Sicherheitsbewusster Umgang mit Projektinformationen

Ein Leitfaden in fünf Schritten. Für Bauherren, Planungsbüros und Betreiber, die mit sensiblen Informationen arbeiten und nicht wissen, wo sie anfangen sollen.

Diese Anleitung gehört zum Vorlagenpaket ISO 19650-5. Sie gibt keinen Normtext wieder und ersetzt die Norm nicht.

Stand September 2026

Wofür das hier gut ist

ISO 19650-5 ist der Teil der Normenreihe, der von keinem einzigen Modell handelt. Er handelt davon, wer welche Information bekommt, unter welchen Bedingungen, und was vorher geprüft wird. Genau deshalb wird er übersehen: Es gibt keine Software dafür, keine Zertifizierung, kein Werkzeug, das sich verkaufen ließe.

Was es gibt, ist ein Verfahren. Es besteht aus einer Prüfung, ein paar Dokumenten und einer Gewohnheit. Diese Anleitung führt Sie in fünf Schritten hindurch und sagt Ihnen bei jedem, welches Dokument aus dem Paket dazugehört, wie lange es ungefähr dauert und woran es in der Praxis scheitert.

Die Reihenfolge ist nicht beliebig. Schritt eins entscheidet, ob die anderen vier überhaupt nötig sind, und ohne die Aufzeichnung aus Schritt eins hängt alles Weitere in der Luft.

Für wen die Norm gilt

Nicht nur für Betreiber. Der Ansatz gilt für jede Organisation, die Zugang zu sensibler Information hat, über die ganze Kette und über alle Beauftragungsebenen hinweg. Das ist der wesentliche Unterschied zu einem Informationssicherheitsmanagement nach ISO 27001, das eine einzelne Organisation absichert. Ein Bauprojekt ist keine Organisation. Es ist eine Kette, deren Besetzung sich über Jahre ändert und in der jeder Beteiligte seine eigene IT mitbringt.

Die geltenden Resilienzgesetze in Deutschland und Österreich richten sich an Betreiber kritischer Einrichtungen. Das Planungsbüro, auf dessen Rechner das Modell der Anlage liegt, kommt darin nicht vor. Die Information liegt trotzdem dort.

> **Verhältnismäßig heißt verhältnismäßig.** Die Norm verlangt ausdrücklich keinen Apparat, der zum Vorhaben nicht passt. Für ein kleines Büro mit einem sensiblen Projekt sind ein aufgezeichnetes Prüfergebnis, ein benannter Verantwortlicher, eine knappe Strategie und eine gelebte Weitergabeprüfung deutlich mehr wert als hundert Seiten, die niemand liest.

Schritt 1: Prüfen, ob es Sie betrifft

Dokument 01, Sensitivitätsprüfung und Triage. Aufwand: eine Sitzung, etwa zwei Stunden mit den richtigen Leuten am Tisch.

Die Prüfung stellt zwei Fragen. Erstens: Ist das eigene Vorhaben sensibel? Zweitens: Liegt sensible Information anderer Organisationen im Zugriff? Aus den Antworten ergeben sich vier mögliche Ergebnisse.

Ergebnis	Eigenes Vorhaben	Fremde Information	Was folgt
ST1	sensibel	sensibel im Zugriff	Voller Ansatz für beides, getrennt dokumentiert
ST2	sensibel	nein	Voller Ansatz für die eigene Information
ST3	nicht sensibel	sensibel im Zugriff	Voller Ansatz für die fremde Information
ST4	nicht sensibel	nein	Grundschutz für Geschäfts- und Personendaten

Wann ein Bauwerk als sensibel gilt

Die Norm nennt dafür Merkmale. Trifft eines zu, ist die Frage entschieden, ohne dass man diskutieren müsste: kritische Infrastruktur, also Energie, Wasser, Verkehr, Telekommunikation, Gesundheit oder Entsorgung. Anlagen mit Verteidigungs-, Strafverfolgungs-, Sicherheits- oder diplomatischer Funktion. Standorte mit wertvollen oder gefährlichen Stoffen. Wahrzeichen und Orte, an denen viele Menschen zusammenkommen.

Darüber hinaus gilt ein Vorhaben auch dann als sensibel, wenn eine Kompromittierung seiner Informationen Integrität, Betrieb, Sicherheit oder Widerstandsfähigkeit erheblich gefährden könnte, oder wenn personenbezogene Daten anfallen, deren Offenlegung Menschen gefährdet. Teilweise Betroffenheit genügt. Ein gewöhnliches Bürogebäude mit einem Rechenzentrum im Keller ist in diesem Teil sensibel.

Die zweite Frage, die alle übersehen

Sie müssen auch dann handeln, wenn Ihr eigenes Projekt völlig harmlos ist, Sie aber nicht öffentlich verfügbare Unterlagen anderer besitzen. Leitungsbestände, Netzunterlagen, Untergrundvermessungen, Betreiberdaten. Ob diese Unterlagen sensibel sind, entscheiden Sie nicht selbst, das klären Sie mit dem Eigentümer. Solange das nicht geklärt ist, behandeln Sie sie als sensibel.

> **Das Ergebnis wird aufgezeichnet.** Jedes Mal, auch wenn nichts herauskommt. Das Nullergebnis ist der Nachweis, dass geprüft wurde, und in zwei Jahren fragt jemand danach. Die Aufzeichnung selbst kann sensibel sein und gehört entsprechend abgelegt.