LSI-Info I#01

KOMMUNALE IT-SICHERHEIT

INFORMATIONEN ZUM SIEGEL „KOMMUNALE IT-SICHERHEIT“ FÜR BAYERISCHE KOMMUNEN

Version 3.0 vom: 01.06.2023

Management Summary

Bei der Digitalisierung der kommunalen Verwaltungen sind steigende Anforderungen an die IT-Sicherheit zu bewältigen – auch von kleinen Gemeinden. Das aus dem BayEGovG hervorgegangene BayDiG verpflichtet deshalb alle bayerischen Kommunen seit 01.01.2020 ein Informationssicherheitskonzept zu erstellen. Das Landesamt für Sicherheit in der Informationstechnik (LSI) unterstützt die bayerischen Kommunen dabei mit dem Siegel „Kommunale IT-Sicherheit“. Zielsetzung ist ein Mindestsicherheitsniveau, das den gesetzlichen Anforderungen entspricht. Das LSI begleitet und berät die Kommunen bei der Umsetzung der hierfür notwendigen Maßnahmen. Mit dem Siegel gibt das LSI gerade kleinen Gemeinden eine wertvolle Orientierung bei dieser anspruchsvollen Herausforderung.

WAS IST DAS SIEGEL „KOMMUNALE IT-SICHERHEIT“?

Das Siegel „Kommunale IT-Sicherheit“ ist selbst kein ISMS (Informationssicherheits-Managementsystem) und ersetzt keinen der gängigen ISMS-Standards. Es kann als eine Art Vorstufe zu einer Zertifizierung auf Basis einer Selbstauskunft betrachtet werden.

Voraussetzung ist, dass die Kommune ein Informationssicherheitskonzept z.B. auf Grundlage des BSI IT-Grundschutz, ISIS12, ISA+, VdS 10.000 oder der Arbeitshilfe der Innovationsstiftung Bayerische Kommune erstellt. Der Fragebogen, den Sie auf Anfrage unter den am Ende genannten Kontaktdaten erhalten, prüft verschiedene Maßnahmen zur Einführung eines Informationssicherheitskonzeptes nach BayDiG ab. Für die Zielgruppe bestätigt das Siegel eine Basisabsicherung nach aktuellem Stand der Technik und Rechtslage in Bayern.

BSI IT-Grundschutz 100-x

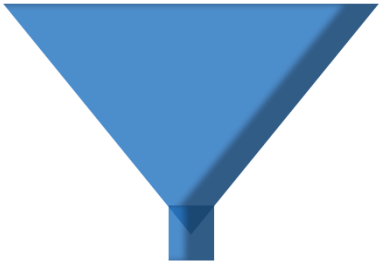
BSI IT-Grundschutz 200-x Profil Basisabsicherung Kommunalverwaltung

ISIS 12

VdS Standard 3473 / 10.000

INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE

ISA+



- **Maßnahmen mit Prüffragen**
- **Basisabsicherung für bayerische Kommunen konform zu BayEGovG**

WELCHEN MEHRWERT BRINGT DAS SIEGEL „KOMMUNALE IT-SICHERHEIT“ BAYERISCHEN KOMMUNEN?

- Nachweis der gesetzeskonformen Einführung eines Informationssicherheitskonzeptes nach Art. 43 Abs. 1 BayDiG
- Einholen von Feedback und Beratung durch das LSI zu erforderlichen technischen und organisatorischen Maßnahmen in der Informationssicherheit
- Darstellung des sicheren Einsatzes von Informations- und Kommunikationstechnologien gegenüber den Bürgerinnen, Bürgern und Gewerbetreibenden
- Möglichkeit, das Siegel „Kommunale IT-Sicherheit“ des LSI während der Gültigkeitsdauer zu verwenden.

WELCHE ASPEKTE DER INFORMATIONSSICHERHEIT DECKT DAS SIEGEL AB?

ISB	Cloud- und Outsourcing
Leitlinie	Software-, Hardware- und Patch-Management
Personal und Organisation	Identitäts- und Berechtigungsmanagement
Backup und Recovery	Server
Datenschutz	Netzwerk
Schutz vor Schadprogrammen	Notfallmanagement
Verschlüsselung	

AN WELCHE ZIELGRUPPE RICHTET SICH DAS SIEGEL „KOMMUNALE IT-SICHERHEIT“?

Das Siegel richtet sich insbesondere an kleinere bayerische Städte, Märkte und Gemeinden.
Auch größeren Kommunen steht es grundsätzlich frei, das Siegel des LSI zu beantragen. Je größer die Kommune, desto mehr wird jedoch das Informationssicherheitskonzept der Organisationsgröße, der komplexeren Netzarchitektur und Prozessen Rechnung tragen müssen. Wir empfehlen diesen Kommunen, eine Zertifizierung nach einem ISMS-Standard anzustreben.

Sollte eine Kommune bereits nach einem ISMS-Standard zertifiziert sein, kann die Zertifizierung anerkannt werden, um das Siegel „Kommunale IT-Sicherheit“ des LSI zu erhalten.

MÜSSEN ALLE MASSNAHMEN AUS DEM SIEGEL VOLLSTÄNDIG UMGESETZT WERDEN?

Es lohnt sich in jedem Fall, den Fragebogen des Siegels auszufüllen und einzusenden. Der Fragenkatalog dient dem LSI als Grundlage für eine passgenaue Beratungsleistung. Der Fragenkatalog enthält auch Maßnahmen, die über eine Basisabsicherung hinausgehen und für eine Erteilung des Siegels noch nicht (vollständig) abgeschlossen sein müssen. Gerade dann, wenn die Kommune noch nicht alle Maßnahmen umgesetzt hat, berät das LSI gerne zu technischen und organisatorischen Maßnahmen der Informationssicherheit.

WIE LANGE IST DAS SIEGEL GÜLTIG?

Das Siegel ist für Kommunen unter 20.000 Einwohner zwei Jahre gültig. Für größere Kommunen aufgrund der höheren Anforderungen ein Jahr. Für Kommunen mit mehr als 50.000 Einwohnern, kreisfreie Städte sowie Landratsämter ist für den Erhalt des Siegels eine Zertifizierung erforderlich. Alternativ ist auch ein Testat nach der Basis-Absicherung des BSI IT-Grundschutzes, bzw. die Abnahme des IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ ausreichend. Mit einem Zertifikat, unabhängig von der Größe der Kommune, richtet sich die Gültigkeitsdauer des Siegels nach der des Zertifikats. Mit Erlöschen des Zertifikats erlischt auch die Gültigkeit des Siegels. Danach haben Kommunen die Möglichkeit, das Siegel wieder neu zu erwerben (unter Vorbehalt der kontinuierlichen Weiterentwicklung der Informationssicherheit und Umsetzung geplanter Maßnahmen).

WAS IST NEU IM SIEGEL 3.0?

Um der aktuellen Sicherheitslage gerecht zu werden und um die schrittweise Verbesserung der Informationssicherheit in Bayern weiter zu unterstützen, wurden mit der Veröffentlichung der neuen Version des Fragebogens am 01.06.2023 einige bestehende Maßnahmen angepasst und andere neu hinzugefügt – neben der Betrachtung von IoT-Geräten / Haus-IT, Vorkehrungen bei exponierten Servern oder SSL-Analyse, flossen Erkenntnisse aus kommunalen Sicherheitsvorfällen ein.

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 I#01 Kommunale IT-Sicherheit (Stand: 01.06.2023)