CyberGovSecure and vulnerability management: What Germany's federal cybersecurity program means for the Bundesverwaltung

In May 2026, Germany's federal cabinet launched CyberGovSecure, the largest coordinated cybersecurity initiative the Bundesverwaltung has ever undertaken. Its purpose is direct: raise the security posture across every federal ministry and agency, and turn NIS2 from a compliance obligation into operational reality. Vulnerability management sits among the four priority areas for 2026.

For information security leads inside organizations of the Bundesverwaltung, this is a moment where policy, budget, and operational reality meet. This piece explains where CyberGovSecure fits in Germany's broader cybersecurity landscape, what its goal is for Behörden this year, and what modern vulnerability management looks like when it needs to keep pace with an AI-accelerated threat landscape.

The bigger picture: NIS2 in Germany

To understand CyberGovSecure, you have to understand the legal ground beneath it. NIS2 is the EU directive that raised the bar for cybersecurity across essential, critical and important sectors. Every member state had until 17 October 2024 to translate it into national law.

Germany missed that deadline by over a year. The European Commission opened an infringement procedure. After extensive parliamentary work, the Bundestag passed the *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (NIS2UmsuCG) on 13 November 2025. The Bundesrat approved it on 20 November, and it entered into force on 6 December 2025 with no transition period. About 29,500 organizations in Germany now fall under it, and fines can reach €10 million.

The law didn't create a separate NIS2 statute. Instead, it substantially amended the BSI-Gesetz, expanding BSI's mandate. Under the new framework, the President of BSI holds the role of *Koordinatorin der Bundesregierung für Informationssicherheit* (CISO Bund), giving the office central authority over federal information security.

CyberGovSecure is the operational answer to a specific question: how does the Bundesverwaltung, the federal administration itself, meet the requirements it now oversees for everyone else?

What is CyberGovSecure?

CyberGovSecure is the German federal government's central program for implementing NIS2 requirements across the Bundesverwaltung. It was decided by cabinet resolution and formally started with kick-off events in Berlin and Bonn on 4 May 2026. All federal ministries and authorities are included, and the program brings standards, measures, and funding together under one framework for the first time.

Two roles govern it. Strategic direction sits with a Lenkungskreis chaired by the *Bundesministerium für Digitales und Staatsmodernisierung* (BMDS). Operational coordination sits with Claudia Plattner, President of the BSI, in her role as head of the CISO Bund.

According to BSI, the program has defined nine action areas (Handlungsfelder) so far:

- Secure configuration and system hardening
- Asset management
- **Vulnerability management**
- Logging and detection
- Network security
- Information security controlling
- Resilient design of central services
- Data and access protection
- Secure and modern mobile device management

For 2026, four of these have been named as immediate priorities: secure back-up, secure configuration and system hardening, vulnerability management, and logging and detection. That priority list matters. It means every Bundesbehörde will be expected to demonstrate meaningful progress in vulnerability management within the next 12 to 18 months, tracked through a central reporting system that the BSI is building.

Why vulnerability management sits at the core

BSI didn't put vulnerability management in the first wave because it makes for a good headline. It's there because it's the foundation for almost every other CyberGovSecure priority.

You cannot harden what you haven't inventoried. You cannot detect attacks against systems you don't know are vulnerable. You cannot back up what you haven't mapped. When vulnerability management works well, secure configuration, detection, and back-up all become possible. When it doesn't, every downstream priority inherits the blind spots.

NIS2 makes this explicit. Article 21(2)(e) of the directive requires organizations to address vulnerability handling and disclosure as part of network and information systems security, and Article 21(2)(g) covers basic cyber hygiene practices. Together, these clauses are what CyberGovSecure translates into an operational program for public administration.

What "zeitgemäßes Schwachstellenmanagement" actually looks like

BSI's language is deliberate. The program calls specifically for "zeitgemäßes Schwachstellenmanagement," modern vulnerability management, not annual audits or quarterly scans. In practice, modern vulnerability management for public administration means five things.

- **Continuous, not periodic.** Vulnerabilities emerge daily, and systems change at a similar pace. A program built on quarterly assessments leaves 90-day windows of exposure and exploitation. Modern practice runs continuously across the full attack surface, so a new vulnerability gets detected when it appears, not months later.
- **Prioritized by real risk, not just severity score.** Not every vulnerability is equally dangerous. Modern practice factors in exploitability, exposure to the internet, and business impact rather than treating a raw CVSS number as the whole story. This matters most when a security team is small and the attack surface is large, which is often the case in Bundesbehörden.
- **Complete asset visibility first.** Vulnerability management depends on knowing what assets exist. That's why asset management is listed as its own Handlungsfeld alongside vulnerability management. Without accurate inventory, vulnerability management inherits every gap in the asset picture.
- **Actionable, not just informational.** Reports that list tens of thousands of vulnerabilities without prioritization aren't useful. Modern practice delivers a clear priority list security teams can actually work through, with concrete remediation guidance.
- **Audit-ready by default.** Central reporting under CyberGovSecure means evidence of improvement matters. Modern practice generates the documentation auditors and reviewers need as a built-in capability, not as a manual exercise after the fact.

The AI acceleration: why timing matters now

There's a reason CyberGovSecure prioritized vulnerability management. The threat landscape is changing faster than public administration cycles are used to accommodating.

Frontier AI models read code, find weaknesses, and produce working exploits at speeds that used to require experienced human researchers. The effort to attack has dropped sharply, while the effort to patch has stayed roughly where it was. The window between disclosure and exploitation has narrowed dramatically, and the safety margin most teams were unknowingly relying on has quietly disappeared.

There's a specific trap in this shift that catches teams off guard. AI is very good at chaining lower-risk vulnerabilities together. Individually, those findings looked minor, so they were deprioritized as low risk. But "low risk" often meant "hard to exploit," not "harmless," and AI removes that difficulty. Strung together, a handful of low-severity issues becomes a realistic attack path.

For a Bundesbehörde relying on annual or quarterly assessments, this means the assumption that "we'll address these in the next cycle" no longer holds. We covered this shift in more detail in our earlier piece on AI vulnerability management. The short version: speed of remediation, not just detection, is now the deciding factor in whether an organization stays out of the headlines.

CyberGovSecure's emphasis on "zeitgemäß" reflects this reality. It's not a stylistic word. It's an acknowledgment that vulnerability management processes from five years ago are no longer sufficient for the threat environment public administration operates in today.

Digital sovereignty in German public procurement

Alongside the operational shifts, there's a strategic one. When Behörden evaluate external partners for CyberGovSecure work, digital sovereignty is now an explicit criterion, not a soft preference.

BSI has been clear about the problem. In its own coverage of digital sovereignty, the agency states that public administration currently has high dependencies on individual US technology providers, which creates the risk of losing control over IT and no longer being able to guarantee information and data protection under national and EU rules. Bund, Länder, and Kommunen have jointly set the goal of preserving and strengthening the digital sovereignty of public administration.

For vulnerability management specifically, this means the sovereignty question deserves a place in the evaluation from the start. Where is your data processed? Where is it stored? Under which jurisdiction? Who has administrative access? These are no longer procurement footnotes for public administration. They're part of the risk picture.

First steps for federal agencies

If CyberGovSecure just landed on your desk, here's a practical starting sequence.

> **1. Inventory first.** You cannot manage vulnerabilities in assets you cannot see. Start with a complete, current asset inventory across all environments, including cloud and remote endpoints.

> **2. Assess your current state honestly.** What vulnerability management processes exist today? What runs automatically, and what still lives in spreadsheets? Where are the gaps?

> **3. Engage BSI early.** The Sicherheitsberatung and CyberGovSecure teams can save weeks of research on both requirements and available support.

> **4. Evaluate European vendors specifically.** Data sovereignty isn't a checkbox. It affects legal exposure, procurement policy, audit readiness, and the risk that a tool becomes unavailable to you because of a decision made in another jurisdiction.

> **5. Plan for evidence from day one.** Central reporting under CyberGovSecure means auditability isn't optional. Choose tools and processes that make evidence generation routine rather than a manual exercise.

How Holm Security supports federal agencies & public sector organizations

Holm Security is a European vulnerability management vendor. Our platform is developed in Sweden and Poland, hosted in the EU, and holds two European cybersecurity sovereignty labels. It covers systems, networks, cloud, web applications, APIs, Active Directory, operational technology, and the human attack surface, with continuous, risk-based operation and audit-ready evidence built in.

For Bundesbehörden evaluating what modern vulnerability management could look like as part of CyberGovSecure implementation, we'd welcome a conversation.