DATENSPARSAMKEIT UND DATENSICHERHEIT

GLEICHE MAßSTÄBE

BEI STAAT UND WIRTSCHAFT

BESCHLUSS DES MIT-BUNDESVORSTANDS AM 30.SEPTEMBER 2026

Cyberkriminalität verursacht der deutschen Wirtschaft Jahr für Jahr Schäden. Nach der aktuellen Studie „Wirtschaftsschutz 2026“ des Digitalverbands Bitkom bewegt sich der jährliche Gesamtschaden für die deutsche Wirtschaft durch Diebstahl, Spionage und Sabotage zwischen 160 und rund 205 Milliarden Euro – ein neuer Rekordwert und bereits seit mehreren Jahren in Folge eine Schadenssumme in dreistelliger Milliardenhöhe.

Diese Zahlen zeigen: Cybersicherheit ist längst keine IT-Fachfrage mehr, sondern eine Frage der wirtschaftlichen Wettbewerbsfähigkeit und der Sicherheit unseres Standorts. Der Mittelstand trägt dabei eine doppelte Last – er ist selbst Ziel von Angriffen und muss gleichzeitig hohe gesetzliche Sicherheitsanforderungen erfüllen, während der Staat, dem Unternehmen zunehmend Daten übermitteln müssen, seine eigenen Hausaufgaben nicht macht.

Zwischen dem 7. und 12. August 2026 erbeutete die Erpressergruppe „Rhysida“ rund 5,8 Terabyte an Daten – etwa 1,44 Millionen Dateien – aus zwei Berliner Senatsverwaltungen. Betroffen waren Daten von Bürgerinnen und Bürgern sowie Unternehmen.

Unter den erbeuteten Daten befanden sich sicherheitsrelevante Informationen zu kritischer Infrastruktur – zu Wasser- und Stromversorgung, also zu Bereichen, die von KRITIS-Betreibern verantwortet werden. Diese Betreiber können ihre eigenen Systeme nach höchsten gesetzlichen Standards absichern und werden trotzdem zum Sicherheitsrisiko, wenn Behörden die über sie gesammelten Informationen nicht schützen.

Staatliche Behörden aber sammeln im Zuge von Genehmigungsverfahren, Vergabeverfahren, Förderprogrammen, Betriebsprüfungen, Statistikpflichten und der Aufsicht über kritische Infrastrukturen laufend hochsensible und teils vertrauliche Informationen über Unternehmen – von Betriebsgeheimnissen über Standort- und Sicherheitsdaten bis zu Kalkulationsgrundlagen in Ausschreibungen. Der Fall Berlin zeigt: Diese Daten sind im öffentlichen Sektor nicht durchgängig nach dem Stand der Technik geschützt. Das ist ein handfestes Wettbewerbs- und Vertrauensproblem: Der Staat verlangt von der Wirtschaft ein Sicherheitsniveau, das er bei sich selbst nicht durchsetzt.

Die Mittelstands- und Wirtschaftsunion (MIT) fordert daher:

1. **Grundsatz: Was der Staat erhebt, muss er schützen können**

Jede neue Melde-, Nachweis- oder Übermittlungspflicht für Unternehmensdaten ist vor ihrer Einführung auf Erforderlichkeit, Bürokratieaufwand und Informationssicherheit zu prüfen. Die Prüfung umfasst Schutzbedarf, Datenumfang, Speicher- und Löschfristen, Zugriffsrechte, Verschlüsselung, Angriffserkennung und Notfallvorsorge. Datenschutz- und Informationssicherheitsbeauftragte sind frühzeitig einzubeziehen. Eine neue Pflicht zur Übermittlung vertraulicher Daten darf erst praktisch wirksam werden, wenn die empfangende Stelle oder ein sicherer alternativer Übermittlungsweg ein angemessenes Schutzniveau nachweisen kann. Bestehende gesetzliche Pflichten dürfen nicht durch den bloßen Ablauf eines Zertifikats unklar werden; dafür sind sichere Übergangswege und verbindliche Nachbesserungsfristen vorzusehen. Insbesondere ist jedwede Funktionsfähigkeit von Hard- und Software von der Laufzeit von Lizenzen unabhängig umzusetzen: Nur weil eine Lizenz abläuft, darf die Handlungsfähigkeit nicht verloren gehen.

2. Einheitliche und überprüfbare Sicherheitsstandards für die gesamte öffentliche Verwaltung

Für Bund, Länder und Kommunen muss ein vergleichbares, verbindliches Schutzniveau gelten. Dass weiterhin der BSI-Grundschutz in der öffentlichen Verwaltung nicht obligatorisch umgesetzt ist, verwundert. Die für die Bundesverwaltung bereits bestehenden Anforderungen sind zu berücksichtigen; Lücken auf Landes- und Kommunalebene sind durch abgestimmte Mindeststandards, klare Meldewege, Aufsicht und verbindliche Umsetzungsfristen zu schließen. Jede öffentliche Stelle muss grundlegende technische und organisatorische Schutzmaßnahmen nachweisen. Bei erhöhtem Schutzbedarf sind ein vollständiges Informationssicherheitsmanagementsystem und unabhängige Prüfungen erforderlich. Sofern eine Kommune aus eigener Kraft – finanziell oder personell – dies nicht gewährleisten bzw. vorhalten kann, kann die Landesverwaltung mit standardisierten und zertifizierten Angeboten aushelfen. Eine Zusammenlegung der IT mehrerer Gemeinden zur Sicherstellung des Schutzniveaus ist über angepasste Gesetze und Richtlinien im Verwaltungs- und Steuerrecht durch Land und Bund kurzfristig zu ermöglichen.

3. Professioneller IT-Betrieb und stärkere Einbindung der IT-Sicherheitswirtschaft

Insbesondere kleinere Kommunen – auch mehrere zusammenarbeitende – können den sicheren Betrieb komplexer Systeme häufig nicht allein mit eigenem Personal leisten. Qualifizierte privatwirtschaftliche IT- und Cybersicherheitsdienstleister sollen daher regelhaft in Planung und Betrieb einbezogen werden – auch im Auftrag öffentlicher IT-Verbünde. Dazu gehören etwa Sicherheitsüberwachung, Patch- und Schwachstellenmanagement, Identitäts- und Berechtigungsmanagement, Datensicherung, Wiederanlauf und Hilfe bei Sicherheitsvorfällen.
Bund und Länder sollen mittelstandsfreundliche Rahmenverträge, offene Schnittstellen und nachvollziehbare Eignungskriterien schaffen. Beschaffungen müssen qualifizierten mittelständischen Systemhäusern und spezialisierten Sicherheitsunternehmen einen fairen Zugang eröffnen. Die Bündelung von IT-Aufgaben in ausgegründeten behördlichen oder behördenähnlichen Strukturen (z. B. AöR) ist bereits gelebte Praxis. Hier ist insbesondere der Schutzbereich des Vergaberechts zu beachten, so dass die konkrete Aufgabenstellung und räumliche Zuständigkeit auf den öffentlich-rechtlichen Eigentümer beschränkt bleiben. Jedwedes Angebot in den Markt, auch an dritte öffentliche Stellen, schädigt den Wettbewerb. Die

Einhaltung des Umsatzsteuerrechts bei wirtschaftlicher Betätigung ist auch durch den öffentlich-rechtlichen Eigentümer jährlich zu prüfen, um eine unmittelbare preisliche Benachteiligung privater Anbieter zu vermeiden. Ideal erscheint die Kooperation privater und öffentlich-rechtlicher Dienstleister: Die öffentliche Stelle bleibt für Schutzbedarf, Auswahl, Steuerung und Kontrolle verantwortlich, während die Wirtschaft technisch aktuelle und operativ agile Leistungen erbringen kann. Die Konzentrations- und Ausfallrisiken großer gemeinsamer Dienstleister sind ausdrücklich zu prüfen.

4. Leitungsverantwortung, Haftung und Ersatz wirtschaftlicher Schäden

Informationssicherheit muss in jeder öffentlichen Stelle eine ausdrücklich zugewiesene Leitungs- und Organisationspflicht sein. Das BSI-Gesetz verpflichtet Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen zur Umsetzung und Überwachung von Risikomanagementmaßnahmen und regelt ihre Haftung; für Einrichtungen der Bundesverwaltung ist § 38 BSIG ausdrücklich ausgenommen. Die MIT fordert, diese Ungleichbehandlung aufzulösen und auch für die Leitung öffentlicher Stellen ein wirksames, rechtssicheres Verantwortungsregime zu schaffen.
Erhebliche Risiken und Prüfungsfeststellungen sind der Behördenleitung vorzulegen. Werden kritische Mängel trotz Warnung nicht behoben, müssen Entscheidung, Begründung, Frist und verantwortliche Person dokumentiert sein. Persönliche Folgen sollen an schuldhafte Organisations- oder Aufsichtsversäumnisse anknüpfen, insbesondere bei vorsätzlicher oder grob fahrlässiger Missachtung verbindlicher Mindestanforderungen; der Erfolg eines Cyberangriffs allein genügt dafür nicht. Die geltenden Amtshaftungs- und Rückgriffsregeln sind auf ihre Wirksamkeit zu prüfen und nötigenfalls zu konkretisieren.
Für Unternehmen muss außerdem klar sein, unter welchen Voraussetzungen die öffentliche Hand nach einem Datenabfluss für nachweisbare wirtschaftliche Schäden einsteht. Das betrifft etwa Kosten für Incident Response, den Austausch kompromittierter Zugangsdaten, Betriebsunterbrechungen und den Verlust von Geschäftsgeheimnissen. Gesetzgeberisch zu klären sind Schutzpflichten, Anspruchsgrundlagen, Kausalitäts- und Nachweisfragen sowie die Behandlung von Folgeschäden. Eine Übermittlungspflicht darf die betroffenen Unternehmen nicht schutzlos gegenüber vermeidbaren Sicherheitsversäumnissen des Empfängers stellen.

5. Kommunen finanziellen Spielraum für Cybersicherheit lassen

Gerade kleinere Gemeinden benötigen verbindliche Basissicherung und einfachen Zugang zu professionellen Sicherheitsleistungen. Es darf nicht von einer nebenamtlich betreuten IT abhängen, ob Updates zeitnah eingespielt, Backups getestet oder Sicherheitswarnungen bearbeitet werden. Regionale und landesweite Beschaffungsverbünde sollen Kommunen qualifizierte Angebote der IT-Sicherheitswirtschaft, insbesondere mittelständischer Anbieter, zugänglich machen; die Leitung vor Ort behält die Verantwortung für Auswahl, Beauftragung und Kontrolle.
Bund und Länder müssen die Umsetzung der vorgegebenen Standards einschließlich laufender Kosten für Personal, externe Sicherheitsdienste, Wartung und Übungen verlässlich finanzieren. Dafür brauchen Kommunen mehr finanziellen Spielraum. Priorität und Mittelbedarf sind in Haushalten transparent auszuweisen; Cybersicherheit ist als Pflichtaufgabe der Kommune zu

verstehen. Nicht sichtbare Sicherheitsinvestitionen dürfen nicht dauerhaft hinter kurzfristig leichter vermittelbaren Ausgaben zurückstehen.