LSI-Info A#01

WAS MUSS EINE KOMMUNE FÜR IHRE (IT-)SICHERHEIT TUN?

RECHTLICHE RAHMENBEDINGUNGEN

Version 1.4 vom: 24.01.2024

Management Summary

Die zunehmende Digitalisierung durchdringt die kommunale Verwaltung immer stärker. Der Gesetzgeber hat im Rechtsrahmen für die digitale Verwaltung auch den Bereich der IT-Sicherheit reguliert. Kommunale Verwaltungen schützen ihre IT-Systeme somit nicht ausschließlich, um den sich verschärfenden Cyberbedrohungen zu begegnen, sondern auch um die gesetzlichen Vorgaben einzuhalten. Überwölbende Herausforderungen bringen die Aufgaben des Onlinezugangsgesetzes, nach dem alle Verwaltungsleistungen auch im Internet anzubieten sind. Um die hierbei entstehenden Risiken zu minimieren und dadurch das Vertrauen der Bürger zu erhalten, ist ein angemessenes IT-Sicherheitsniveau anzustreben.

Diese LSI-Info soll über die für Kommunen besonders wichtigen rechtlichen Rahmenbedingungen zur IT-Sicherheit einen Überblick geben.

- Seit 01. Januar 2020: Angemessene Maßnahmen zur Erhöhung der organisatorischen und technischen IT-Sicherheit ergreifen und ein Informationssicherheits-Konzept erstellen.

HINTERGRUND

Der Gesetzgeber will beispielsweise vermeiden, dass

- bei Ihnen gespeicherte Daten an die Öffentlichkeit gelangen,
- diese Daten bösartig oder durch einen Unglücksfall unwiederbringlich vernichtet werden,
- ihre Rechner mit Schadsoftware verseucht werden und fremde Systeme angreifen.

GESETZLICHE GRUNDLAGEN

Art. 36 Sätze 1 und 2 BayDiG (vormals bedeutungsgleicher Art. 8 Abs. 1 BayEGovG):

[1]Die Behörden unterhalten die zur Erfüllung ihrer Aufgaben erforderlichen digitalen Verwaltungsinfrastrukturen. [2]Sie gewährleisten deren Sicherheit und fördern deren gegenseitige technische Abstimmung und Barrierefreiheit.

Art. 43 Abs. 1 BayDiG (vormals bedeutungsgleicher Art. 11 Abs. 1 BayEGovG):

[1]Die Sicherheit der informationstechnischen Systeme der Behörden ist im Rahmen der Verhältnismäßigkeit sicherzustellen.
[2]Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen im Sinn von Art. 32 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und Art. 32 des Bayerischen Datenschutzgesetzes und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.

WELCHE KONSEQUENZEN DROHEN IHRER KOMMUNE UND DEN VERANTWORTLICHEN PERSONEN?

Wer (personenbezogene) Daten ohne ein entsprechendes IT-Sicherheitskonzept verarbeitet, erfüllt – unabhängig von den bereits bestehenden datenschutzrechtlichen Bestimmungen – spätestens seit 01. Januar 2020 nicht mehr die gesetzlichen Anforderungen. Im Falle eines Datenlecks oder der Verletzung des Schutzes personenbezogener Daten geht neben möglichen haftungsrechtlichen Konsequenzen auch ein monetär nicht messbarer Reputationsverlust einher.

- Ein IT-Sicherheitskonzept gliedert sich in drei Bereiche: **Organisation**, **Technik** und **Awareness**. Für die Erreichung eines hohen und einheitlichen Sicherheitsniveaus müssen alle gleichermaßen Berücksichtigung finden.

WAS IST BEISPIELSWEISE ZU TUN (ORGANISATION)?

- Benennung eines Informationssicherheitsbeauftragten (ISB).
- Verabschiedung einer Sicherheitsleitlinie.
- Auswahl eines für die Kommune passenden Vorgehensmodells zur Erstellung eines Informationssicherheitskonzeptes, z. B. Einführung eines passenden Informations-Sicherheits-Management-Systems (ISMS).
- Abarbeitung der darin genannten technischen und organisatorischen Maßnahmen.

- Ein ISB ist der zentrale Ansprechpartner für die Informationssicherheit. Er koordiniert den Sicherheitsprozess und berichtet dem Bürgermeister oder dem Landrat (idealerweise direkt).
- Eine Sicherheitsleitlinie drückt die Bedeutung der Sicherheit für die Kommune aus, ist vom Bürgermeister oder Landrat unterschrieben und sensibilisiert so die Mitarbeiter.

WELCHES KONZEPT BZW. ISMS PASST ZU IHRER KOMMUNE?

- Arbeitshilfe (der Innovationsstiftung Bayerische Kommune)
- BSI IT-Grundschutz „Basis-Absicherung Kommunalverwaltung“
- BSI IT-Grundschutz „Basis-Absicherung“
- BSI IT-Grundschutz „Standard-Absicherung“
- CISIS12 (IT-Sicherheitscluster e.V.)
- ISIS12 (letzte Zertifizierung bis 06/2024)

- ISMS4KMO
- ISO 27001
- VdS 10000 (ehemals VdS 3473)

Jeder Schritt zur Erhöhung des IT-Sicherheitsniveaus ist richtig und wichtig. Deshalb ist die Wahl eines geeigneten ISMS-Standards mit Blick auf den Schutzbedarf der Daten ein erster wichtiger Schritt. Gerne berät das LSI die bayerischen Kommunen hierzu individell.

Im Informationssicherheits-Prozess sind u. a. folgende Fragen zu beantworten: Welchen Schutzbedarf haben meine Daten (z. B. Einwohnermeldeverfahren, Personaldaten), welche IT-Systeme sind beteiligt und entsprechend zu schützen? Dabei ist der ganze Informationsverbund – auch Außenstellen wie Kindergärten, Bauhof etc. – zu betrachten. Teile eines Informationssicherheitskonzeptes sind:

- Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und Maßnahmen.
- Zuständigkeiten festlegen.
- Erlass von Sicherheitsrichtlinien.
- Bekanntmachen der Regelungen und Zuständigkeiten.
- Sensibilisierung und Schulung der Mitarbeiter.

Die Gewährleistung der Informationssicherheit ist ein dauerhafter Prozess. Die meisten Aufgaben müssen regelmäßig überprüft oder erneut durchlaufen werden, um auch zukünftigen Bedrohungslagen begegnen zu können.

WELCHE TECHNISCHEN MASSNAHMEN SIND MINDESTENS ZU ERGREIFEN (TECHNIK)?

- Patch-Management
- Malwareschutz mit regelmäßiger Signaturaktualisierung
- Netzwerksegmentierung (Brandabschnitte im Netzwerk)
- Firewall
- Hilfreich ist ein Anschluss an das Bayerische Behördennetz

Detaillierte Infos zu Patchmanagement bietet das LSI-Info T#08.

WIE KANN BEI MITARBEITERN EIN SICHERHEITSBEWUSSTSEIN GESCHAFFEN WERDEN (AWARENESS)?

- Mitarbeit in das Zentrum der Sicherheit rücken (Awareness-Kampagnen)
- Schulungen (Fortbildungen, eLearning-Kurse)
- Nachhaltigkeit schaffen (Blöcke mit Sprüchen zur Sicherheit, Postkarten, etc.)

Detaillierte Infos zu Awareness bietet das LSI-Info A#02.

DAS LSI EMPFIEHLT FÜR ALLE DREI BEREICHE:

Beginnen Sie mit diesen Maßnahmen so frühzeitig wie möglich. Erfahrungsgemäß benötigen viele kleinere Gemeinden hierfür externe IT-Dienstleister.
Nutzen Sie das immense Potential, das Ihnen ein kommunales Behördennetz sicherheitstechnisch bietet.

IT-SICHERHEIT IST GRUNDLAGE FÜR DIE EINHALTUNG DER DATENSCHUTZ-VORSCHRIFTEN.

§ Seit 25. Mai 2018 gelten die **EU-Datenschutzgrundverordnung** (DSGVO) und ergänzend das bayerische Datenschutzgesetz (BayDSG).

Die Behörde hat zu gewährleisten, dass die datenschutzrechtlichen Vorgaben der DSGVO eingehalten werden und die Verarbeitung personenbezogener Daten in ihrem Verantwortungsbereich rechtmäßig erfolgt.

- Die alleinige Verantwortung bis zu einer Delegation trägt zunächst der erste Bürgermeister bzw. Landrat.
- Er kann diese vielfältigen Pflichten mittels einer Geschäftsanweisung auf Organisation, IT und Datenschutz sowie die Fachabteilungen übertragen.

Behörden haben als „Verantwortlicher“ auf jedem Fall einen Datenschutzbeauftragten zu benennen (Art. 37 Abs. 1 Buchstabe a DSGVO, Art. 12 BayDSG) und an den BayLfD zu melden (Art. 37 Abs. 7 DSGVO).

- Datenschutzbeauftragte entscheiden nicht allein über die Verarbeitung von personenbezogenen Daten. Sie unterrichten und beraten den

Verantwortlichen. Auch nehmen sie Überwachungsaufgaben wahr und sind Anlaufstelle für die Aufsichtsbehörden, Art. 39 DSGVO. Somit tragen Verwaltungsleiter, Amtsleiter oder Leiter eines Fachsachgebiets die Verantwortung für den Datenschutz in ihrem Zuständigkeitsbereich trotz Benennung eines Datenschutzbeauftragten weiterhin mit. Die Letztverantwortlichkeit verbleibt beim ersten Bürgermeister als Behördenleitung.

- Nach Art. 32 Abs. 1 DSGVO sind zur Gewährleistung eines angemessenen Schutzniveaus geeignete Maßnahmen zu treffen. Die Kommunen können diesen Pflichten am besten durch die Einführung eines ISMS und der Abarbeitung der sich daraus ergebenden Schritte nachkommen.

- Arbeitshilfen und Muster finden sie unter

  https://www.stmi.bayern.de/sus/datenschutz/arbeitshilfen/index.php

Die Meldung des Datenschutzbeauftragten kann über diesen Link erfolgen:
https://www.datenschutz-bayern.de/service/bdsb.html.

KONTAKT

Weitere Informationen finden Sie unter:
https://lsi.bayern.de/kommunen/
Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:
Beratung-Kommunen@lsi.bayern.de.
Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911 21549-523 für Sie erreichbar.

Landesamt für Sicherheit in der Informationstechnik – Leitfaden A#01 Was muss eine Kommune für Ihre (IT-)Sicherheit tun? (Stand: 24.01.2024)
Verwendungshinweis: Dieses Dokument darf nur in unveränderter Form unter eindeutiger Angabe der Quelle und des Sachstands verbreitet werden.