

Whitepaper zur Nachrichtendienstrechtsreform: Staatliches Schwachstellenmanagement klar regeln

Die Reform des Nachrichtendienstrechts ist Teil der laufenden Neuordnung der deutschen Sicherheitsarchitektur und soll die Aufklärungsfähigkeiten von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz insbesondere im Cyberraum erweitern. Damit wird auf die deutlich zugespitzte Sicherheitslage und die wachsenden hybriden und digitalen Bedrohungen für Deutschland reagiert. Vorgesehen sind unter anderem Befugnisse zur aktiven Cyberabwehr.

Die verschärfte Bedrohungslage erfordert leistungsfähige Sicherheitsbehörden und wirksame Instrumente zur Aufklärung und Abwehr von Cyberangriffen. Der Ausbau staatlicher Befugnisse darf jedoch keine zusätzlichen Anreize schaffen, bekanntgewordene IT-Schwachstellen bewusst offenzuhalten oder ihre Schließung zu verzögern. Denn jede nicht behobene Sicherheitslücke kann von Dritten ausgenutzt werden und birgt damit erhebliche Risiken für Bürgerinnen und Bürger, Unternehmen, Behörden und kritische Infrastrukturen und gefährdet nicht zuletzt das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Für den staatlichen Umgang mit Schwachstellen braucht es deshalb klare Vorgaben:

- **Schwachstellen müssen grundsätzlich geschlossen werden.** Die Behebung von Sicherheitslücken, Responsible Disclosure und der Schutz betroffener Systeme müssen Vorrang haben und den Regelfall darstellen.
- **Der Umgang mit Schwachstellen braucht klare Grenzen.** Erlangen Nachrichtendienste Kenntnis von Schwachstellen, dürfen diese nicht ohne Weiteres operativ ausgenutzt oder ihre Behebung hinausgezögert werden. Es braucht ein gesetzlich verankertes Schwachstellenmanagement, das:
 - für jede Entscheidung über das Offenhalten einer Lücke einen verpflichtenden, strukturierten Abwägungsprozess vorschreibt, der die Gefahren einer weiteren Verbreitung gegen den konkreten Nutzen abwägt;
 - klar definierte, transparente Kriterien für die Abwägung vorschreibt und zu Mitigationsmaßnahmen verpflichtet;
 - einer effektiven Kontrolle unterworfen wird;
 - sicherstellt, dass diese gesetzlichen Schutzvorgaben nicht durch vertragliche Vereinbarungen umgangen oder abgeschwächt werden können.
- **Vertrauensbasierte Meldewege müssen geschützt bleiben.** Schwachstelleninformationen, die dem Bundesamt für Sicherheit in der Informationstechnik im Rahmen seiner Melde- und Koordinierungsfunktionen anvertraut werden, dürfen unter keinen Umständen – auch nicht freiwillig – an die Nachrichtendienste übermittelt werden.

Die Reform des Nachrichtendienstrechts sollte genutzt werden, um diese Leitplanken gesetzlich zu verankern. Ein gesetzlich verankertes staatliches Schwachstellenmanagement ist verfassungsrechtlich geboten: Das Bundesverfassungsgericht hat bereits entschieden, dass den Staat eine grundrechtliche Schutzpflicht trifft und er den Umgang mit ihm bekannten Sicherheitslücken gesetzlich regeln muss.