CyberGovSecure und Schwachstellenmanagement: Was steckt hinter dem neuen Cyber Security-Programm des Bundes?

Im Mai 2026 hat das Bundeskabinett CyberGovSecure ins Leben gerufen. Es ist die größte koordinierte Cyber Security-Initiative, die die Bundesverwaltung je unternommen hat. Der Zweck ist klar: die Sicherheitslage in jedem Bundesministerium und jeder Bundesbehörde erhöhen und NIS2 von einer Compliance-Verpflichtung auch hier in die operative Realität überführen. Schwachstellenmanagement zählt bereits 2026 zu den ersten vier Prioritätsbereichen.

Für Verantwortliche der Informationssicherheit in Organisationen der Bundesverwaltung ist dies ein Moment, in dem Politik, Budget und operative Realität zusammenfinden. In diesem Beitrag gehen wir darauf ein, wo CyberGovSecure in der breiteren Cyber Security-Landschaft Deutschlands verortet ist, was das Ziel für Behörden in diesem Jahr ist und wie zeitgemäßes Schwachstellenmanagement aussieht, wenn es mit einer KI-beschleunigten Bedrohungslandschaft Schritt halten muss.

Die Ursache: NIS2 in Deutschland

Um CyberGovSecure zu verstehen, muss man das rechtliche Fundament darunter verstehen. NIS2 ist die EU-Richtlinie, die die Anforderungen an die Cyber Security in wesentlichen, kritischen und wichtigen Sektoren angehoben hat. Alle Mitgliedstaaten hatten bis zum 17. Oktober 2024 Zeit, sie in nationales Recht zu überführen.

Deutschland hat diese Frist um mehr als ein Jahr verpasst. Die Europäische Kommission leitete daraufhin ein Vertragsverletzungsverfahren ein. Nach umfangreicher parlamentarischer Arbeit hat der Bundestag das *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (NIS2UmsuCG) am 13. November 2025 verabschiedet. Der Bundesrat stimmte ihm am 20. November zu, und am 6. Dezember 2025 trat es ohne Übergangsfrist in Kraft. Rund 29.500 Organisationen in Deutschland fallen nun darunter, und Bußgelder können bis zu 10 Millionen Euro erreichen.

Das Gesetz hat keine eigenständige NIS2-Regelung geschaffen. Stattdessen wurde das BSI-Gesetz umfassend novelliert und der Zuständigkeitsbereich des BSI erweitert. Nach dem neuen Rahmen hat die Präsidentin des BSI die Rolle der *Koordinatorin der Bundesregierung für Informationssicherheit* (CISO Bund) inne. Damit erhält die Behörde zentrale Zuständigkeit für die Informationssicherheit des Bundes.

CyberGovSecure ist die operative Antwort auf eine bestimmte Frage: Wie erfüllt die Bundesverwaltung, die föderale Administration selbst, die Anforderungen, die sie nun für alle anderen überwacht?

Was ist CyberGovSecure?

CyberGovSecure ist das zentrale Programm der Bundesregierung zur Umsetzung der NIS2-Anforderungen in der Bundesverwaltung. Es wurde durch Kabinettsbeschluss verabschiedet und ist mit Kick-off-Veranstaltungen in Berlin und Bonn am 4. Mai 2026 offiziell gestartet. Alle Bundesministerien und Bundesbehörden sind einbezogen. Das Programm bringt Standards, Maßnahmen und Finanzierung erstmals in einem einheitlichen Rahmen zusammen.

Zwei Rollen leiten das Programm. Die strategische Steuerung liegt bei einem Lenkungskreis unter der Leitung des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS). Die operative Koordination liegt bei Claudia Plattner, Präsidentin des BSI, in ihrer Funktion als Leiterin des CISO Bund.

Laut BSI hat das Programm bisher neun Handlungsfelder definiert:

- Sichere Konfiguration und Systemhärtung
- Assetmanagement
- **Schwachstellenmanagement**
- Protokollierung und Detektion
- Netzwerksicherheit
- Informationssicherheitscontrolling
- Resilienter Aufbau der zentralen Dienstleistungen
- Daten- und Zugriffsschutz
- Sicheres und modernes Mobile Device Management

Für 2026 wurden vier dieser Felder zu unmittelbaren Prioritäten erklärt: Sicheres Back-Up, Sichere Konfiguration und Systemhärtung, Schwachstellenmanagement sowie Protokollierung und Detektion. Diese Prioritätenliste ist bedeutsam. Sie bedeutet, dass jede Bundesbehörde in den nächsten 12 bis 18 Monaten belastbare Fortschritte im Schwachstellenmanagement nachweisen muss, verfolgt über ein zentrales Berichtssystem, das das BSI aufbaut.

Warum Schwachstellenmanagement 2026 noch auf der To-Do-Liste steht

Das BSI hat Schwachstellenmanagement nicht in die erste Welle aufgenommen, weil es sich gut in einer Überschrift macht. Es steht dort, weil es das Fundament für nahezu jede andere CyberGovSecure-Priorität ist.

Sie können nicht härten, was Sie nicht inventarisiert haben. Sie können keine Angriffe auf Systeme erkennen, deren Verwundbarkeit Ihnen nicht bekannt ist. Sie können nicht sichern, was Sie nicht erfasst haben. Wenn Schwachstellenmanagement gut funktioniert, werden sichere Konfiguration, Angriffserkennung und Back-Up möglich. Wenn es schlecht funktioniert, übernimmt jede nachgelagerte Position im Cybersecurity-Prozess die blinden Flecken.

NIS2 macht dies ausdrücklich. Artikel 21(2)(e) der Richtlinie verpflichtet Organisationen dazu, Schwachstellenmanagement und Offenlegung als Teil der Sicherheit von Netz- und Informationssystemen zu adressieren, und Artikel 21(2)(g) behandelt grundlegende Cyber-Hygiene-Praktiken. Zusammen sind diese Bestimmungen das, was CyberGovSecure in ein operatives Programm für die öffentliche Verwaltung übersetzt.

Wie zeitgemäßes Schwachstellenmanagement in der Praxis aussieht

Die Wortwahl des BSI ist bewusst. Das Programm fordert ausdrücklich „zeitgemäßes Schwachstellenmanagement", nicht jährliche Audits oder vierteljährliche Scans. In der Praxis bedeutet zeitgemäßes Schwachstellenmanagement, unser Erfahrung nach, für die öffentliche Verwaltung fünf Dinge.

- **Kontinuierlich, nicht periodisch.** Schwachstellen entstehen täglich, und Systeme ändern sich in vergleichbarem Tempo. Ein Programm, das auf vierteljährlichen Scanläufe aufbaut, hinterlässt 90-tägige Zeitfenster für Exposition und Ausnutzung. Zeitgemäße bedeutet kontinuierliche Scans der gesamten Angriffsfläche. So wird eine neue Schwachstelle rechtzeitig erkannt, nicht erst Monate später.
- **Nach realem Risiko priorisiert, nicht nur nach Schweregrad.** Nicht jede Schwachstelle ist gleich gefährlich. Zeitgemäße Tools berücksichtigen Ausnutzbarkeit, Internet-Exposition und operative sowie wirtschaftliche Konsequenzen. Das ist besonders wichtig, wenn ein Security-Team klein und die Angriffsfläche groß ist, was in Bundesbehörden häufig der Fall ist.
- **Vollständige Asset-Sichtbarkeit zuerst.** Schwachstellenmanagement hängt davon ab zu wissen, welche Assets überhaupt in der IT-Infrastruktur existieren. Deshalb ist Assetmanagement und -discovery als eigenes Handlungsfeld neben Schwachstellenmanagement aufgeführt. Ohne präzises Inventar erbt Schwachstellenmanagement jede Lücke in der CMDB.
- **Handlungsfähig, nicht nur informativ.** Berichte, die Zehntausende Schwachstellen ohne Priorisierung auflisten, sind nicht nützlich. Zeitgemäße Praxis liefert eine klare Prioritätenliste, die ein Security-Team tatsächlich abarbeiten kann, mit konkreten Empfehlungen zur Behebung.
- **Auditfähig als Standard.** Die zentrale Berichterstattung im Rahmen von CyberGovSecure bedeutet, dass Nachweise über Fortschritte wichtig sind. Zeitgemäße Praxis erzeugt die Dokumentation, die Auditoren und Prüfer benötigen, als eingebaute Funktion und nicht als manuelle Übung im Nachhinein.

Die KI-Beschleunigung: Warum Timing jetzt entscheidend ist

Es gibt einen Grund, warum CyberGovSecure Schwachstellenmanagement priorisiert hat. Die Bedrohungslandschaft verändert sich schneller, als es Cybersecurity-Verantwortliche bisher gewohnt sind.

Frontier-KI-Modelle lesen Code, finden Schwachstellen und erzeugen funktionierende Exploits in Geschwindigkeiten, die früher erfahrene menschliche Sicherheitsforscher erforderten. Der Aufwand für Angriffe ist stark gesunken, während der für das Patchen ungefähr gleich geblieben ist. Das Zeitfenster zwischen Offenlegung und Exploit hat sich drastisch verkleinert, und die Sicherheitsmarge, auf die sich die meisten Teams unbewusst verlassen haben, ist stillschweigend verschwunden.

Es gibt eine spezifische Falle in dieser Entwicklung, die Teams unvorbereitet trifft. KI ist sehr gut darin, Schwachstellen mit geringerem Risiko zu verketten. Einzeln betrachtet wirkten diese Funde insignifikant und wurden als „geringes Risiko" depriorisiert. Aber „geringes Risiko" bedeutete oft „schwer auszunutzen", nicht „harmlos", und KI beseitigt genau diese Schwierigkeit. Aneinandergereiht wird aus einer Handvoll niedriger Schwachstellen ein realistischer Angriffspfad.

Für eine Bundesbehörde, die sich auf jährliche oder vierteljährliche Assessments verlässt, gilt die Annahme „das behandeln wir im nächsten Zyklus" nicht mehr. Wir haben diese Verschiebung ausführlicher in unserem früheren Beitrag zum KI-Schwachstellenmanagement behandelt. Kurz gesagt: Die Geschwindigkeit der Behebung, nicht nur der Erkennung, entscheidet heute darüber, ob eine Organisation aus den Schlagzeilen bleibt.

Der Fokus von CyberGovSecure auf „zeitgemäß" spiegelt diese Realität wider. Es ist kein stilistisches Wort. Es ist die Anerkennung, dass Schwachstellenmanagement-Prozesse von vor fünf Jahren für die heutige Bedrohungsumgebung, in der die öffentliche Verwaltung arbeitet, nicht mehr ausreichen.

Digitale Souveränität in der öffentlichen Beschaffung

Neben den operativen Veränderungen gibt es eine strategische. Wenn Behörden externe Partner für CyberGovSecure-Arbeit bewerten, ist digitale Souveränität heute ein ausdrückliches Kriterium und keine Präferenz mehr.

Das BSI ist bezüglich des Problems eindeutig. In seiner eigenen Berichterstattung zur digitalen Souveränität stellt die Behörde fest, dass die öffentliche Verwaltung derzeit hohe Abhängigkeiten von einzelnen US-Technologieanbietern hat. Dies birgt das Risiko, die Kontrolle über die eigene IT zu verlieren und Informations- und Datenschutz nach nationalen und EU-Vorgaben nicht mehr gewährleisten zu können. Bund, Länder und Kommunen haben gemeinsam das Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung zu bewahren und zu stärken.

Für Schwachstellenmanagement bedeutet das konkret: Die Souveränitätsfrage verdient von Anfang an einen Platz in der Bewertung. Wo werden Ihre Daten verarbeitet? Wo werden sie gespeichert? Unter welcher Jurisdiktion? Wer hat administrativen Zugriff? Das sind keine Beschaffungsfußnoten mehr für die öffentliche Verwaltung. Sie sind Teil des Risikobildes.

Erste Schritte für Bundesbehörden

Wenn CyberGovSecure gerade auf Ihrem Schreibtisch gelandet ist, hier eine praktische Reihenfolge für den Start.

1. Inventarisierung zuerst. Sie können keine Schwachstellen in Assets managen, die Sie nicht sehen. Beginnen Sie mit einer vollständigen, aktuellen Discovery Ihrer Assets und Angriffsfläche über alle Umgebungen hinweg, einschließlich Cloud, OT- und Remote-Endpoints.

2. Bewerten Sie den aktuellen Stand ehrlich. Welche Prozesse für Schwachstellenmanagement existieren heute? Was läuft automatisiert, und was lebt noch in Tabellen? Wo sind die Lücken?

3. Sprechen Sie früh mit dem BSI. Die Sicherheitsberatung und die CyberGovSecure-Teams können Wochen an Recherche zu Anforderungen und verfügbarer Unterstützung sparen.

4. Bewerten Sie speziell europäische Anbieter. Datensouveränität ist keine Checkbox. Sie betrifft rechtliches Risiko, Beschaffungspolitik, Auditfähigkeit und das Risiko, dass ein Tool aufgrund einer Entscheidung in einer anderen Jurisdiktion nicht mehr verfügbar ist.

5. Planen Sie Reports von Tag eins an. Die zentrale Berichterstattung im Rahmen von CyberGovSecure bedeutet, dass Auditierbarkeit nicht optional ist. Wählen Sie Tools und Prozesse, die die Erzeugung von Nachweisen zur Routine machen und nicht zur manuellen Fleißarbeit.

Wie Holm Security Bundesbehörden und Organisationen der Öffentlichen Hand unterstützen kann

Holm Security ist ein europäischer Anbieter für Schwachstellenmanagement. Unsere Plattform wird in Schweden und Polen entwickelt, wird in der EU gehostet und trägt zwei europäische Auszeichnungen für digitale Souveränität. Sie deckt Systeme, Netzwerke, Cloud, Webanwendungen, APIs, Active Directory, Operational Technology und die menschliche Angriffsfläche ab, mit kontinuierlichem, risikobasiertem Betrieb und auditbereiten Nachweisen als eingebaute Funktion.

Für Bundesbehörden, die bewerten, wie zeitgemäßes Schwachstellenmanagement im Rahmen einer CyberGovSecure-Umsetzung aussehen könnte, freuen wir uns über ein Gespräch.