Wirtschaftsrat der CDU e.V.
Maik Hofmann
Head of Cybersecurity
E-Mail: info@wirtschaftsrat.de

Drei Prioritäten für Sicherheit, Resilienz und digitale Souveränität

Politischer Auftrag: Von Programmen zu nachweisbarer Schutzwirkung

Deutschlands Wettbewerbsfähigkeit, staatliche Handlungsfähigkeit und gesellschaftliche Stabilität hängen von sicheren digitalen Infrastrukturen ab. Cyberangriffe, Spionage und Sabotage treffen dabei nicht nur einzelne IT-Systeme, sondern Verwaltungsleistungen, Lieferketten und das Vertrauen in den Staat. Deutschland wird nicht jeden Cyberangriff verhindern können. Entscheidend ist, Angriffe früh zu erkennen, Schäden zu begrenzen, Leistungen aufrechtzuerhalten und aus Vorfällen zu lernen. [1]

Die Bundesregierung hat wichtige Grundlagen angestoßen: CyberGovSecure wurde nach dem vorliegenden Entwurf am 22. Juli 2026 für die Bundesverwaltung beschlossen; der Marktplatz Deutschland Digital ist seit dem 19. März 2026 in Betrieb; für den geplanten Cyberdome wurden am 7. September 2026 Sensorik, Analyseverbund und Schutzökosystem als drei Säulen beschrieben. Ein Beschluss ist jedoch noch keine flächendeckend verfügbare Schutzleistung, ein Marktplatz noch kein erfolgreicher Beschaffungsprozess und ein Architekturkonzept noch kein einsatzfähiger Verbund.

Die Bundesfachkommission Cybersicherheit empfiehlt deshalb, die Cybernation-Strategie in drei miteinander verzahnte Umsetzungsprioritäten zu übersetzen. Maßstab sind Schutzgewinn, Anschlussfähigkeit, wirtschaftlicher Hebel, Umsetzbarkeit und überprüfbare Ergebnisse bis Ende 2028.

1. Kommunale Handlungsfähigkeit sichern

Kritische Verwaltungsleistungen schützen: finanzierbar, abgestuft und praxistauglich

Kommunen erbringen unverzichtbare Leistungen für Bürger und Unternehmen. Ihre Sicherheits- und Personalausstattung ist jedoch sehr unterschiedlich. Gerade kleinere Verwaltungen können hochspezialisierte Sicherheitsfunktionen selten eigenständig vorhalten. Eine einheitliche Technikpflicht für alle wäre weder wirtschaftlich noch zweckmäßig. Erforderlich ist ein risikobasiertes, finanziertes Mindestniveau für die tatsächlich kritischen Leistungen. [2][3]

Unsere Forderung

Bund und Länder sollen 2027 gemeinsam mit kommunalen Spitzenverbänden und dem IT-Planungsrat einen abgestuften Umsetzungsrahmen für priorisierte Verwaltungsleistungen beschließen. Die Länder organisieren den kommunalen Zugang zu geeigneten Sicherheitsdiensten und sichern den Betrieb; der Bund unterstützt im Rahmen seiner Zuständigkeiten und über rechtlich tragfähige Finanzierungswege. Neue Pflichten dürfen nicht ungedeckt auf Kommunen übertragen werden.

- **Priorisierung nachvollziehbar festlegen:** IT-Planungsrat und Länder entwickeln mit Kommunen einen gemeinsamen Kriterienkatalog nach gesellschaftlicher Kritikalität, Ausfallfolgen, Wiederherstellungsbedarf, Abhängigkeiten und Migrationsfähigkeit. Zahl und Auswahl der Leistungen werden erst nach einer Bestandsaufnahme festgelegt, nicht ohne Datengrundlage vorgegeben.
- **Ein technologieoffenes Mindestniveau vorsehen:** starke Identitäten und Zugriffssteuerung, abgesicherte Endgeräte, Protokollierung und Angriffserkennung nach Schutzbedarf, sichere

Backups, getestete Wiederanlauf- und Notbetriebsverfahren, klare Melde- und Unterstützungswege sowie regelmäßige Übungen und wirksamkeitsgeprüfte Sensibilisierung der Beschäftigten. [4]

- **Gemeinsame SOC-, CERT- und Identitätsdienste landesweit oder länderübergreifend bereitstellen,** vorhandene Angebote bevorzugen und ihre Schnittstellen auf eine spätere Anbindung an den Cyberdome ausrichten. Mandantentrennung, Redundanz und eigene Ausfallvorsorge verhindern neue Konzentrationsrisiken.
- **Finanzierung und Personal zusammen denken:** mehrjährige Betriebsmittel für Implementierung, Migration, Fachkräfte, Qualifizierung, Wartung, Übungen und Wiederherstellung vorsehen. Eine belastbare Kostenschätzung wird aus Piloten und kommunalen Bestandsdaten abgeleitet.
- **Stufenweise einführen:** 2027 Kriterien, Finanzierung und Pilotkommunen festlegen; 2028 erprobte Modelle auf weitere Kommunen übertragen. Eine vollständige Umsetzung in sämtlichen Kommunen bis Ende 2028 wird nicht vorausgesetzt.

Erfolgskontrolle bis Ende 2028

Gemessen werden der Anteil priorisierter Leistungen mit finanziertem Schutzbetrieb, die erfolgreiche Durchführung von Notbetriebs- und Wiederanlauftests, die tatsächliche Verfügbarkeit wesentlicher Leistungen im Krisenfall sowie die Umsetzung der Übungserkenntnisse. Ergebnisse müssen zwischen Kommunen vergleichbar sein, ohne unterschiedliche Ausgangslagen zu ignorieren. Ergänzend wird die Melderate tatsächlich verdächtiger Vorkommnisse durch Beschäftigte unter vergleichbaren Bedingungen gegenüber einer dokumentierten Ausgangslage ausgewiesen; Fehlmeldungen und Meldequalität werden dabei berücksichtigt.

2. Sicherheit und Souveränität verbindlich beschaffen

Öffentliche Beschaffung als Schutz- und Innovationshebel

Der Staat kann als strategischer Erst- und Referenzkunde sichere digitale Lösungen in die Breite bringen. Digitale Souveränität bedeutet dabei nicht nationale Abschottung, sondern die Fähigkeit, Abhängigkeiten zu verstehen, wirksam zu kontrollieren und im Krisenfall zu wechseln. Für sicherheitskritische IT-Beschaffungen sind deshalb nachprüfbare, risikobasierte Kriterien erforderlich. [5]

Unsere Forderung

BMDS, öffentliche Beschaffungsstellen, Länder, FITKO und öffentliche IT-Dienstleister sollen unter Einbindung des BSI bis 2027 ein modulares Prüf- und Musterklauselwerk erarbeiten, zunächst für ausgewählte besonders kritische Beschaffungen. Ein abgestuftes Verfahren vermeidet neue pauschale Nachweislasten.

- **Risiko vor Herkunft:** Schutzbedarf, Funktion des Systems, Datenarten, Betriebsmodell, Lieferkette, Zugriffsrechte, Update- und Supportabhängigkeiten sowie mögliche Rechtszugriffe Dritter bewerten. Entwicklungs-, Betriebs- und Eigentümerstrukturen können risikorelevante Indikatoren sein und gilt es daher einer sachlich rechttreuen Bewertung zu unterziehen.
- **Kontrollierbarkeit sicherstellen:** offene Schnittstellen, dokumentierte Datenformate, überprüfbare Sicherheitsnachweise, Datenhoheit, Interoperabilität, getestete Exit- und Migrationspfade sowie Notfallfähigkeit vertraglich festlegen. Auch die Speicherung und Nutzung von Sicherheits- und Telemetriedaten sind einzubeziehen. [5]
- **Innovationsfreundlich beschaffen:** verhältnismäßige Nachweise, gleichwertige Alternativen zu teuren Zertifikaten und gegebenenfalls Unterstützung bei Prüfkosten für junge und mittelständische Anbieter ermöglichen; angemessene Losbildung und transparente Auswahlverfahren sichern Wettbewerb.

- **Bestehende Infrastruktur nutzen:** die Cybersicherheitsfunktion des Marktplatzes Deutschland Digital gezielt weiterentwickeln statt eine parallele nationale Plattform zu errichten. Piloten sollen über innovationsorientierte Beschaffung und reguläre Vergabeverfahren in skalierbare Aufträge überführt werden.
- **Rechtliche Tragfähigkeit vor Anwendung prüfen:** Musterkriterien durch Vergabe- und Datenschutzexpertise validieren, transparent dokumentieren und in Pilotvergaben erproben, bevor sie breit eingesetzt werden.

Erfolgskontrolle bis Ende 2028

Ausgewiesen werden Zahl und Volumen aus Piloten hervorgegangener Regelaufträge, Vergabedauer, Vielfalt erfolgreicher Anbieter, nachweisliche Übertragbarkeit erprobter Lösungen auf weitere Verwaltungen und der Anteil kritischer Verträge mit praktikablem, getestetem Wechselverfahren.

3. Cyberdome, Reaktion und unabhängiges Lernen verbinden

Ein föderaler Wirkverbund statt zusätzlicher Parallelstrukturen

Deutschland verfügt über leistungsfähige Behörden, CERTs, Lagezentren und betriebliche Sicherheitsteams. Der geplante Cyberdome kann ihren Nutzen steigern, wenn Sensorik, Analyse und Schutzmaßnahmen interoperabel zusammenwirken. Ein gemeinsames Lagebild, operative Einsatzführung und unabhängige Vorfallanalyse erfüllen unterschiedliche Aufgaben. Diese Funktionen müssen verbunden, aber institutionell und rechtlich klar abgegrenzt werden. [7]

Unsere Forderung

BMI und BSI sollen mit Ländern, IT-Planungsrat und der Cybersicherheitswirtschaft ein schrittweise umsetzbares, föderales Realisierungskonzept für den Cyberdome vorlegen. Der Beteiligungsprozess muss große, mittelständische und junge Anbieter einbeziehen; vergaberechtliche Vorkehrungen sollen faire spätere Wettbewerbsverfahren trotz früher Marktkonsultation ermöglichen.

- **Föderale Zuständigkeiten vorab klären:** eine mit Bund und Ländern vereinbarte Verantwortungs- und Eskalationsmatrix regelt Befugnisse, Hilfeersuchen, Entscheidungswege und Einsatzführung im Rahmen bestehender Kompetenzen. Offene Rechtsfragen sind ausdrücklich zu benennen und erforderlichenfalls gesetzgeberisch zu lösen.
- **Dezentrale Datenverarbeitung als Regelfall:** Sicherheitsdaten bei Betreibern und Dienstleistern erfassen und vorverarbeiten; für übergreifende Analysen nur erforderliche, soweit möglich pseudonymisierte Informationen austauschen. Datenhoheit, Zweckbindung, Vertraulichkeit und robuste Ausfallvorsorge sichern.
- **Offene Anschlussbedingungen schaffen:** für Sensorik, Analyseverbund und Schutzökosystem dokumentierte Schnittstellen, Datenmodelle und Konformitätskriterien veröffentlichen; vorhandene Fähigkeiten anschließen und neue Komponenten nur bei nachgewiesenen Lücken aufbauen.
- **Meldewege sinnvoll verzahnen:** Schnittstellen zu gesetzlichen Meldeverfahren nach NIS2 und BSI-Gesetz so ausgestalten, dass Informationen mehrfach genutzt werden können; rechtliche Meldepflichten bleiben bestehen, solange keine zulässige Integration umgesetzt ist. [6]
- **Wirkung messbar machen:** einheitliche Definitionen für Vorfallbeginn, Erkennungszeit, Reaktionsbeginn, Eindämmung, Wiederaufnahme des Notbetriebs und vollständige Wiederherstellung festlegen. Mean Time To Detect (MTTD) und getrennte Reaktions- und Wiederherstellungszeiten sind nur mit vergleichbaren Messpunkten aussagekräftig.

- **Unabhängiges Lernen institutionell absichern:** eine unabhängige Überprüfungsfunktion nach dem Modell eines Cyber Safety Review Boards für schwere und systemisch relevante Vorfälle auf Grundlage eines geprüften Rechts- und Organisationsmodells vorsehen. Vorrangig ist zu prüfen, ob diese Funktion an bestehende Strukturen angebunden werden kann, ohne ihre fachliche Unabhängigkeit zu beeinträchtigen. Unabhängige Fachleute aus Staat, Wissenschaft und Praxis sollten transparent und mit Regeln zu potentiellen Interessenkonflikten berufen werden. Zugang zu Informationen, Schutz von Geschäftsgeheimnissen, Datenschutz und Verhältnis zu BSI, Aufsicht und Strafverfolgung müssen rechtlich geklärt sein.

Realistischer Umsetzungspfad und Erfolgskontrolle

Bis Ende 2027 sollen Zuständigkeitsmatrix, erste veröffentlichte Anschlussstandards, abgestimmte Austauschregeln und ein gemeinsames föderales Übungsszenario vorliegen. Bis Ende 2028 sollen ausgewählte Verbundkomponenten im praktischen Betrieb erprobt, Eskalationswege getestet und Veränderungen von Erkennungs-, Reaktions- und Wiederherstellungszeiten gegenüber einer dokumentierten Ausgangslage ausgewiesen sein. Das Review-Modell soll rechtlich und organisatorisch geklärt und an ersten geeigneten Fällen erprobt werden.

Gemeinsames Arbeitsprogramm 2027–2028

Die drei Prioritäten verstärken einander: Kommunale Dienste schaffen Schutz und geeignete dezentrale Anknüpfungspunkte; der Cyberdome verbindet Informationen und antizipatorische Reaktion; risikobasierte, souveräne Beschaffung sichert Interoperabilität, Wettbewerb und Wechselmöglichkeiten. Der Cyberdome sollte selbst nach den Sicherheits- und Souveränitätsanforderungen des zweiten Schwerpunkts beschafft werden.

- **2027: Zuständigkeiten und Priorisierung vereinbaren:** Pilotvorhaben, Finanzierungs- und Personalbedarf erfassen; Musterklauseln und erste Schnittstellen veröffentlichen; gemeinsame Übungen vorbereiten.
- **2028: erprobte Ansätze stufenweise übertragen:** betriebliche Schutzwirkung und Dienstverfügbarkeit messen; Beschaffungs- und Wechselverfahren evaluieren; föderale Reaktionsabläufe üben und Erkenntnisse aus Vorfällen nachverfolgen.
- **Steuerung**: BMDS und BMI sollen gemeinsam mit Ländern, Kommunen und Wirtschaft eine schlanke, öffentlich nachvollziehbare Fortschrittsübersicht mit wenigen einheitlichen Wirkungskennzahlen etablieren. Zuständigkeiten bleiben bei den jeweils rechtlich verantwortlichen Stellen.

Forderung an die Bundesregierung

Die Bundesfachkommission Cybersicherheit des Wirtschaftsrates der CDU e.V. empfiehlt BMDS und BMI, gemeinsam mit den Ländern aus diesen drei Prioritäten ein verbindlich abgestimmtes, finanziell unterlegtes und messbares Arbeitsprogramm zu entwickeln. Entscheidend ist nicht die Zahl neuer Institutionen oder Strategien, sondern ob Verwaltungsleistungen auch unter Angriffen verfügbar bleiben, kritische Technologie beherrschbar und wechselbar ist und Cybervorfälle schneller erkannt, bekämpft und systematisch ausgewertet werden. Deutschland wird nicht jeden Cyberangriff verhindern können. Es kann aber die Voraussetzungen schaffen, damit Staat und Wirtschaft auch im Cyberkrisenfall handlungsfähig bleiben.

Quellen und fachliche Grundlagen

- [1] Bundesamt für Sicherheit in der Informationstechnik (BSI), Lageberichte zur IT-Sicherheit in Deutschland (offizielle Übersicht). https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/cyber-sicherheitslage.html
- [2] ENISA, NIS Investments 2025, 8. Dezember 2025. EU-weite Befragung; kein spezifischer Kommunaldatensatz. https://www.enisa.europa.eu/publications/nis-investments-2025
- [3] ENISA, Sectorial Threat Landscape – Public Administration, 6. November 2025. https://www.enisa.europa.eu/publications
- [4] BSI, IT-Grundschutz-Kompendium (offizielle Publikations- und Informationsseiten). https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
- [5] Verordnung (EU) 2024/2847 (Cyberresilienz-Verordnung), Amtsblatt der Europäischen Union vom 20. November 2024. Betrifft Produkte mit digitalen Elementen; kein allgemeines Vergaberecht. https://eur-lex.europa.eu/eli/reg/2024/2847/oj
- [6] ENISA, NIS2 Technical Implementation Guidance, Juni 2025. Sektorspezifische Umsetzungshilfe; nicht auf alle Verwaltungsstellen unmittelbar übertragbar. https://www.enisa.europa.eu/publications
- [7] ENISA, NIS360, Ausgabe 2026, 28. Mai 2026. https://www.enisa.europa.eu/publications
- [8] ENISA, The ENISA Cybersecurity Exercise Methodology, 16. Februar 2026. https://www.enisa.europa.eu/publications/the-enisa-cybersecurity-exercise-methodology

Berlin, Oktober 2026