REFORM-DOSSIER
Nr. 9

Innere Sicherheit & KRITIS

Föderiertes Lagebild, Cyber- und Infrastrukturresilienz, Grundrechtsschutz

aus der Reihe
Betriebssystem Deutschland
Eine Reformarchitektur für einen funktionierenden Staat

Verwendbarer Baustein · Stand Juni 2026

Steckbrief

Reformwelle	Welle 1–3 (KRITIS-Register früh, Lagebild später)
Alltagsspürbarkeit	Mittel (sichtbar v. a. in Krisen)
Breitenwirkung	Hoch – Schutz von Bevölkerung und Versorgung
Rechtsweg	Sehr sensibel – Ländersache, NIS2/CER (EU), Grundrechte
Datenschutzrisiko	Hoch – strikte Trennung, keine zentrale Bürgerdatenbank
Politische Angreifbarkeit	Hoch (Freiheit vs. Sicherheit)
Leitidee	Handlungsfähigkeit und Grundrechtsschutz gleichrangig

1. Ausgangsproblem

Innere Sicherheit braucht ein gemeinsames Lagebild, schnelle Reaktionsfähigkeit und den Schutz kritischer Infrastrukturen. Zugleich ist die Versuchung zur Zentralisierung hier besonders groß – und besonders gefährlich, weil sie in einen Überwachungsstaat führen kann. Hinzu kommt: Mit der Digitalisierung wachsen die Systeme zusammen und werden zur gemeinsamen Angriffsfläche; Cyber- und Infrastrukturrisiken sind heute systemkritisch.

2. Zielbild

Eine föderiert integrierte Lage- und Resilienzarchitektur, die Handlungsfähigkeit und Grundrechtsschutz als zwei gleichrangige Prinzipien behandelt – nicht als Gegensatz. Ein gemeinsames Lagebild entsteht aus der kontrollierten Verbindung der Daten der Länderpolizeien, nicht aus einer zentralen Sicherheitsdatenbank aller Bürger. Cyber- und KRITIS-Resilienz werden zur verbindlichen Querschnittspflicht.

> *Freiheit braucht einen Staat, der schützen kann – und kontrolliert wird. Kein kritisches System geht produktiv ohne Notbetrieb, Wiederanlauf, Sicherheitsprüfung und Angriffssimulation.*

3. Reformdividende

Höhere Resilienz gegen Cyberangriffe und Infrastrukturausfälle, ein besseres gemeinsames Lagebild und nachweisbare Wiederanlauffähigkeit kritischer Systeme. Das KRITIS-Register und die Resilienzpflichten sind rechtlich gut zugänglich und früh wirksam; das föderierte Lagebild ist anspruchsvoller und folgt später.

4. Startmodule

- **KRITIS-Register & Meldeprozesse** – Erfassung kritischer Infrastrukturen, Melde- und Mindeststandards (NIS2/CER).
- **Cyberlagebild** – gemeinsame Sicht auf die Bedrohungslage.
- **Red-Team-Übungen & Notbetriebsnachweise** – Angriffssimulationen und nachgewiesene Wiederanlauffähigkeit als Bauvoraussetzung.

5. Rechtsrahmen

Innere Sicherheit ist überwiegend Ländersache; Cyber- und KRITIS-Vorgaben sind durch EU-Recht geprägt (NIS2-Richtlinie mit 18 Sektoren, CER-Richtlinie)[1]. Einfachgesetzlich zugänglich sind KRITIS-Register, Meldeprozesse und Cyber-Mindeststandards. Verfassungsnah und besonders sensibel sind Polizeidatenfusion, umfassende KRITIS-Datensammlung und der Einsatz der Bundeswehr im Inneren. Nicht tragfähig in Radikalform: die Abschaffung der Länderpolizeien, eine zentrale Sicherheitsdatenbank aller Bürger, autonome Sicherheitsentscheidungen ohne Mensch und Militär im Inneren ohne Verfassungsgrundlage.

6. Zielarchitektur

Föderiert, nicht zentralisiert. Ein gemeinsames Lagebild entsteht aus der kontrollierten Verbindung der Länderdaten. Eine digitale Beweiskette trennt sauber zwischen Verdacht, Fakt und Prognose. KRITIS-Objekte werden mit Software-Stücklisten (SBOM) und Resilienznachweisen geführt; regelmäßige Red-Team-Übungen prüfen die Widerstandsfähigkeit. Künstliche Intelligenz unterstützt bei Analyse und Anomalieerkennung – sie entscheidet nicht autonom über polizeiliche Eingriffe.

7. Datenräume & Schnittstellen

Der Sicherheitsdatenraum bleibt strikt von Gesundheits-, Steuer-, Bildungs-, Migrations- und Mobilitätsdaten getrennt; eine Fusion ist ausgeschlossen. Über Grundrechtseingriffe entscheidet ein Mensch mit Rechtsgrundlage und gerichtlicher Kontrolle. Zugriffe sind zweckgebunden, protokolliert und richterlich kontrollierbar. KRITIS-Schnittstellen verbinden Betreiber, Aufsicht und Lagebild.

8. Finanzierungslogik

Sicherheit und Resilienz erzeugen vor allem Risikoreduktion (Nutzenkategorie C8) – sie rechtfertigen Investitionen, schaffen aber keine frei verfügbaren Haushaltsmittel. Der Wert liegt in vermiedenen Schäden durch Cyberangriffe, Infrastrukturausfälle und Krisen. KRITIS-Mindeststandards verlagern zudem einen Teil der Resilienzkosten zu den Betreibern.

9. Migrationspfad

Phase	Zeitraum	Schritte
0 · Baseline	0–2 J.	KRITIS-Sektoren erfassen, Schutzklassen, NIS2-/CER-Pflichten umsetzen (NIS2-Umsetzungsgesetz seit 12/2025, KRITIS-Dachgesetz seit 03/2026 in Kraft)
1 · Resilienz	1–5 J.	KRITIS-Register, Cyber-Mindeststandards, Notbetriebs- und Wiederanlaufnachweise, Red-Team-Übungen
2 · Lagebild	3–8 J.	Föderiertes Lagebild, digitale Beweiskette, abgestimmte Polizeidatenstandards
3 · Integration	8+ J.	Integrierte Resilienzarchitektur bei erhaltener föderaler Zuständigkeit

[1] NIS2-Richtlinie (18 Sektoren) und CER-Richtlinie (11 Sektoren, physische Resilienz kritischer Einrichtungen). Das deutsche NIS2-Umsetzungsgesetz (NIS2UmsuCG) ist seit dem 6. Dezember 2025 in Kraft; BSI-Registrierungsportal seit Januar 2026. Quelle: OpenKRITIS.

10. Kennzahlen (KPI)

- Abdeckungsgrad des KRITIS-Registers, Erfüllungsquote der Mindeststandards
- Nachgewiesene Wiederanlauffähigkeit kritischer Systeme
- Ergebnisse von Angriffssimulationen (Red Teaming)
- Qualität und Aktualität des gemeinsamen Lagebilds

11. Risiken & Worst Case

Das zentrale Risiko ist eine Architektur, die unter dem Sicherheitsargument Grundrechte aushöhlt – eine zentrale Bürgerdatenbank oder autonome Eingriffsentscheidungen. Das Gegenmittel ist in die Architektur eingebaut: Datentrennung, Human-in-the-Loop, richterliche Kontrolle. Der zweite Risikofall ist der reale Schaden durch unzureichende Resilienz. Im Worst Case verzögern Grundrechts- und Föderalismuskonflikte das Lagebild – deshalb beginnt die Reform mit den unstrittigen Resilienzmodulen.

12. Politische Anschlussfähigkeit

Lager	Anknüpfungspunkt
CDU/CSU	Handlungsfähigkeit, Schutz, Resilienz
SPD	Bevölkerungsschutz, KRITIS, öffentliche Sicherheit
Grüne / Linke	Grundrechtsschutz, richterliche Kontrolle, keine Massendaten
Liberale Akteure	Rechtsstaatlichkeit, Verhältnismäßigkeit, Datenschutz
Länder & Betreiber	Föderiertes Lagebild statt Zentralisierung, klare Pflichten

Die Resilienzmodule (KRITIS, Cyber, Notbetrieb) sind über die Lager hinweg anschlussfähig und gehören in die erste Welle. Das Lagebild ist sensibler und nur tragfähig, wenn der Grundrechtsschutz von Anfang an gleichrangig mitgebaut wird.