufgaben erforderlich i.S.d. § 3 Abs. 1 Satz 2 Nr. 3 BSIG ist.

3.3. Fazit

Eine allgemeine Zuständigkeit des BSI für die Entwicklung von Authentifizierungs- und Identifikationssystemen i.S.d. eIDAS-VO könnte sich grundsätzlich aus § 3 Abs. 1 Satz 2 Nr. 3 BSIG ergeben. Voraussetzung dafür ist jedoch, dass die staatliche Schutzpflicht für die Vertraulichkeit und Integrität informationstechnischer Systeme nicht durch die Entwicklung von Authentifizierungs- und Identifikationssystemen auf Länderebene erfüllt werden kann. Inwieweit dies der Fall ist oder nicht, entzieht sich im Rahmen dieser Bearbeitung einer Beurteilung.

Soweit es um die Entwicklung von Authentifizierungs- und Identifikationsverfahren zum Schutz der eigenen Informationstechnik des Bundes geht, ergibt sich die Zuständigkeit des BSI aus § 3 Abs. 1 Satz 2 Nr. 1, 11 BSIG.

***