Schule im ISMS der Kommune

– ein gut gemeinter, aber folgenreicher Irrtum

Ausgangslage: Wenn die Kasse klingelt, aber das Hausrecht fehlt

Bayerische Kommunen kennen das Spielfeld gut. Auf der einen Seite das BayDiG, konkret Art. 43, der ihnen seit seinem Inkrafttreten unmissverständlich sagt: Informationssicherheitskonzept her, und zwar eines, das funktioniert. Auf der anderen Seite die örtliche Schule, für deren technische Infrastruktur die Kommune als Sachaufwandsträger zahlt. Manchmal sogar wartet, betreibt und administriert. Mit eigenem IT-Personal, eigenem Equipment, und – das ist der Punkt, an dem es interessant wird – ohne auch nur einen Hauch von Weisungsrecht gegenüber dem Lehrpersonal oder der Schulleitung.

Was liegt also näher, als die Schule einfach in den Geltungsbereich des kommunalen ISMS aufzunehmen? Man ist ja sowieso drin, technisch gesehen. Man kennt die Server. Man kennt die Switches. Man hat den Schlüssel zum Serverraum. Gefühlt ist das doch alles eine Einheit.

Gefühlt. Genau da liegt das Problem.

Dieses Papier nimmt sich der Frage an, warum dieser Reflex – so verständlich er ist – in die falsche Richtung führt. Und zwar nicht nur aus einem vagen Unbehagen heraus, sondern aus drei sehr konkreten Gründen: dem Recht, der ISMS-Methodik, und der schlichten Unmöglichkeit, etwas zu steuern, das sich der eigenen Steuerung grundsätzlich entzieht.

Am Ende steht keine Bankrotterklärung, sondern ein Modell, das funktioniert. Aber der Reihe nach.

Teil 1: Die rechtliche Einordnung – wer zahlt, hat nicht das Sagen

Sachaufwandsträger ist kein Synonym für Verantwortungsträger

Im bayerischen Schulrecht ist die Aufgabenverteilung zwischen Staat und Kommune seit Jahrzehnten klar geregelt, auch wenn sie im Alltag gerne durcheinandergerät. Der Freistaat Bayern trägt den sogenannten Personalaufwand: Lehrerinnen und Lehrer sind Staatsbeamte, das Schulamt ist zuständig, die Dienstaufsicht liegt beim Kultusministerium. Die Kommune hingegen trägt den Sachaufwand. Das bedeutet: Gebäude, Mobiliar, Heizung, und eben auch – zunehmend – die technische Infrastruktur. Breitband, Endgeräte, LAN, Server.

Wer jetzt denkt, wer zahlt, schafft an – der liegt im Schulrecht strukturell falsch. Die Finanzierungsverantwortung begründet keine Leitungs- oder Weisungsbefugnis. Die Schule ist und bleibt eine staatliche Einrichtung. Der Schulleiter untersteht nicht dem Bürgermeister oder dem Landrat. Die Lehrkräfte sind nicht bei der Kommune angestellt. Und

die pädagogische wie organisatorische Verantwortung für den Schulbetrieb liegt eindeutig beim Freistaat, nicht bei der Gemeinde.

Das klingt nach Verwaltungsrecht aus dem ersten Semester, ist in der Praxis aber erstaunlich oft vergessen – besonders dann, wenn die Kommune faktisch tief in der IT der Schule steckt.

Was das BayDiG wirklich sagt

Art. 43 BayDiG verpflichtet bayerische öffentliche Stellen zur Einführung von Informationssicherheitskonzepten. Die Kommune ist öffentliche Stelle. Die Schule – als staatliche Einrichtung – ist es auch, aber eben eine andere. Zwei Rechtspersönlichkeiten, zwei Verantwortungsbereiche, zwei potenzielle Verpflichtungsadressaten.

Das BayDiG begründet keine gemeinsame Verantwortungsstruktur allein deshalb, weil zwei Stellen technisch miteinander verzahnt sind. Es folgt dem klassischen Prinzip: Pflicht liegt dort, wo Verantwortung liegt. Und die Verantwortung für die Institution Schule liegt nicht bei der Kommune.

Eine Kommune, die die Schule in ihr ISMS aufnimmt mit dem Argument, das BayDiG verlange es oder erlaube es zumindest, argumentiert am Gesetz vorbei. Das BayDiG verlangt von der Kommune, die eigene Organisation abzusichern – nicht fremde Organisationen.

Der Datenschutz zeigt, wie es geht

Ein hilfreicher Blick über den Zaun lohnt sich hier: das Datenschutzrecht. Die DSGVO kennt das Konzept der Verantwortlichkeit sehr präzise. Verantwortlicher ist, wer über Zwecke und Mittel der Verarbeitung entscheidet. Dieses Konzept ist auf die Informationssicherheit übertragbar, und es ist kein Zufall, dass es dort strukturell genauso funktioniert.

Die Schule entscheidet, welche Daten sie verarbeitet, welche Systeme sie nutzt, welche Anwendungen sie einsetzt. Die Kommune stellt dafür unter Umständen die Infrastruktur bereit – aber sie entscheidet nicht über Zwecke und Betrieb. Wer datenschutzrechtlich Verantwortlicher ist, trägt auch die ISMS-Verantwortung. Und das ist in der Schule der Freistaat, vertreten durch die Schulleitung und die nachgeordneten Behörden.

Oder anders gesagt: Was im DSMS (Datenschutzmanagementsystem) als Auftragsverarbeitung einzustufen wäre, kann im ISMS nicht plötzlich zur eigenen Verantwortungsträgerschaft werden. Die Logik ist dieselbe, nur das Kürzel ändert sich.

Und die Aufsicht?

Ein letztes Indiz, das in der Diskussion selten genannt wird, aber eigentlich alles sagt: Wer übt die Aufsicht über die Schule aus? Das Schulamt. Das Kultusministerium. Nicht der Landrat, nicht der Bürgermeister. Aufsichtsstrukturen folgen Verantwortungsstrukturen. Und dort, wo die Aufsicht nicht bei der Kommune liegt, liegt die Verantwortungsträgerschaft auch nicht bei der Kommune.

Das ist kein Trick und kein Schlupfloch. Es ist die konsequente Anwendung dessen, was Rechtsordnung und Verwaltungsorganisation seit jeher regeln – nur halt auf ein Thema, das es vor zwanzig Jahren in dieser Form noch nicht gab.

Teil 2: Die ISMS-Methodik – oder warum ein Geltungsbereich ohne Steuerung kein Geltungsbereich ist

Scope follows Control – nicht follows Budget

Wer ein ISMS einführt, egal ob nach IT-Grundschutz, ISO 27001 oder der Arbeitshilfe für Kleinorganisationen, steht ganz am Anfang vor einer zentralen Frage: Was gehört dazu? Die Antwort auf diese Frage ist der Geltungsbereich, im Englischen schlicht der Scope. Und dieser Geltungsbereich folgt einer eisernen Logik, die alle drei Normen teilen, auch wenn sie es unterschiedlich formulieren.

Der Geltungsbereich umfasst das, was die Organisation tatsächlich steuern kann. Nicht das, was sie finanziert. Nicht das, was sie technisch berührt. Sondern das, worüber sie Kontrolle hat – organisatorisch, fachlich, personell.

Das BSI formuliert es im IT-Grundschutz-Kompendium grob so: Der Informationsverbund umfasst die Teile einer Organisation, die gemeinsam betrachtet und abgesichert werden sollen. Entscheidend ist dabei, dass Maßnahmen auch tatsächlich umgesetzt und kontrolliert werden können. Eine Organisation kann keinen sinnvollen Informationsverbund definieren, der Bereiche einschließt, auf die sie keinen Einfluss hat. Das wäre so, als würde man den Brandschutzplan für ein Gebäude erstellen, das einem jemand anderem gehört – und zu dem man nur den Schlüssel zum Heizungskeller hat.

Informationssicherheit ist mehr als IT-Sicherheit

Hier liegt ein Denkfehler, der in der kommunalen Praxis erstaunlich verbreitet ist – und der direkt aus der Sachaufwandsträger-Rolle erwächst. Weil die Kommune die Technik stellt, konzentriert sich ihr Blick auf die Technik. Firewall läuft, Virenscanner ist aktuell, das LAN ist (hoffentlich) segmentiert. Fertig, oder?

Nein. Denn Informationssicherheit ist nicht dasselbe wie IT-Sicherheit. IT-Sicherheit ist eine Untermenge. Eine wichtige, keine Frage. Aber eben nur ein Teil des Ganzen.

Ein ISMS im Sinne des IT-Grundschutz oder der ISO 27001 umfasst ausdrücklich auch die organisatorische und die personelle Dimension. Es geht um Richtlinien, die jemand einhalten muss. Um Prozesse, die jemand leben muss. Um Sensibilisierung, die bei jemandem ankommen muss. Und genau hier wird es für die Kommune in der Schule strukturell unmöglich.

Der Mensch klickt – und die Kommune schaut zu

Nehmen wir das Szenario, das in der Realität für die meisten Sicherheitsvorfälle verantwortlich ist: der Mensch. Eine Lehrkraft öffnet einen Mailanhang, den sie nicht hätte öffnen sollen. Ein Kollege startet ein Office-Makro, weil das Dokument freundlich darum gebeten hat. Jemand nutzt ein privates Gerät für dienstliche Zwecke, weil es gerade praktisch ist. Nicht zu vergessen: Schatten-IT und immer aktueller Schatten-KI.

Das sind keine Ausnahmen. Das ist der Normalzustand in jeder Organisation, die keine konsequente Sicherheitskultur etabliert hat. Und eine Sicherheitskultur entsteht nicht durch Technik. Sie entsteht durch Schulungen, durch klare Verhaltensregeln, durch Richtlinien, durch Vorleben – und durch die Möglichkeit, Konsequenzen zu ziehen, wenn jemand diese Regeln ignoriert.

Die Kommune hat gegenüber dem Personal in der Schule keines dieser Instrumente. Sie kann keine Pflichtschulungen anordnen. Sie kann keine Nutzungsrichtlinien verbindlich einführen. Sie kann niemanden ermahnen, wenn Regeln nicht eingehalten werden. Das Personal ist nicht bei ihr angestellt, unterliegt nicht ihrer Dienstaufsicht, und hat ihr gegenüber – rechtlich betrachtet – keine Rechenschaftspflicht in Sicherheitsfragen.

Was bleibt, ist die Technik. Und die Technik kann vieles abfedern, aber sie ist kein Ersatz für eine funktionierende Sicherheitsorganisation. Wer glaubt, mit einer gut konfigurierten Firewall und einem Virenscanner (die sind ja mittlerweile auch voller KI, die angeblich Wunder vollbringen kann) die menschliche Komponente kompensieren zu können, darf sich beim nächsten Ransomware-Vorfall nicht wundern.

Was der BSI IT-Grundschutz konkret voraussetzt

Im Kommunalprofil, das für bayerische Kommunen der de-facto-Standard ist, wird die etwas abgespeckte Basis-Absicherung als pragmatischer Einstieg beschrieben. Auch hier gilt: Die Maßnahmen aus den Bausteinen des IT-Grundschutz-Kompendiums setzen voraus, dass die verantwortliche Stelle sie anordnen, umsetzen und deren Einhaltung überprüfen kann.

Nehmen wir den Baustein ORP.3 – Sensibilisierung und Schulung. Die Kommune soll sicherstellen, dass alle Personen im Geltungsbereich angemessen zur Informationssicherheit sensibilisiert werden. Klingt vernünftig. Aber wie macht sie das mit Lehrkräften, die nicht bei ihr angestellt sind, die ihrer Weisung nicht unterliegen, und die – das sei ohne Wertung gesagt – erfahrungsgemäß wenig Begeisterung entwickeln, wenn die Gemeindeverwaltung ihnen erklärt, wie sie mit IT umzugehen haben?

Oder ORP.2 – Personal. Sicherheitsrelevante Aufgaben und Verantwortlichkeiten müssen geregelt sein, Mitarbeitende müssen in ihre Pflichten eingewiesen werden. Wessen Mitarbeitende? Die der Schule. Und die Schule ist eben kein Teil der kommunalen Organisation.

Das sind keine Randszenarien. Das ist strukturelle Unmöglichkeit.

Die ISO 27001 sagt dasselbe, nur auf Englisch

Wer mit ISO 27001 arbeitet, kennt Clause 4.3 – die Festlegung des Scope. Dort wird explizit gefordert, dass Schnittstellen und Abhängigkeiten zu anderen Organisationen berücksichtigt werden. Andere Organisation. Nicht eine Abteilung, nicht ein Standort – eine andere Organisation. Genau das ist die Schule. Sie ist eine eigenständige Institution mit eigener Leitung, eigenem Personal, eigenen Entscheidungsstrukturen.

ISO 27001 kennt kein Konzept, das es erlaubt, eine fremde Organisation einfach in den eigenen Scope zu ziehen. Was es gibt, ist die Möglichkeit, Lieferanten und Dienstleister zu betrachten – aber eben als externe Parteien, nicht als Teil der eigenen Organisation. Genau diese Einordnung ist die richtige, und dazu kommen wir in Teil 3.

Das eigentliche Risiko: Scheinabsicherung mit echter Haftung

Wenn eine Kommune die Schule in ihren ISMS-Scope aufnimmt, erklärt sie damit gegenüber der Aufsichtsbehörde, dem Gemeinderat, und im Zweifel auch vor Gericht, dass sie die Informationssicherheit in diesem Bereich verantwortet und steuert. Sie tut das aber faktisch nicht – weil sie es, wie gezeigt, strukturell gar nicht kann.

Im Schadensfall liegt genau dieses Dokument auf dem Tisch. Und die Frage lautet dann nicht: Habt ihr die Schule versucht abzusichern? Die Frage lautet: Ihr habt erklärt, ihr seid verantwortlich – warum hat dann niemand das Personal geschult? Warum gab es keine verbindliche Nutzungsrichtlinie? Warum wurde der Sicherheitsvorfall nicht nach den eigenen Prozessen behandelt?

Eine Scheinabsicherung, die auf dem Papier vollständig aussieht, schafft echte Haftungsrisiken. Für die Kommune, für den Bürgermeister oder Landrat als Behördenleiter, und für den Informationssicherheitsbeauftragten, der das Konzept verantwortet.

Gut gemeint ist hier nicht gut gemacht. Es ist schlicht gefährlich.

Teil 3: Was stattdessen funktioniert – Trennung, Klarheit, und ein sauberes Dienstleistermodell

Trennung ist keine Kapitulation

Wer an diesem Punkt angelangt ist, könnte den Eindruck gewinnen, die Botschaft laute: Kommunen sollen die Finger von der Schulinfrastruktur lassen. Das ist ausdrücklich nicht gemeint. Die Botschaft lautet: Kommunen sollen klar zwischen zwei Rollen unterscheiden, die sie gleichzeitig innehaben können – aber eben nicht vermischen dürfen.

Rolle eins ist die des Sachaufwandsträgers. Die ist gesetzt, gesetzlich geregelt, und lässt sich nicht wegdiskutieren.

Rolle zwei ist die des IT-Dienstleisters. Diese Rolle ist freiwillig, praktisch sinnvoll, und grundsätzlich unproblematisch. Wenn sie als das behandelt wird, was sie ist: eine Dienstleistungsbeziehung zwischen zwei eigenständigen Institutionen.

Beide Rollen unter einem Dach sind möglich. Aber sie brauchen getrennte Strukturen, klare Verträge, und vor allem ein gemeinsames Verständnis davon, wer hier was entscheidet.

Technische Trennung als Fundament

Der erste und wichtigste Schritt ist die konsequente technische Trennung der Schulinfrastruktur von der kommunalen Infrastruktur. Getrennte Netze, getrennte Systeme, klare Übergabepunkte. Was technisch voneinander getrennt ist, muss nicht gemeinsam bewertet werden. Was nicht im kommunalen Netz hängt, gehört nicht in den kommunalen Informationsverbund. Und kann dort auch keinen Schaden für die Kommune verursachen. Das ist anstrengend, da im Zweifel die Schule von Anfang in die kommunalen Systeme integriert war und mitgewachsen ist. Ein Grund mehr, nun die Trennung konsequent anzugehen.

Das klingt nach Aufwand, und das ist es auch. Aber es ist ein einmaliger Aufwand, der dauerhaft Klarheit schafft. Die Alternative – alles in einem Topf, dafür aber konzeptionell unlösbar – ist der teurere Weg. Spätestens dann, wenn der erste ernsthafte Sicherheitsvorfall einschlägt und die Frage kommt, wer eigentlich wofür verantwortlich war.

Das Dienstleistermodell – und was dafür geregelt sein muss

Wenn die Kommune IT-Leistungen für die Schule erbringt, ist das eine Auftragsbeziehung. Die Schule ist Auftraggeber, die Kommune ist Auftragnehmer. Das muss dokumentiert sein, und zwar nicht in einem formlosen Beschluss aus der Gemeinderatssitzung von 2019, sondern in einer belastbaren vertraglichen Grundlage.

Was gehört hinein?

Erstens der Leistungsumfang. Was macht die Kommune konkret? Betrieb der Server, Netzwerkpflege, Helpdesk, Softwareverteilung – das muss klar definiert sein. Was nicht im Vertrag steht, ist keine Verpflichtung der Kommune und kann dann auch keine Erwartung der Schule sein.

Zweitens die Verantwortungsabgrenzung. Die Kommune verantwortet in der Rolle als Dienstleister die von ihr betriebenen technischen Systeme. Die Schule verantwortet alles andere – die Organisation, das Personal, die Prozesse, die Nutzung. Diese Abgrenzung ist nicht nur für das ISMS wichtig, sie ist auch datenschutzrechtlich relevant. Wer personenbezogene Daten im Auftrag verarbeitet, braucht einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Wer das noch nicht hat, sollte das nachholen – am besten gleichzeitig mit der Strukturbereinigung.

Drittens die Eskalations- und Entscheidungswege. Was passiert, wenn die Kommune aus Sicherheitsgründen eine Maßnahme für notwendig hält, die Schule aber nicht will? Wer

entscheidet? In welchem Zeitrahmen? Diese Frage klingt hypothetisch, bis sie es nicht mehr ist. Oder die Schule als Auftraggeber möchte etwas und die kommunale IT will das eher nicht. Dann ist es gut, wenn die Antwort bereits schriftlich existiert.

Was im kommunalen ISMS dann tatsächlich auftaucht

Nach der Trennung sieht das kommunale ISMS die Schule nur noch in einer einzigen Perspektive: als externen Dienstleistungsempfänger, für den die Kommune bestimmte technische Services erbringt. Diese Schnittstelle muss im ISMS adressiert werden – aber eben als Schnittstelle, nicht als Geltungsbereich.

Das ist methodisch sauber, revisionskonform, und vor allem ehrlich. Es beschreibt die Realität, wie sie ist, nicht wie man sie sich wünscht.

Und für die Schule? Für die Schule entsteht damit klarer Handlungsbedarf auf der richtigen Ebene. Sie braucht entweder ein eigenes Informationssicherheitskonzept – was die zuständigen staatlichen Stellen eigentlich längst auf den Weg bringen müssten – oder zumindest eine klare Regelung innerhalb der staatlichen Zuständigkeitskette. Das ist eventuell unbequem, weil es bedeutet, dass eine Lücke sichtbar wird, die bisher durch gut gemeinte aber falsch verstandene kommunale Initiative verdeckt wurde.

Diese Lücke zu benennen ist kein Angriff auf die Schule. Es ist ein Dienst an der Realität.

Kurz zusammengefasst: Zwei Rollen, eine klare Linie

Die Kommune kann Sachaufwandsträger und IT-Dienstleister für die Schule sein. Sie kann beide Rollen gut ausfüllen. Was sie nicht kann – und was sie rechtlich, methodisch und praktisch nicht darf – ist, die Schule als Teil ihrer eigenen Organisation zu behandeln und deren Informationssicherheit als ihre eigene Verantwortung zu deklarieren.

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