Informationsmanagement in der kommunalen Praxis

Inhaltsübersicht

Aktuelle Situation

- 2019 besaßen rund 91% der privaten Haushalte einen Internetzugang
- Nach Angaben des Statistischen Bundesamtes nutzen 50% der der Bevölkerung in Deutschland das Internet für Kontakte mit Behörden
- Die Durchdringung der privaten Haushalte mit Kommunikationstechnik und deren verstärkte Nutzung führen auch zur Öffnung der Behördennetze und der Bereitstellung von Internetangeboten.
- Damit stellen sich für die Behördenleitungen plötzlich viele Fragen

Aktuelle Situation

- Wie abhängig bin ich von einer funktionierenden Informationsverarbeitung?
- Kann ich meine Dienstleistungen auch ohne IT erbringen?
- Welche Auswirkungen hat ein Ausfall der Technik?
- Wie hoch sind die finanziellen und organisatorischen Auswirkungen?
- Kenne ich alle rechtlichen Vorgaben?

ISMS in der Behörde

Um ein ISMS einzuführen und ein höchstmögliches Sicherheitsniveau zu erreichen ist es notwendig

- Regeln,
- Prozesse und
- Maßnahmen

zu etablieren.

Dazu gehört es auch Aufgaben und Verantwortlichkeiten zu definieren und den entsprechenden Personen und Organisationseinheiten verbindlich zuzuweisen.

ISMS in der Behörde

Der Aufbau und Umfang eines ISMS ist international standardisiert und im ISO 27001 definiert

In deutschen Behörden hat sich der BSI-Standard etabliert, dieser bietet einen Leitfaden beim Aufbau und dauerhaften Betrieb eines ISMS

ISMS in der Behörde

Das Thema Informationssicherheit muss in alle Geschäftsprozesse der Behörde eingebunden werden.

Wichtige Punkte sind unter anderem:

- Aktuelle Dokumentation der eingesetzten Hard- und Software
- Prozessbeschreibungen der Inbetriebnahme und Einführung von Hard- und Software
- Beschreibung eines kontinuierlichen Verbesserungsprozesses
- Entsorgung von Hardware
- Handbücher und Arbeitsanweisungen

Verantwortung

Beim Thema Informationssicherheit müssen demnach immer eine Vielzahl von Organisationseinheiten eigebunden werden. Hauptverantwortung obliegt der Behördenleitung. Die Dezernenten und Amtsleiter tragen in der Regel die Verantwortung für ihr jeweiliges Ressort.

Nachfolgende Einzelverantwortliche sollten nach den Empfehlungen des BSI benannt werden

Verantwortung

- **Sicherheitsteam** – IT-Experten gemeinsam mit Querschnittsämtern
- **Informationssicherheitsbeauftragter** – nach ISO empfohlen
- **Datenschutzbeauftragter** – gesetzlich vorgeschrieben
- **Dienststellen** - als Informationseigentümer
- **Informationstreuhänder** – in der Regel die Informationsverarbeitende Stelle (IT-Dienstleister)
- **Nutzer*innen** – alle Nutzer*innen sind den gesetzlichen Vorgaben und den internen Richtlinien der Behörde verpflichtet

Auditierung und Zertifizierung

- Die Umsetzung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik zum Schutz der Informationen und die Umsetzung eines geeigneten ISMS ist in vielen Fällen gesetzlich vorgeschrieben. Bekanntestes Beispiel ist die DSGVO
- Ein entsprechendes Audit oder eine Zertifizierung des ISMS ist keine reine Marketingmaßnahme, sondern hat die Aufgabe einen juristisch belastbaren Nachweis zu führen, dass die Behördenleitung ihren gesetzlichen Verpflichtungen nachgekommen ist
- Für diese Nachweise eignen sich Standards wie das BSI-Kompendium oder die ISO 27000 Familie

Auswirkung unzureichender Maßnahmen

Die Gesetzgeber auf europäischer und nationaler Ebene haben auf die Risiken durch den Einsatz von IT reagiert

- DSGVO, DSG, Bundessicherheitsgesetz, SGB, KonTraG, GmbH-Gesetz, ePR-Verordnung, um nur einige zu nennen

Sie alle sehen vor, dass die Daten nach dem Stand der Technik durch entsprechende organisatorische und technische Maßnahmen durch den Verantwortlichen zu schützen sind

Auswirkung unzureichender Maßnahmen

Wenn aufgrund von unzureichenden Maßnahmen Schäden entstehen, stellt sich die Frage der Verantwortung der Führungskräfte der Behörde.

Die gesetzlichen Regelungen sehen unterschiedliche Sanktionen gegen Verstöße gegen die gesetzlichen Vorgaben vor.

z.B.

- Zivilrechtliche Haftung nach dem BGB
- OWiG
- Strafrecht
- Bußgelder

Fazit

Informationssicherheit ist auch im Behördenumfeld keine freiwillige Aufgabe

Gesetzliche Vorgaben machen die Umsetzung eines ISMS zu einer Verpflichtung

ISMS ist Chefsache – Nichtbeachtung birgt enorme juristische Risiken

Wichtig:

Der Aufbau eines ISMS **ist kein Projekt**, sondern ein fortlaufender Prozess, der kontinuierlich umgesetzt und überwacht werden muss

Nun freue ich mich auf Ihre Fragen