



Schule im ISMS der Kommune – ein gut gemeinter, aber folgenreicher Irrtum Management-Zusammenfassung

Bayerische Kommunen sind als Sachaufwandsträger für die technische Infrastruktur ihrer Schulen verantwortlich – und erbringen in vielen Fällen darüber hinaus IT-Dienstleistungen für den laufenden Betrieb. Das ist sinnvoll und legitim. Es führt jedoch immer wieder zu einem folgenreichen Missverständnis: der Annahme, die Schule gehöre damit zum Geltungsbereich des kommunalen ISMS.

Das ist falsch – aus drei Gründen:

Rechtlich ist die Schule eine staatliche Einrichtung. Personal, Dienstaufsicht und organisatorische Verantwortung liegen beim Freistaat Bayern, nicht bei der Kommune. Die Finanzierungsverantwortung des Sachaufwandsträgers begründet keine Leitungs- oder Weisungsbefugnis. Art. 43 BayDiG verpflichtet die Kommune, die eigene Organisation abzusichern – nicht fremde Institutionen.

Methodisch setzt ein ISMS voraus, dass die verantwortliche Stelle ihren Geltungsbereich tatsächlich steuern kann. IT-Grundschutz, ISO 27001 und die Arbeitshilfe folgen dabei derselben Logik: Scope follows Control. Informationssicherheit umfasst nicht nur Technik, sondern ausdrücklich auch Organisation und Personal. Genau hier hat die Kommune in der Schule keinerlei Handhabe. Sie kann dem Schulpersonal keine Richtlinien vorgeben, keine Schulungen anordnen, keine Verhaltensregeln verbindlich einführen. Technik allein – Firewall, Virenschanner, Netzwerksegmentierung – ersetzt keine Sicherheitskultur. Und Sicherheitskultur entsteht nur dort, wo jemand das Recht hat, sie einzufordern.

Haftungsrelevant wird der Irrtum spätestens im Schadensfall. Wer im ISMS erklärt, einen Bereich zu verantworten, den er faktisch nicht steuert, muss im Ernstfall erklären, warum Maßnahmen nicht umgesetzt wurden – obwohl er doch angeblich verantwortlich war.

Die Lösung

Die Kommune kann Sachaufwandsträger und IT-Dienstleister für die Schule sein. Beide Rollen sind vereinbar – aber nur, wenn sie sauber voneinander getrennt werden. Das bedeutet: technische Trennung der Schulinfrastruktur von der kommunalen Infrastruktur, und eine belastbare vertragliche Grundlage für die IT-Dienstleistungsbeziehung, einschließlich klarer Verantwortungsabgrenzung und – wo personenbezogene Daten verarbeitet werden – eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO.

Die Schule erscheint im kommunalen ISMS dann dort, wo sie hingehört: als externe Partei an einer definierten Schnittstelle. Nicht als Teil der eigenen Organisation.

Der Geltungsbereich des kommunalen ISMS endet dort, wo die kommunale Steuerungsmöglichkeit endet. Spätestens an der Schultür.