

Handlungsbedarf bei IT-Sicherheit

[20.12.2022] Bei der IT-Sicherheit hinkt die öffentliche Verwaltung ihrem Anspruch hinterher. Zwar erkennen Bund, Länder und Kommunen die Wichtigkeit des Themas, den Maßnahmen fehlt es jedoch an Wirksamkeit. Dies ist das Kernergebnis des Branchenkompass Public Sector 2022 von Sopra Steria.

Für 97 Prozent der Behörden in Deutschland sind die Abwehr und der Umgang mit Cyber-Attacken sowie der Schutz von Daten die Top-Herausforderungen der kommenden Jahre. Bund, Länder und Kommunen wissen also um die Wichtigkeit des Themas IT-Sicherheit. Allerdings fehlt es bei der Umsetzung von Maßnahmen an Wirksamkeit und Stringenz, um eigene Anforderungen vollständig zu erfüllen. Das sind die Ergebnisse der Studie Branchenkompass Public Sector 2022, die das Meinungsforschungsinstitut Forsa im Auftrag der Management- und Technologieberatung Sopra Steria durchführte. Befragt wurden dazu 105 Entscheiderinnen und Entscheider aller Ebenen der öffentlichen Verwaltung, zudem enthält die Studie einige ausführliche Interviews mit Top-Entscheidern.

Zusammenarbeit muss sicherer werden

Nicht nur die Befragung untermauert den Handlungsbedarf bei der IT-Sicherheit. Sopra Steria verweist auch auf Analysen des Bundesrechnungshofs zum Geheimschutz in Bundesbehörden. Demnach werde unter anderem der Schutz in einigen Dienststellen mit besonders strengen Sicherheitsbestimmungen nicht häufig genug geprüft. Zudem sollen teilweise Sicherheitskonzepte fehlen, die für eine ressortübergreifende Kommunikation in Bundesnetzen Standard wären.

Künftig werde mehr Effizienz bei der Umsetzung von Digitalisierungs- und den damit eng verbundenen Sicherheitsstrategien gebraucht, sagt Ronald de Jonge, Operating Officer Public Sector bei Sopra Steria. Das betreffe die Prozesse und die Zusammenarbeit zwischen den Behörden, die innerbehördliche Zusammenarbeit der Mitarbeiter und natürlich auch die Interaktionen von Behörden mit der Wirtschaft.

Digitale Souveränität in Gefahr

Auch mit Blick auf eine souveräne öffentliche Verwaltung seien mehr Effizienz und hohe Sicherheitsstandards wichtige Schlüsselfaktoren, so Sopra Steria. 82 Prozent der Befragten sehen diese durch internationale Cyber-Angriffe in Gefahr. Vier von zehn Behörden haben dabei die zunehmende Kooperation und Vernetzung mit externen Partnern und IT-Dienstleistern im Blick. Insbesondere die Kommunen befürchten dadurch aber auch Einschränkungen ihrer Handlungsfähigkeit. „Mehr Kooperationen sind unerlässlich, um beim Aufbau einer digitalen Verwaltung schneller voranzukommen. Umso wichtiger ist es, die potenzielle Gefährdung für Datenschutz und IT-Sicherheit effizient zu managen“, sagt Ronald de Jonge von Sopra Steria.

Effizienzoffensive der Verwaltung geplant

Um Leistungen schneller und sicher digital anbieten zu können, planen die öffentlichen Verwaltungen eine Reihe strategischer, organisatorischer und technologischer Maßnahmen, so die Studie. Neun von zehn Befragten setzen demnach verstärkt auf Kooperationen mit anderen Behörden. Die Hälfte möchte mithilfe von Start-ups schneller bei Innovationsprojekten vorankommen. Fast ebenso viele (47 Prozent) investieren

in Technologien wie künstliche Intelligenz, etwa um Vorgänge zu automatisieren und so das Tempo zu steigern und die Fehleranfälligkeit zu senken.

Von den geplanten Maßnahmen könne auch die Baustelle IT-Sicherheit profitieren, prognostiziert de Jonge: Wenn Verwaltungen die IT-Sicherheit bei jeder neu digitalisierten Behördenleistung mitdenken, sparten sie Entwicklungszeit und minimierten Risiken. Zudem könnten Behörden durch mehr Kooperation von erprobten und bewährten Sicherheitskonzepten anderer profitieren und Best Practices übernehmen. Notwendig sei hierfür auch ein verstärktes Bemühen um interoperable Standards. Dadurch erhöhe sich die Resilienz des Gesamtsystems, die so zur digitalen Souveränität auf allen Verwaltungsebenen beitrage, resümiert de Jonge.

(sib)

Branchenkompass Public Sector 2022 interaktiv

Stichwörter: IT-Sicherheit, Branchenkompass Public Sector 2022, Sopra Steria Consulting, Studie