Programm der Bundesregierung zur Steigerung der Cybersicherheit in der Bundesverwaltung (CyberGovSecure)

Präambel

Die Cybersicherheit der Bundesverwaltung hat großen Nachholbedarf. Bestehende IT-Verfahren erfüllen teilweise weder die Anforderungen der Nutzenden noch sind sie angesichts der aktuellen Bedrohungslage ausreichend robust aufgestellt. Erforderlich ist eine klare und übergreifende Cybersicherheits-Governance, die strategische Vorgaben macht und alle Ressorts dabei unterstützt, die notwendigen Priorisierungen zugunsten von Cybersicherheit und -resilienz vorzunehmen, um entsprechende Maßnahmen umsetzen zu können.

Auch der Haushaltsausschuss des Deutschen Bundestages weist in seinem Maßgabebeschluss vom 13.11.2025 zum NIS2-Umsetzungsgesetz auf die Notwendigkeit einer kohärenten Sicherheitsarchitektur in der Bundesverwaltung hin und erwartet, dass die dafür erforderlichen Personal- und Sachmittel im Bundeshaushalt ausgebracht werden. Im Lichte dieser Erwartungshaltung werden die Verhandlungen der Haushaltsaufstellungsverfahren geführt.

Die Bundesregierung beschließt deshalb ein Programm zur Steigerung des Niveaus der Cybersicherheit und -resilienz in der Bundesverwaltung (Titel „CyberGovSecure“) mit den folgenden Kernpunkten:

- Aufbau eines Lenkungskreises auf ministerialer Leitungsebene unter Vorsitz des BMDS, der den übergeordneten strategischen Rahmen für das Programm festlegt. Die Koordination der operativen Umsetzung und die Entwicklung des Programms erfolgt durch die Koordinatorin oder den Koordinator der Bundesregierung für Informationssicherheit (CISO Bund) gemeinsam mit den Ressort-Informationssicherheits-

beauftragten. Die fachlichen Vorgaben innerhalb dieses Rahmens werden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Benehmen, unter Berücksichtigung der Bedarfe, mit den Ressorts entwickelt und koordiniert.

- Auf der operativen Ebene wird die Umsetzung dieses Programms CISO Bund konsequent nachverfolgt. Das Programm soll u.a. folgende zentrale Punkte umfassen:
    - Steigerung der Cybersicherheit und -resilienz der Bundesverwaltung durch Umsetzung der Vorgaben des BSI-Gesetzes, Aufbau eines transparenten und aufwandsarmen Berichtswesens, das den aktuellen Stand der Maßnahmen sowie frühzeitig Handlungsbedarfe darstellt. Das Berichtswesen dient der Dokumentation von Fortschritten und bildet eine verlässliche Grundlage für fundierte Entscheidungen.
    - Aufbau von Cybersicherheitsfähigkeiten bei allen Einrichtungen des Bundes gemäß § 29 BSIG (einschließlich der IT-Dienstleister) und den in § 2 Nr. 21 BSIG genannten Gerichten und Verfassungsorganen durch zentrale Unterstützung von Seiten des BSI
    - Etablierung von übergreifenden Prozessen und Tools zur fortlaufenden Sicherstellung der Cybersicherheit und -resilienz
    - Klare Vorgaben für Regelkommunikation, Austauschprozesse und gemeinsame Übungen in der Bundesverwaltung zur Cybersicherheit

CISO Bund wird Beauftragungsmöglichkeiten und Angebote identifizieren bzw. zur Verfügung stellen, die die Ressorts für eine fachliche Begleitung und den Kompetenztransfer in die jeweilige Einrichtung bei der Umsetzung der Cybersicherheitsvorgaben nutzen können.

Die Verantwortung für die Umsetzung verbleibt bei der jeweiligen Einrichtungsleitung. Die Verantwortung für die Durchführung des Programms obliegt CISO Bund.

Ausgestaltung und Umsetzung des Programms, insbesondere zu Berichtswesen und Gremienstrukturen, erfolgen bürokratiearm. Für die betroffenen Einrichtungen der Bundesverwaltung werden keine Pflichten eingeführt, die über europarechtliche Anforderungen hinausgehen.

Die Bundesregierung stimmt darin überein, dass mit dem Programm „CyberGovSecure“ ein dringend notwendiger Beitrag für den Schutz und die digitale Wehrhaftigkeit Deutschlands erbracht wird. Aus den folgenden und weiteren Themenkomplexen werden im Benehmen mit den Ressorts unter Berücksichtigung der Bedarfe ressortübergreifende Einzelmaßnahmen im Rahmen verfügbarer Ressourcen und Haushaltsmittel umgesetzt; die abschließende Festlegung der Maßnahmen obliegt dem Lenkungskreis:

- *Sichere Konfiguration und Systemhärtung:*
  Einheitliche Sicherheitsrichtlinien für Clients, Server und Active Directory: Verhinderung von „Lateral Movement“ eines Angreifers
- *Assetmanagement:*
  Identifizierung von Risiken durch undokumentierte und veraltete Assets in der Bundesverwaltung
- *Schwachstellenmanagement:*
  Aufbau eines Schwachstellenmanagements gemäß BSIG in den Einrichtungen der Bundesverwaltung, inkl. Durchführung behördeninterner Schwachstellenscans
- *Protokollierung und Detektion:*
  Ausbau der zentralen Protokollierungs- und Detektionsinfrastrukturen des Bundes, inkl. Ausgestaltung der Anbindung von Bundeseinrichtungen
- *Netzwerksicherheit:*
  Sicherheits-Gateway, auch in virtualisierten Umgebungen, Segmentierung, Zero-Trust-Architektur, Anomalieerkennung und Protokollierung, Post-Quanten-Kryptographie
- *Informationssicherheitscontrolling:*
  Aufbau und Pflege eines zentralen Informationssicherheitscontrollings als Bestandteil des Informationssicherheitsmanagementsystems zur Dokumentation des Cybersicherheitsstatus der Bundesverwaltung
- *Resilienter Aufbau der zentralen Dienstleistungen:*
  Ausbau des Sabotageschutzes in den strategisch relevanten Rechenzentren der Bundesverwaltung
- *Daten- und Zugriffsschutz:*
  Verschlüsselung, zentrales Identity und Access Management, zentrale Bereitstellung einer Lösung für Multifaktorauthentisierung
- *Sicheres und modernes Mobile Device Management:*
  Um ressortübergreifende, fortschrittliche und ultramobile digitale Arbeitsplätze sicher zur Verfügung stellen zu können, wird sich das BMDS mit dem BSI und den zentralen IT-Dienstleistern für einheitliche, sichere und moderne Endgeräte sowie standardisierte Mobile Device Management (MDM) Strukturen einsetzen.

Das Programm „CyberGovSecure“ behandelt für den Bereich der gesamten Bundesverwaltung die Themen u. a. Detektion/Sensorik, Analyse und Schutzfunktionen. Diese Funktionalitäten werden auch in dem parallel in der Konzeption befindlichen Programm „Cyberdome“ adressiert, das den Aufbau einer gesamtstaatlichen Schutz-Infrastruktur zur Früherkennung, Analyse und Abwehr von Cyberangriffen zum Ziel hat. Mit dem Cyberdome soll Deutschland vor Cyberangriffen auf Staat, Wirtschaft und Verwaltung geschützt werden. CyberGovSecure und Cyberdome haben beide einen wesentlichen Anteil an der Stärkung der Cybersicherheit.

§ 1 Ziel und Zweck des Programms

1. Die Cybersicherheit der von der Bundesregierung eingesetzten informationstechnischen Systeme und der damit verarbeiteten Daten soll durch das Programm „CyberGovSecure“ maßgeblich und messbar gesteigert und fortführend sichergestellt werden. Das Programm hat die Aufgabe, die Cybersicherheit und -resilienz in der Bundesverwaltung zu steigern, indem dezentrale und zentrale Cybersicherheits-Fähigkeiten sowie Prozesse für die fortlaufende Sicherstellung der Cybersicherheit aufgebaut werden. Das Programm soll die Ressorts dabei unterstützen, die gesetzlichen Verpflichtungen zur Cybersicherheit zu erfüllen.
2. Dem Bundeskabinett wird durch den Koordinator oder die Koordinatorin für Informationssicherheit gemäß § 48 BSIG (nachfolgend „Chief Information Security Officer Bund“ - kurz „CISO Bund“ - genannt) zu Beginn eines Jahres ein Bericht über den Umsetzungsstand des Vorjahres samt Vorschlägen für konkrete Verbesserungen bzw. strategischer Handlungsbedarfe vorgelegt.

§ 2 Inhalte und Durchführung des Programms

1. Das Programm richtet sich an Einrichtungen des Bundes gemäß § 29 BSIG und steht den in § 2 Nr. 21 BSIG genannten Gerichten und Verfassungsorganen bei Bedarf für eine freiwillige Teilnahme offen.
2. Für die fachliche Ausrichtung des Programms werden die geltenden gesetzlichen Vorgaben zur Informationssicherheit gemäß § 44 BSIG herangezogen. Daraus und aus den Erkenntnissen der BSI-Erhebungen und Prüfungen (u.a. auf Basis von § 7 BSIG) leitet CISO Bund im Bundesamt für Sicherheit in der Informationstechnik (BSI) Handlungsbedarfe ab. Diese unterlegt CISO Bund, im Benehmen mit den Ressorts und unter Berücksichtigung der Bedarfe, mit konkreten Maßnahmen, welche im Rahmen der eigenen Verantwortung zur Gewährleistung der Cybersicherheit von den Einrichtungsleitungen angemessen berücksichtigt werden. Die operative Umsetzung der vereinbarten Maßnahmen innerhalb der Ressorts wird kooperativ zwischen der jeweiligen obersten Bundesbehörde und dem BSI abgestimmt.

3. Auf Basis der gemäß § 44 BSIG einzuhaltenden Vorgaben für die Bundesverwaltung legt CISO Bund im Benehmen mit den Ressorts unter Berücksichtigung der Bedarfe Zielwerte für die in Abs. 2 beschriebenen Maßnahmen fest um die Ressorts dabei zu unterstützen, die gesetzlichen Verpflichtungen zur Informationssicherheit zu erfüllen.
4. Für die Durchführung des Programms sind zusätzliche Mittel und Stellen zum Haushalt 2027 und zur mittelfristigen Finanzplanung angemeldet worden. Entsprechend seines gesetzlichen Auftrages unterstützt das BSI die Einrichtungen bei der Durchführung des Programms im Rahmen seiner haushalterischen Möglichkeiten. Die Notwendigkeit der Nutzung bestehender Rahmenverträge und – vorbehaltlich ihrer Verfügbarkeit – die Nutzung eigener oder Beantragung weiterer Haushaltsmittel der Ressorts bleibt dadurch unberührt. Das BSI unterstützt die Ressorts bei der operativen Umsetzung von Sicherheitsmaßnahmen vor Ort im Rahmen seiner Möglichkeiten und kann dazu auch Dritte beauftragen.
5. Bestehende gesetzliche Sonderregelungen und Ausnahmen des NIS2-Umsetzungsgesetzes (insb. gem. §§ 7, 29 und 44 BSIG) bleiben unberührt.

§ 3 Lenkungskreis

1. Die strategische Steuerung erfolgt durch einen Lenkungskreis unter Vorsitz des Bundesministeriums für Digitales und Staatsmodernisierung. Der Lenkungskreis nimmt die Funktion des Auftraggebers für die Koordination der operativen Umsetzung und die Entwicklung des Programms wahr und ist zugleich für die Abnahme der Ergebnisse verantwortlich. Er beauftragt die Umsetzung der Maßnahmen gemäß § 2 Abs. 2 und beschließt damit das Ziel für alle von § 44 Abs. 1 BSIG erfassten Einrichtungen, die Zielwerte gemäß § 2 Abs. 2 innerhalb eines vorgegebenen Zeitraums zu erreichen.
2. Die obersten Bundesbehörden entsenden die für Fragen der Informationssicherheit zuständigen Staatssekretärinnen oder Staatssekretäre oder eine stimmberechtigte Vertretung. Zudem ist CISO Bund ein nicht stimmberechtigter Teilnehmer des Lenkungskreises. Der Lenkungskreis gibt sich einstimmig eine Geschäftsordnung.

§ 4 Koordinierung der operativen Umsetzung und die Entwicklung des Programms

1. Die Koordinierung der operativen Umsetzung und die Entwicklung des Programms erfolgt gemäß § 48 BSIG durch CISO Bund unter Berücksichtigung der Bedarfe und im Benehmen mit den obersten Bundesbehörden, vertreten durch die Informationssicherheitsbeauftragten der Ressorts (Programmausschuss).
2. Der Programmausschuss führt hierzu regelmäßig Sitzungen durch und gibt sich eine Geschäftsordnung. Der allgemeine Bericht nach § 1 Abs. 2 wird vor seiner Vorstellung im Kabinett im Programmausschuss im Benehmen mit den obersten Bundesbehörden behandelt.