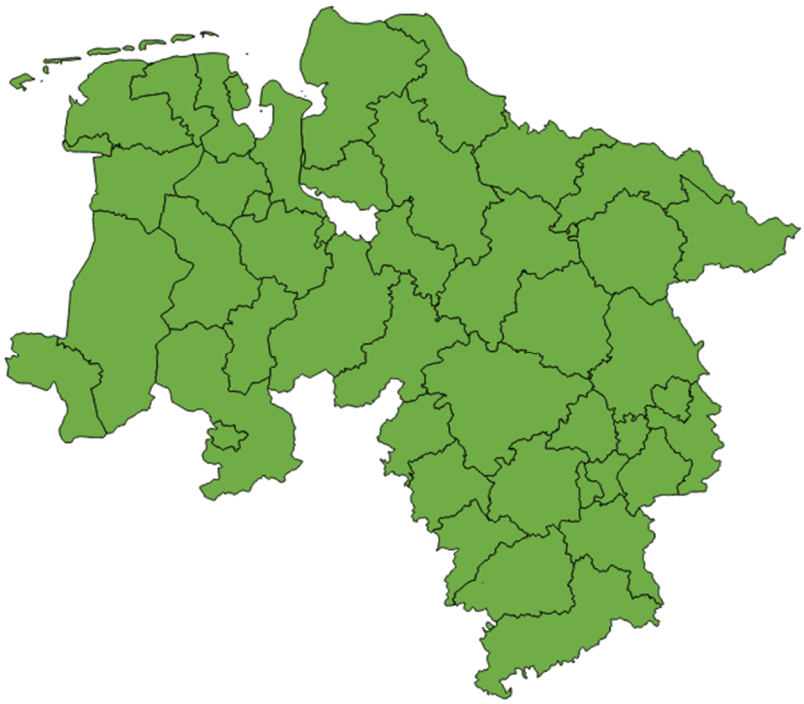
Die Präsidentin des
Niedersächsischen Landesrechnungshofs

- Überörtliche Kommunalprüfung -



Kommunalbericht 2017

Niedersachsen

Kommunalbericht

der

Präsidentin

des Niedersächsischen Landesrechnungshofs

- Überörtliche Kommunalprüfung -

2017

Übersandt an

- Nds. Landtag
- Nds. Landesregierung
- Nds. Landkreistag
- Nds. Städtetag
- Nds. Städte- und Gemeindebund

Herausgeberin:

Die Präsidentin des Nds. Landesrechnungshofs
Justus-Jonas-Str. 4
31137 Hildesheim
http://www.lrh.niedersachsen.de

5.10 Informationssicherheit in Kommunen – Bisher ist es meist gut gegangen

Bei 20 geprüften Kommunen bestand in den Bereichen Informationssicherheitsmanagement, Gebäudesicherheit und Notfallmaßnahmen Handlungsbedarf, um die Informationssicherheit zu verbessern.

Lediglich ein Viertel der 20 geprüften Kommunen verfügte über eine Leitlinie zur Informationssicherheit, die Kernelemente, wie Sicherheitsstrategie und -ziele, festlegte.

Hintergrund und Ziel der Prüfung

Der digitale Wandel beeinflusst alle kommunalen Verwaltungsprozesse. Die überörtliche Kommunalprüfung untersuchte 2016 bei 20 Kommunen[50] mit bis zu 15.000 Einwohnern[51] mit Hilfe eines umfassenden Fragenkatalogs, wie intensiv sich die geprüften Kommunen mit den Themen Informationssicherheit und Datenschutz im Sinne des NDSG auseinandergesetzt und diese organisatorisch umgesetzt hatten. Der Fragenkatalog deckte unter anderem die Bereiche Informationssicherheitsmanagement, Gebäudesicherheit, Notfallmaßnahmen, Schulungen und Unterweisungen kommunaler Mitarbeiter sowie Datenschutzbeauftragte ab.

Verbindliche Leitlinie für die Informationssicherheit fehlte häufig

Um eine bestmögliche Unterstützung kommunaler Verwaltungsprozesse durch den Einsatz der Informationstechnik zu erreichen, ist es geboten, unter Beachtung des Grundsatzes der Wirtschaftlichkeit (§ 110 Abs. 2 NKomVG) Rahmenwerke, Richtlinien und Organisationsstrukturen (Informationssicherheits-Managementsysteme) zu entwickeln und fortlaufend bedarfsgerecht anzupassen.[52]

Eine Leitlinie zur Informationssicherheit, in der für alle Mitarbeiter verständlich beschrieben war, welche Sicherheitsziele angestrebt werden und in welchem organisatorischen Rahmen diese umzusetzen sind, hatten zum Prüfungszeitpunkt nur fünf der geprüften 20 Kommunen eingeführt. Lediglich drei der 20 Kommunen verfügten über einen Notfallplan, der personenunabhängige Abläufe zur Bewältigung von Störungen im IT-Betrieb beschrieb.

Verfahrensbeschreibung nach NDSG

Nach § 8 S. 1 NDSG hat eine Kommune, die Verfahren zur automatisierten Verarbeitung personenbezogener Daten einrichtet oder ändert, in einer Verfahrensbeschreibung die

---

50 Geprüft wurden die Gemeinden Auetal, Bad Rothenfelde, Glandorf, Grasberg, Ilsede, Liebenburg, Söhlde, Wietze und Wagenfeld sowie die Samtgemeinden Eilsen, Grasleben, Lachendorf, Liebenau, Marklohe, Niedernwöhren, Rethem (Aller), Schwarmstedt, Sottrum, Steimbke und Thedinghausen.

51 Die Einwohnerzahl der Gemeinde Ilsede wuchs zwischenzeitlich infolge des Zusammenschlusses mit der Gemeinde Lahstedt auf rund 22.000 Einwohner an.

52 Deutscher Landkreistag (Hrsg.), Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, 2014, S. 6 ff.; Rechnungshöfe des Bundes und der Länder, Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik, 2016, S. 9.

Datenhaltung und -verarbeitung festzulegen. Nur in sechs der 20 Kommunen lagen Verfahrensbeschreibungen vollständig vor.

Serverräume noch besser sichern

Im Bereich Gebäudesicherheit stellte die überörtliche Kommunalprüfung fest, dass die geprüften Kommunen weitestgehend geeignete Maßnahmen, wie Zutrittskontrollen, getroffen hatten, um einen ungeregelten Zutritt unberechtigter Personen zu Bereichen mit schutzbedürftigen Informationen und Geräten zu verhindern oder zumindest zu erschweren.

Handlungsbedarf sah die überörtliche Kommunalprüfung dagegen beim Schutz von Serverräumen. In sechs Kommunen fehlten an den Türen der Serverräume Türschlösser oder die Türschlösser waren Teil einer Schließanlage, bei der alle Mitarbeiter der Kommune grundsätzlich unbeschränkten Zutritt zu den Serverräumen hatten. Lediglich sechs Kommunen sicherten ihre Serverräume durch Sicherheitstüren mit Widerstandsklassen. Sieben Kommunen nutzten ihre Serverräume auch als Lager- oder Archivräume und erhöhten dadurch die Brandlast. Teilweise führten wasserführende Druckleitungen durch Serverräume, ohne dass beispielsweise eine Absicherung gegen Wassereinbruch durch Gefahrenmelder erfolgte.

Ansicht 17: Wasserführende Druckleitung in einem Serverraum

Notfallvorsorge – Ein wichtiger Baustein der Informationssicherheit

IT-gestützte Prozesse und Systeme müssen sicher und zuverlässig funktionieren, da Störungen oder Ausfälle nicht unerhebliche Schäden nach sich ziehen können. Regelmäßige ereignisunabhängige Tests sind wichtig, um präventiv Schwachstellen zu beseitigen und Risiken zu reduzieren. Nur eine Kommune testete ereignisunabhängig ihre Notfallmaßnahmen.

Eine unterbrechungsfreie Stromversorgung (USV) garantiert einerseits bei Netzausfall einen ununterbrochenen Betrieb der IT-Geräte und -Systeme und ermöglicht andererseits eine rechtzeitige Reaktion, wie die Benachrichtigung eines Verantwortlichen oder das geordnete Herunterfahren eines elektronischen Systems ohne Datenverluste. Vier Kommunen verfügten bisher über keine unterbrechungsfreie Stromversorgung und setzten sich im Falle eines Stromausfalles dem Risiko eines Datenverlusts aus.

Mitarbeiter für das Thema Datenschutz und -sicherheit sensibilisieren

Für den Schutz von personenbezogenen Daten reicht es regelmäßig nicht aus, sich auf technische Lösungen zu beschränken. Häufig stellen fehlende Kenntnisse oder mangelndes Problembewusstsein einzelner Mitarbeiter ein Risiko dar. Ein angemessenes Sicherheitsniveau lässt sich nur erreichen und halten, wenn Mitarbeiter regelmäßig für die Themen Datenschutz und -sicherheit, zum Beispiel durch Schulungen, sensibilisiert werden. Nur drei der 20 geprüften Kommunen sensibilisierten ihre Mitarbeiter im Rahmen einer Schulung für die Themen Datenschutz und -sicherheit.

Die Bestellung eines Datenschutzbeauftragten ist gesetzliche Pflicht

Kommunen, die personenbezogene Daten automatisiert verarbeiten, sind verpflichtet, behördliche Datenschutzbeauftragte zu bestellen. Anstelle eigener Mitarbeiter (interne Datenschutzbeauftragte) können Kommunen auch Personen, die nicht der datenverarbeitenden Stelle angehören (externe Datenschutzbeauftragte), als Datenschutzbeauftragte beauftragen, § 8a Abs. 1 NDSG.

Datenschutzbeauftragte unterstützen die Kommunen bei der Sicherstellung des Datenschutzes. Als Datenschutzbeauftragte dürfen Kommunen nur Personen bestellen, die die erforderliche Sachkenntnis auf den Gebieten der Datenverarbeitung, der behördlichen Organisation und der einschlägigen Rechtsvorschriften sowie die erforderliche Zuverlässigkeit besitzen.[53] Ferner dürfen Kommunen als Datenschutzbeauftragte nur Personen bestellen, die durch die Bestellung keinen Interessenkonflikten mit anderen dienstlichen Aufgaben ausgesetzt sind, § 8a Abs. 2 NDSG.

Eine Kommune hatte es versäumt, einen Datenschutzbeauftragen zu bestellen. Fünf der 20 Kommunen hatten zum Zeitpunkt der örtlichen Erhebungen einen externen Datenschutzbeauftragten bestimmt.

Bei knapp einem Drittel der Kommunen mit einem internen Datenschutzbeauftragten wünschten die Datenschutzbeauftragten zusätzliche Schulungen, um die für die Aufgabe erforderliche Sachkenntnis zu vertiefen. Ferner waren bei knapp einem Drittel der Kommunen die Datenschutzbeauftragen nicht frei von etwaigen Interessenskonflikten, da sie im Rahmen ihrer weiteren Verwaltungsaufgaben, zum Beispiel als Beschäftigte im IT- oder Personalbereich, ebenfalls mit der Verarbeitung personenbezogener Daten befasst waren.

Die überörtliche Kommunalprüfung stellte in Kommunen mit einem externen Datenschutzbeauftragten weniger Verstöße gegen datenschutzrechtliche Regeln fest als in Kommunen mit einem internen Datenschutzbeauftragten.

Empfehlungen

Mit zunehmender Digitalisierung nehmen Informationssicherheit und Datenschutz einen immer höheren Stellenwert ein. Die überörtliche Kommunalprüfung empfiehlt den Kommunen aufgrund ihrer Prüfungserkenntnisse unter Beachtung des Grundsatzes der Wirtschaftlichkeit,

- Rahmenwerke und Richtlinien zur Informationssicherheit und zum Datenschutz zu entwickeln oder zu erweitern und fortlaufend anzupassen,

---

[53] Vgl. Der Landesbeauftragte für den Datenschutz Niedersachsen (Hrsg.), Das Niedersächsische Datenschutzgesetz, Gesetzestext und Kommentar, 2014, S. 68.

- mittelfristig ein an die Größe ihrer Kommune angepasstes Informationssicherheits-Managementsystem zur Sicherstellung gesetzlicher Anforderungen und zur Abwehr von Gefahren zu etablieren,
- ihre bestehenden Konzepte zur Gebäudesicherheit und zur Notfallvorsorge zu überprüfen, um (präventiv) Störungen oder Notfälle und damit Schäden durch den Ausfall von Informationstechniken oder dem Verlust von Daten zu vermeiden,
- ihre Mitarbeiter noch stärker für die Themen Informationssicherheit und Datenschutz zu sensibilisieren und sie zu diesen Themen bedarfsgerecht zu schulen und
- zu prüfen, ob eine kleine Kommune die häufig komplexen, einem fortlaufenden Wandel unterliegenden Aufgaben des Datenschutzes und der -sicherheit allein noch ordnungsgemäß und frei von Interessenkonflikten abbilden kann, oder ob es zur Reduzierung von Risiken geboten erscheint, Aufgaben auf eine hierauf spezialisierte externe Stelle oder Einrichtung, wie einen Zweckverband oder ein Dienstleistungsunternehmen, zu übertragen.