IT-Sicherheit und Basis-Absicherung für Geobasisdaten

Handlungsempfehlungen für Vermessung & Kataster

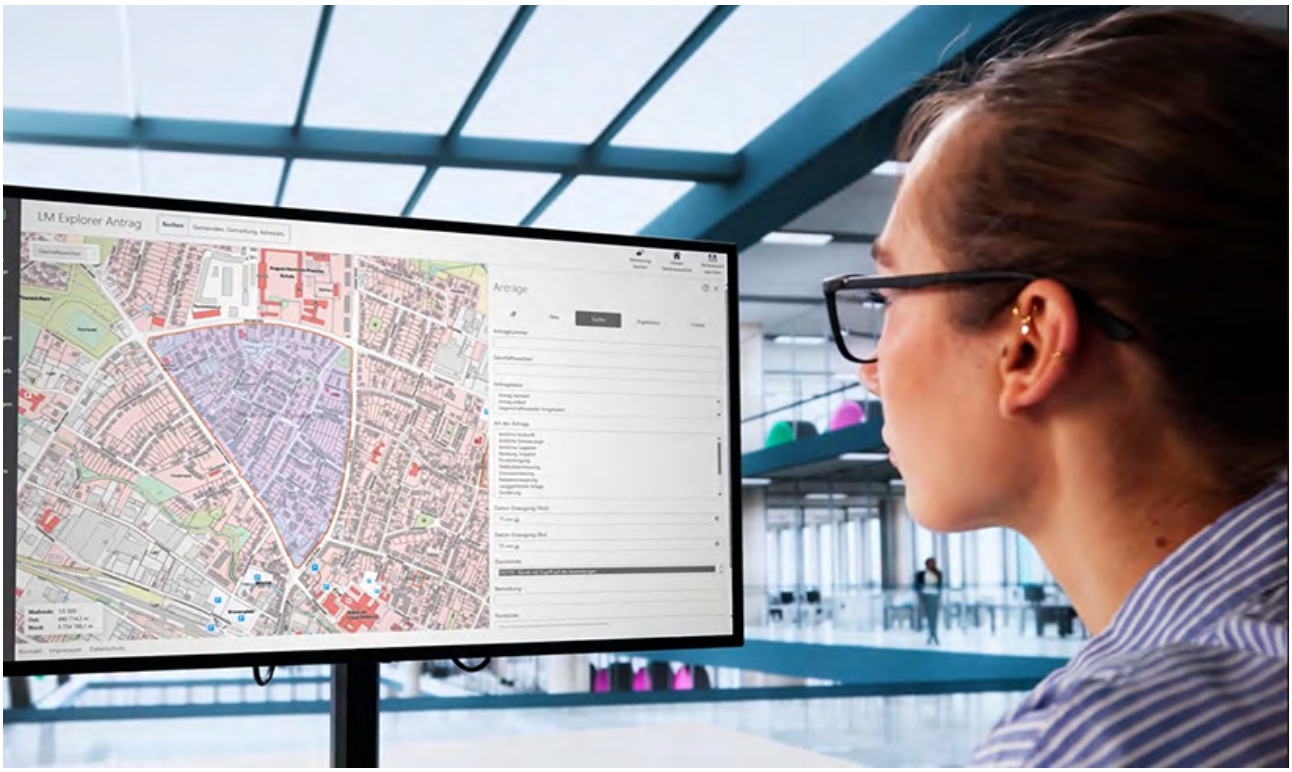
VertiGIS™

VertiGIS™

Die fortschreitende Digitalisierung stellt Vermessungs- und Katasterverwaltungen vor erhebliche organisatorische und technische Herausforderungen. Geobasisdaten sind als Bestandteil der kritischen Infrastruktur von zentraler Bedeutung – ihre Integrität, Verfügbarkeit und Sicherheit sind zentrale Voraussetzungen für eine funktionierende Verwaltung, eine moderne Daseinsvorsorge und nicht zuletzt für ein aktuelles und rechtssicheres Liegenschaftskataster. Katasterbehörden tragen hierbei eine besondere Verantwortung, da sie jederzeit die Vollständigkeit, Richtigkeit, Nachvollziehbarkeit und den Schutz der Daten gewährleisten müssen.

Parallel dazu steigen die Anforderungen an IT-gestützte Fachverfahren kontinuierlich. Die zunehmende Digitalisierung von Verwaltungsprozessen, die wachsende Zahl technischer Schnittstellen sowie die Vernetzung mit kommunalen, Landes- und Bundesbehörden führen einerseits zu Effizienzgewinnen und höherem Automatisierungsgrad, erhöhen jedoch andererseits die Komplexität der Systemlandschaften und das sicherheitsrelevante Risikopotenzial. Insbesondere auf kommunaler Ebene zeigen wiederkehrende Cyberangriffe die Verwundbarkeit bestehender Strukturen und führen zu Ausfällen, Betriebsunterbrechungen und erheblichen Wiederherstellungsaufwänden.

Vor diesem Hintergrund gewinnt Informationssicherheit eine zentrale Bedeutung. Sie ist nicht nur eine technische Notwendigkeit, sondern die Grundvoraussetzung für verlässliches Verwaltungshandeln, rechtssichere Datenhaltung und die nachhaltige Modernisierung des Liegenschaftskatasters. Cloud-Plattformen können hierzu einen wesentlichen Beitrag leisten, indem sie standardisierte und geprüfte Sicherheitsarchitekturen, resilientere Betriebsmodelle sowie geeignete Rahmenbedingungen für digitale Souveränität bereitstellen.



1. Digitalisierung und kritische Infrastrukturen

Geobasisdaten und die damit eng verknüpften Fachdaten der Vermessungs- und Katasterverwaltungen sind von zentraler Bedeutung für Verwaltung, Wirtschaft und öffentliche Sicherheit. Sie bilden die Grundlage zahlreicher Prozesse – von Bauanträgen und Planungsverfahren über Infrastruktur- und Versorgungsprojekte bis hin zu Notfall- und Katastrophenschutz. Ein Ausfall dieser Daten oder der zugehörigen Fachverfahren hätte unmittelbare und weitreichende Folgen: Verwaltungsabläufe würden ins Stocken geraten, wirtschaftliche Aktivitäten behindert und sicherheitskritische Einsatzprozesse erheblich beeinträchtigt.

Mit der wachsenden Abhängigkeit steigt zugleich die Komplexität der Anforderungen: Daten müssen jederzeit verfügbar, korrekt, manipulationssicher und belastbar gegen externe Angriffe sein. Diese Anforderungen lassen sich nur mit einem ganzheitlichen, professionell betriebenen Sicherheitskonzept erfüllen, das technologische, organisatorische und prozessuale Aspekte integriert.

Die Konsequenz ist klar: Ohne Informationssicherheit gibt es keine funktionierende gesellschaftliche Daseinsvorsorge. Sie bildet das Fundament, auf dem moderne Verwaltungsprozesse, rechtssichere Entscheidungen und die Zuverlässigkeit des Liegenschaftskatasters aufbauen.

2. Regulatorische Anforderungen

Im Hinblick auf die steigenden regulatorischen Anforderungen durch die NIS-2-Richtlinie, das KRITIS-Dachgesetz und den BSI-Grundschutz sind die Vermessungs- und Katasterverwaltungen zum Handeln aufgefordert.

Die NIS-2-Richtlinie der EU, die am 06.12.2025 in Kraft getreten und damit in nationales Recht umgesetzt wird, weitet die Anforderungen an Cybersicherheit auf zahlreiche Sektoren der öffentlichen Verwaltung aus – darunter auch die Betreiber von Geobasisdaten und ALKIS-Systemen. Zu den zentralen Pflichten zählen:

- Einführung eines Risikomanagements für Netz- und Informationssysteme, das technische und organisatorische Maßnahmen umfasst (z. B. Zugriffskontrolle, Verschlüsselung, Notfallmanagement)
- Meldepflichten: Sicherheitsvorfälle müssen innerhalb von 24 Stunden an die zuständige Behörde gemeldet werden.
- Verantwortung der Behördenleitung: Die Leitung der Behörde ist verpflichtet, sich regelmäßig über Cybersicherheitsrisiken zu informieren und entsprechende Schulungen zu absolvieren.
- Sicherheitsstrategien und Nachweispflichten: Es müssen strukturierte Sicherheitskonzepte vorliegen und deren Umsetzung dokumentiert werden.

Gerade für die Vermessungs- und Katasterverwaltung bedeutet dies, dass alle IT-Systeme, die Geobasisdaten verarbeiten oder bereitstellen, dem Stand der Technik entsprechend abgesichert und kontinuierlich überwacht werden müssen. Die NIS-2-Richtlinie macht Cybersicherheit zur Chefsache und verlangt eine enge Verzahnung von IT und Fachverwaltung.

Das KRITIS-DachG (BSI-KritisV, §8a BSIG) konkretisiert die Anforderungen für Betreiber kritischer Infrastrukturen. Auch wenn Katasterämter nicht immer automatisch unter die KRITIS-Verordnung fallen, prüfen viele Bundesländer dessen Relevanz für Geobasisdaten.

Grundsätzlich gilt:

- Einführung und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) nach BSI-Grundschutz.
- Nachweise zur IT-Sicherheit und regelmäßige Prüfungen durch unabhängige Stellen.
- Meldepflichten bei Sicherheitsvorfällen und Einrichtung einer 24/7-Kontaktstelle.
- Erstellung eines Resilienzplans mit Risikoanalyse, Bewertung und Umsetzung technischer und organisatorischer Maßnahmen, um im Störungsfall handlungsfähig zu bleiben.

Für die Vermessungs- und Katasterverwaltung bedeutet dies, dass insbesondere der Schutz sensibler Geodaten, die Sicherstellung der Verfügbarkeit und die Nachvollziehbarkeit aller Zugriffe und Änderungen gewährleistet sein müssen.

Der BSI-Grundschutz bildet die Basis für ein umfassendes Sicherheitskonzept in der öffentlichen Verwaltung. Er fordert eine umfassende Risikoanalyse und Ableitung angemessener Schutzmaßnahmen. Hierzu zählen u.a.:

- Technische Maßnahmen wie Verschlüsselung, Zugriffskontrolle, Protokollierung und regelmäßige Sicherheitsaudits.
- Organisatorische Maßnahmen wie Sensibilisierung und Schulung des Personals, klare Verantwortlichkeiten und Notfallmanagement.
- Sichere Cloud-Nutzung: Bei Auslagerung in Cloud-Umgebungen müssen die Anforderungen an Datenschutz, Integrität und Verfügbarkeit auch beim Dienstleister nachweislich erfüllt werden.

Gerade für die Vermessungs- und Katasterverwaltung ist die konsequente Umsetzung des BSI-Grundschutzes von zentraler Bedeutung. Nur so lassen sich Integrität, Verfügbarkeit und Vertraulichkeit der Geobasisdaten zuverlässig gewährleisten und die gesetzlichen Vorgaben erfüllen.

Gleichzeitig führt die steigende Komplexität der regulatorischen Vorgaben – von NIS-2 über KRITIS bis hin zum BSI-Grundschutz – zu erheblichen Herausforderungen in Personal, Technik und Organisation. Viele Verwaltungen stoßen dabei an strukturelle und ressourcenbedingte Grenzen.

Damit rückt die Wahl des richtigen Betriebsmodells in den Mittelpunkt. Ein professionell geführter, zertifizierter und skalierbarer IT-Betrieb ist in Eigenregie kaum noch wirtschaftlich oder dauerhaft sicher zu gewährleisten.

Moderne Betriebsmodelle – insbesondere cloudbasierte, herstellergeführte Plattformen – gewinnen deshalb massiv an Bedeutung: Sie ermöglichen ein Sicherheitsniveau, das mit vertretbarem Aufwand nur zentralisiert erreichbar ist, und schaffen langfristig stabile, revisionssichere und entlastende Rahmenbedingungen für die Behörden.

3. Handlungsempfehlungen

Bei der Umsetzung der regulatorischen Anforderungen trägt die Geschäftsleitung die Gesamtverantwortung für die Informationssicherheit. Sie muss diese Verantwortung aktiv wahrnehmen und Informationssicherheit als verbindliche Führungsaufgabe etablieren. Entscheidend dabei ist, sich regelmäßig über Risiken und Bedrohungslagen zu informieren, strategische Leitlinien vorzugeben, Zuständigkeiten klar zu definieren und die erforderlichen personellen und finanziellen Ressourcen bereitzustellen.

Nur wenn die Leitungsebene Informationssicherheit als strategische Daueraufgabe versteht, kann die Verwaltung den steigenden gesetzlichen Anforderungen gerecht werden und ein belastbares, revisionssicheres Sicherheitsniveau erreichen.

Das BSI-Projekt „Weg in die Basis-Absicherung“ (WiBA) bietet Ländern und Kommunen einen praxisnahen, niederschwelligen Einstieg in den IT-Grundschutz. Es richtet sich explizit an die Leitungsebene und unterstützt diese mit Checklisten und klaren Maßnahmenempfehlungen.

WiBA ermöglicht es, ohne sofortige Einführung eines vollständigen ISMS, zentrale Sicherheitsmaßnahmen umzusetzen und die Risiken von Cybervorfällen zu minimieren. Die Geschäftsleitung übernimmt dabei die Steuerung und Kontrolle des Prozesses und setzt den Startschuss für die Sicherheitsstrategie.

Die Umsetzung der WiBA-Empfehlungen bildet das Fundament für alle weiteren Handlungsempfehlungen zur Erfüllung der regulatorischen Anforderungen nach NIS-2, KRITIS und BSI-Grundschutz und sollte damit als erster, konkreten Schritt genutzt nutzen werden, um die nachfolgenden Maßnahmen durchzuführen. Im Folgenden erhalten Sie praxisnahe Handlungsempfehlungen, mit denen Sie direkt aktiv werden und die nächsten Schritte gezielt umsetzen können.

1. Risikomanagement und Sicherheitskonzepte etablieren

Führen Sie eine umfassende Risikoanalyse aller IT-Systeme und Prozesse durch, die Geobasisdaten betreffen. Entwickeln Sie ein strukturiertes Sicherheitskonzept, das technische (z. B. Verschlüsselung, Zugriffskontrolle) und organisatorische Maßnahmen (z. B. klare Verantwortlichkeiten, Notfallmanagement) umfasst. Dokumentieren Sie alle Maßnahmen und überprüfen Sie diese regelmäßig auf Aktualität und Wirksamkeit.

2. Informationssicherheitsmanagementsystem (ISMS) nach BSI-Grundschutz einführen

Implementieren Sie ein ISMS, das auf den Vorgaben des BSI-Grundschutzes basiert. Schulen Sie regelmäßig alle Mitarbeitenden zu IT-Sicherheit und sensibilisieren Sie diese für aktuelle Bedrohungen. Führen Sie regelmäßige Sicherheitsaudits und externe Prüfungen durch, um die Einhaltung der Standards nachzuweisen.

3. Melde- und Reaktionsprozesse aufbauen

Richten Sie klare Meldewege für Sicherheitsvorfälle ein, um die gesetzlichen Meldepflichten (z.B. 24-Stunden-Frist nach NIS2) einzuhalten. Stellen Sie eine 24/7-Erreichbarkeit für Notfälle sicher, z. B. durch eine zentrale Kontaktstelle. Entwickeln Sie einen Resilienz- und Notfallplan, um im Störungsfall schnell und koordiniert reagieren zu können.

4. Technische und organisatorische Maßnahmen umsetzen

Setzen Sie moderne Verschlüsselungs- und Zugriffskontrollsysteme ein, um die Integrität und Vertraulichkeit der Geobasisdaten zu gewährleisten. Protokollieren Sie alle Zugriffe und Änderungen an sensiblen Daten nachvollziehbar. Prüfen Sie regelmäßig die Einhaltung der technischen und organisatorischen Maßnahmen durch interne und externe Audits.

5. Sichere Cloud-Nutzung gewährleisten

Wählen Sie Cloud-Dienstleister, die nachweislich alle Anforderungen an Datenschutz, Integrität und Verfügbarkeit erfüllen. Achten Sie auf die Einhaltung europäischer Standards und die Nutzung von Open-Source-Technologien, um digitale Souveränität zu sichern. Dokumentieren Sie die Auswahl- und Prüfprozesse für Cloud-Dienstleister transparent.

6. Führung und Verantwortlichkeit stärken

Die Behördenleitung muss Cybersicherheit als Führungsaufgabe begreifen und sich regelmäßig über Risiken und Maßnahmen informieren. Definieren Sie klare Verantwortlichkeiten für die Informationssicherheit und überprüfen Sie Zuständigkeiten regelmäßig.

7. Cloud-Infrastruktur nutzen

Die Umsetzung der vielfältigen regulatorischen Anforderungen ist für viele Vermessungs- und Katasterverwaltungen komplex, zeitaufwendig und personell kaum zu stemmen. Eine professionelle, speziell auf diese Anforderungen ausgerichtete Cloud-Infrastruktur wie die LM Cloud kann hier entscheidend entlasten. Sie stellt geprüfte Sicherheitsstandards bereit, übernimmt zentrale technische und organisatorische Aufgaben im Hintergrund und schafft damit ideale Voraussetzungen, um gesetzliche Vorgaben zuverlässig und nachweisbar einzuhalten.

Im Folgenden wird die LM Cloud vorgestellt – mit einem Überblick auf ihre Funktionen, Sicherheitsstandards und die konkreten Vorteile für die Vermessungs- und Katasterverwaltungen.

4. Die Rolle der LM Cloud

Die LM Cloud ist auf die Anforderungen der Vermessungs und Katasterverwaltungen zugeschnitten und wird in einem deutschen Rechenzentrum der Telekom Cloud Public (TCP) betrieben. Sie erfüllt die regulatorischen Vorgaben nach NIS-2, KRITIS und BSI-Grundschutz und gewährleistet dabei digitale Souveränität.

Die nachfolgende Übersicht zeigt, dass die Anforderungen aus allen drei Regelwerken ineinandergreifen und sich gegenseitig verstärken. Für die Vermessungs- und Katasterverwaltung bedeutet dies, dass ein ganzheitliches Sicherheitskonzept notwendig ist, das sowohl technische als auch organisatorische Maßnahmen umfasst. Die LM Cloud unterstützt die Verwaltung dabei, diese komplexen Anforderungen effizient und nachweisbar zu erfüllen.

Regelwerk	Zentrale Anforderung	Bedeutung für Vermessungs- und Katasterverwaltung
NIS-2	• Risikomanagement für IT-Systeme • Meldespflichten und Behördenleitung • Nachweis und Dokumentation von Sicherheitsmaßnahmen	• Schutz und Überwachung aller Systeme, die Geobasisdaten verarbeiten • Schnelle Reaktion und Meldung bei Vorfällen • Cybersicherheit als Führungsaufgabe • Regelmäßige Überprüfung und Dokumentation der IT-Sicherheit
KRITIS	• Einführung eines ISMS nach BSI-Grundschutz • Nachweis der IT-Sicherheit • Regelmäßige Prüfungen • 24/7-Kontaktstelle • Resilienz- und Notfallplanung	• Aufbau eines Informationssicherheitsmanagementsystems • Nachweis der Einhaltung von Sicherheitsstandards • Sicherstellung der Verfügbarkeit und Integrität von Geobasisdaten • Notfallmanagement für kritische Prozesse
BSI-Grundschutz	• Umfassende Risikoanalyse • Technische Maßnahmen (Verschlüsselung, Zugriffskontrolle, Protokollierung) • Organisatorische Maßnahmen (Schulungen, klare Verantwortlichkeiten) • Sichere Cloud-Nutzung	• Identifikation und Absicherung sensibler Geodaten • Umsetzung technischer und organisatorischer Schutzmaßnahmen • Gewährleistung, das Cloud-Dienstleister sämtliche Anforderungen erfüllen

Die integrierte Ausgestaltung technischer und organisatorischer Sicherheitsmaßnahmen folgt dabei konsequent dem Prinzip „Compliance by Design“. Regulatorische Vorgaben sind von Beginn an in Architektur und Prozesse eingebunden und werden zentral, effizient und nachvollziehbar umgesetzt. Dadurch wird die zunehmende technische und regulatorische Komplexität beherrschbar gemacht und die Fachbereiche werden nachhaltig entlastet.

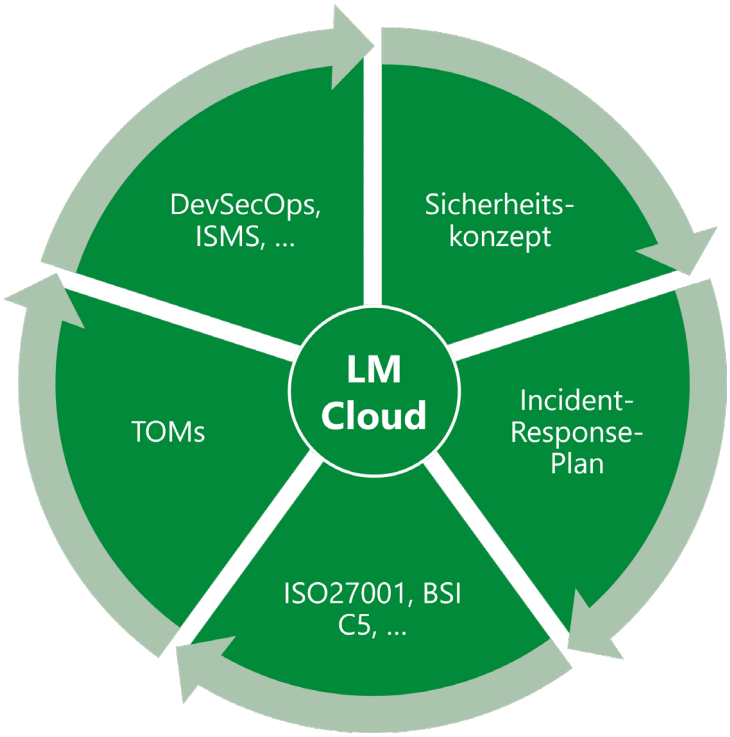
Im Zentrum steht ein ganzheitliches Sicherheitskonzept, das mehrere Ebenen berücksichtigt:

Governance & Standards
Ein etabliertes Information Security Management System (ISMS) sorgt für systematische Risikobewertung und -steuerung. Die LM Cloud erfüllt internationale Standards wie ISO 27001 und BSI C5 und wird in zertifizierten europäischen Rechenzentren betrieben – inklusive Audit-Nachweisen.

Technische & organisatorische Maßnahmen
Umfassender Zugriffsschutz, Verschlüsselung, Patch- und Backupmanagement sowie kontinuierliches Monitoring und regelmäßige Überprüfungen gewährleisten höchste Betriebssicherheit.

Sicherheitskultur & Entwicklung
Schulungen und Awareness-Programme fördern eine gelebte Sicherheitskultur. Mit DevSecOps wird Sicherheit direkt in die Softwareentwicklung integriert.

LM Cloud – „Compliance by Design“



5. Beispiele aus der Praxis

Referenzprojekt SenStadt – Berlin
Das Projekt „Managed Services Berlin“ umfasst die Migration und den Betrieb der AAA-Verfahren (AFIS, ALKIS, ATKIS) für die Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen Berlin (SenStadt) in der Telekom Cloud Public (TCP). Ziel ist die sichere, skalierbare und effiziente Bereitstellung von Geobasisdaten für die Hauptstadt. Das Projekt gilt als Vorbild für die sichere und effiziente Cloud-Migration von Geobasisdaten auf Landesebene. Die Senatsverwaltung profitiert von hoher Betriebssicherheit, Flexibilität und einer modernen IT-Infrastruktur.
Zum vollständigen Referenzbericht

Referenzprojekt LGV Hamburg und Geoinformation Bremen
Das Projekt „Managed Services Hamburg/Bremen“ umfasst die Migration und den Betrieb der AAA-Verfahren für die Freie und Hansestadt Hamburg sowie die Freie Hansestadt Bremen in der LM Cloud Plattform. Das Projekt Hamburg/Berlin zeigt, wie die Cloud-Migration und der Betrieb von Geobasisdaten in auf Landesebene erfolgreich umgesetzt werden. Die Lösung bietet hohe Sicherheit, Verfügbarkeit und Flexibilität für die Verwaltung und den Zugriff auf Geobasisdaten.
Zum vollständigen Referenzbericht

6. Fazit

Die Vermessungs- und Katasterverwaltungen stehen vor einem tiefgreifenden Transitionsprozess. Steigende regulatorische Anforderungen, zunehmende Cyberbedrohungen, komplexer werdende IT-Strukturen sowie die Verantwortung für ein jederzeit aktuelles, rechtssicheres und hochverfügbares Liegenschaftskataster prägen diesen Wandel maßgeblich.

Die Analyse macht deutlich: Ein professionell geführter, resilienter und nachweisbar sicherer IT-Betrieb ist unter heutigen Rahmenbedingungen kaum noch vollständig in Eigenregie zu leisten.

Moderne Cloud-Plattformen – insbesondere eine herstellergeführte LM Cloud – eröffnen einen klaren Weg, diese Herausforderungen effizient, wirtschaftlich und zukunftssicher zu bewältigen. Sie vereinen technische Sicherheit, regulatorische Compliance und organisatorische Entlastung in einem Betriebsmodell, das Landesbehörden und kommunale Verwaltungen nachhaltig stärkt.

Dies macht zeitnahes Handeln erforderlich: Wer in den kommenden Jahren die Anforderungen aus NIS-2, KRITIS und BSI-Grundschutz erfüllen, Risiken wirksam reduzieren und zugleich die eigene digitale Souveränität sichern möchte, sollte jetzt die nächsten Schritte einleiten.

Empfohlen wird ein stufenweises Vorgehen: eine WiBA-Basisabsicherung, eine kritische Evaluation des bestehenden Betriebsmodells sowie die Prüfung des Einsatzes der LM Cloud als zukunftssichere Plattform für den sicheren Betrieb von Geobasisdaten. VertiGIS unterstützt diesen Prozess mit zertifizierter Infrastruktur, erprobten Migrationspfaden sowie fundierter Beratung und einem erfahrenen Serviceteam.

Sprechen Sie uns an und nutzen Sie die Möglichkeit, gezielt Unterstützung einzuholen. Gemeinsam schaffen wir die Grundlage für ein modernes, widerstandsfähiges und zukunftsfähiges Liegenschaftskataster.

Über VertiGIS:

VertiGIS nutzt das Potenzial von geografischen Informationen, um Organisationen dabei zu unterstützen, intelligenter und effizienter zu arbeiten. Mit innovativen Geodatenlösungen verbindet VertiGIS komplexe Standortinformationen nahtlos mit den Arbeitsabläufen von Versorgungsunternehmen, Behörden, Telekommunikationsanbietern sowie Teams aus Handel und Industrie. So können Organisationen ihre Ressourcen präzise verwalten, die Effizienz steigern und herausragende Ergebnisse erzielen.

Die Technologievision von VertiGIS treibt diese digitale Transformation voran. Cloud-basierte, branchenspezifische und KI-gestützte Tools werden mit einem leistungsstarken Portfolio kombiniert, darunter VertiGIS Studio, VertiGIS Networks, VertiGIS FM, VertiGIS LM und VertiGIS ConnectMaster. Diese branchenfokussierten Lösungen optimieren bestehende Arbeitsprozesse und sind flexibel skalierbar – von kleinen Teams bis hin zu organisationsweiten Implementierungen.

Weltweit vertrauen mehr als 5.000 Organisationen auf VertiGIS, um Geoinformationen in entscheidungsrelevante Daten zu verwandeln.

Weitere Informationen finden Sie unter http://www.vertigis.com/de.