Studie

Framework für digitale Resilienz

[01.10.2026] Cybersicherheit allein reicht nicht aus, um Staat und Verwaltung auch in Krisen handlungsfähig zu halten. Zu diesem Ergebnis kommt eine Studie des The Open Government Institute. Die Forscher entwickeln deshalb das Konzept der „digitalen öffentlichen Resilienz“ und schlagen unter anderem die Einrichtung eines Chief Resilience Officers vor.

Die zunehmende Abhängigkeit der öffentlichen Verwaltung von digitalen Infrastrukturen, Daten, Fachverfahren und Kommunikationsnetzen verändert die Anforderungen an die Krisenvorsorge. Cyberangriffe, Ausfälle kritischer Infrastrukturen, Extremwetterereignisse und geopolitische Spannungen gehören ebenso zum Bedrohungsszenario wie Desinformation und KI-gestützte Manipulationen.

Professor Jörn von Lucke und Sander Frank vom The Open Government Institute (TOGI) der Zeppelin Universität in InstituteFriedrichshafen haben deshalb untersucht, wie Resilienz, Cyberresilienz, digitale Souveränität und zivile Verteidigung zusammenspielen. Grundlage ihrer Studie sind eine systematische Literaturrecherche sowie eine qualitative Gap-Analyse europäischer und deutscher Strategien, Regulierungen, Rahmenwerke und Forschungsansätze.

Maßnahmen bislang häufig isoliert

Wie das TOGI in seinem aktuellen Newsletter mitteilt, gibt es nach Einschätzung der Forscher bereits zahlreiche Maßnahmen zur Stärkung der Widerstandsfähigkeit öffentlicher Institutionen. Diese würden jedoch häufig isoliert entwickelt und umgesetzt. Weitgehend fehle ein integrierter Ansatz, der die digitale Handlungs- und Leistungsfähigkeit von Staat und Verwaltung auch unter Krisen- und Verteidigungsbedingungen sicherstellt.

Diese Lücke soll das Konzept der „digitalen öffentlichen Resilienz“ schließen. Gemeint ist damit die Fähigkeit öffentlicher Institutionen, digitale Leistungen auch unter schwierigen Bedingungen aufrechtzuerhalten, sich an Veränderungen anzupassen und aus Störungen zu lernen. Das von den Forschern entwickelte Framework umfasst fünf Gestaltungsdimensionen: Strategie, Priorisierung, Implementierung, Training und Governance. Verwaltungen sollen damit unter anderem Abhängigkeiten und Risiken erkennen, Maßnahmen priorisieren, Beschäftigte qualifizieren und Verantwortlichkeiten festlegen können.

Chief Resilience Officer als zentrale Schnittstelle

Für die organisatorische Verankerung schlagen von Lucke und Frank einen Chief Resilience Officer (CRO) vor. Diese Funktion soll bestehende Zuständigkeiten bündeln und die ressort- und ebenenübergreifende Resilienzstrategie koordinieren. Technische, organisatorische, informationelle und soziale Aspekte könnten so stärker miteinander verzahnt werden. Zu einer vergleichbaren Empfehlung kam im August 2026 eine unabhängig davon erstellte Resilienzstudie für das Land Berlin. Auch dort wurde die Einrichtung eines Chief Resilience Officers bei der Senatskanzlei vorgeschlagen.

Die TOGI-Studie macht damit deutlich, dass digitale Resilienz über klassische IT- und Cyber-Sicherheit hinausgeht. Robuste Infrastrukturen und digitale Souveränität gehören ebenso dazu wie vertrauenswürdige Kommunikationswege, kontinuierliches Lernen, digitale Kompetenzen und eine vorausschauende Governance. Ziel ist letztlich, die staatliche Handlungsfähigkeit auch dann zu erhalten, wenn digitale Systeme und Verwaltungsstrukturen unter außergewöhnlichem Druck stehen.

()

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, Digitale Resilienz, TOGI, Zeppelin Universität