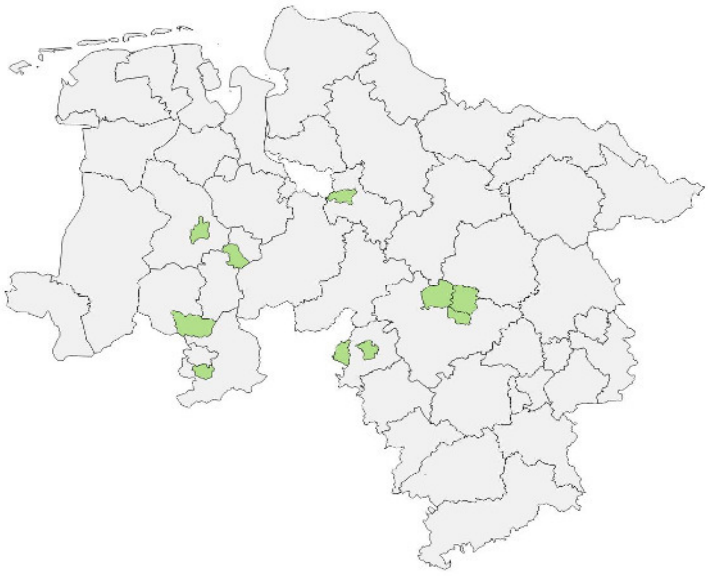
Die Präsidentin des
Niedersächsischen Landesrechnungshofs

– Überörtliche Kommunalprüfung –

Prüfungsmitteilung

Informationssicherheit in Kommunen



Übersandt an:

- Städte Achim, Bramsche, Bückeburg, Burgwedel, Cloppenburg, Georgsmarienhütte, Stadthagen und Vechta sowie Gemeinden Isernhagen und Wedemark
- Landkreise Cloppenburg, Osnabrück, Schaumburg, Vechta und Verden sowie Region Hannover
- Niedersächsisches Ministerium für Inneres und Sport

Hildesheim, 07.03.2018
Az.: 6.2-10712-111/3-17

Niedersachsen

Inhaltsverzeichnis

Anlagenverzeichnis

Abkürzungsverzeichnis

NDSG	Niedersächsisches Datenschutzgesetz
NKomVG	Niedersächsisches Kommunalverfassungsgesetz
TKG	Telekommunikationsgesetz

Quellenhinweis

Die Karte des Deckblattes basiert auf den Geobasisdaten der Niedersächsischen Vermessungs- und Katasterverwaltung aus dem Jahr 2017 © LGLN.

1 Prüfungsanlass und -durchführung

Die Digitalisierung der kommunalen Verwaltungsprozesse ist mit Chancen verbunden, birgt aber auch erhebliche Risiken. Diese haben in der Vergangenheit auch im kommunalen Bereich immer wieder zu materiellen und immateriellen Schäden, zum Beispiel durch Ausfall von IT-Systemen oder durch Verlust von Daten, geführt.[1]

IT-gestützte Prozesse und Systeme müssen daher sicher und zuverlässig funktionieren.

Die drei wesentlichen Schutzziele der Informationssicherheit hierbei sind

- Vertraulichkeit (Zugang zu Informationen nur für Befugte),
- Integrität (Unversehrtheit und Korrektheit von Informationen),
- Verfügbarkeit (Informationen bei Bedarf bereitstellen).

Ein angemessenes, von diesen drei Zielen getragenes Maß an Informationssicherheit herzustellen, stellt die Kommunen angesichts des schnellen technologischen Wandels vor immer größere Herausforderungen.

Vor diesem Hintergrund untersuchte die überörtliche Kommunalprüfung von April bis August 2017 bei zehn Kommunen mit bis zu 33.000 Einwohnern mithilfe eines Fragenkatalogs, wie intensiv sich die geprüften Kommunen mit den Themen Informationssicherheit und Datenschutz im Sinne des NDSG auseinandergesetzt und diese organisatorisch umgesetzt hatten.

Die überörtliche Kommunalprüfung bezog folgende zehn Kommunen in diese Prüfung ein:

Die Städte Achim, Bramsche, Bückeburg, Burgwedel, Cloppenburg, Georgsmarienhütte, Stadthagen und Vechta sowie die Gemeinden Isernhagen und Wedemark.

[1] Vgl. statt vieler, NWZonline vom 15. Februar 2014, Datenverlust in der Finanzabteilung der Gemeinde Ritterhude, wonach infolge eines technischen Defekts aufgrund unzureichender Sicherheitsmaßnahmen mehrere Tausend Datensätze vernichtet worden sind.

Die Prüfung führte die überörtliche Kommunalprüfung wie folgt durch:

Zahlreiche Institutionen und Einrichtungen, wie das Bundesamt für Sicherheit in der Informationstechnik[2], der Deutsche Landkreistag[3], das Netzwerk Informationssicherheit im Mittelstand des Bayerischen IT-Sicherheitscluster e.V.[4] oder die Rechnungshöfe des Bundes und der Länder[5] haben Normen, Standards und Empfehlungen zur Informationssicherheit herausgeben. Aus diesen Normen, Standards und Empfehlungen hat die überörtliche Kommunalprüfung aufgegliedert auf die Themenbereiche

- Informationssicherheitsmanagement,
- Gebäudesicherheit,
- Zugang zu IT-Systemen,
- Auftragsdatenverarbeitung,
- Notfallmaßnahmen,
- Sensibilisierung und Schulung von Mitarbeitern und
- Datenschutzbeauftragte

einen rund 100 Fragen umfassenden Fragenkatalog (vgl. Anlage 1) entwickelt.

Diesen Fragenkatalog beantworteten die Kommunen vor Beginn der örtlichen Erhebungen. Anschließend, während der örtlichen Erhebungen, hat die überörtliche Kommunalprüfung die Antworten der Kommunen mit Hilfe von rund 100 weiteren Fragen in Interviews vertieft. Dabei sichtete sie auch Unterlagen, wie Dienstanweisungen oder Verträge, und hat Gebäude sowie Anlagen in Augenschein genommen.

Die Antworten auf die gestellten Fragen hat die überörtliche Kommunalprüfung in einer Ja-/Nein-Matrix verdichtet, um anschließend für jede Kommune aufgegliedert auf die sieben untersuchten Themenbereiche Quoten ermitteln zu können.

[2] Bundesamt für Sicherheit in der Informationstechnologie, IT-Grundschutz-Kataloge.

[3] Deutscher Landkreistag (Hrsg.), Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, 2014.

[4] Netzwerk Informationssicherheit im Mittelstand des Bayerischen IT-Sicherheitscluster e.V., ISIS12-Handbuch und -Katalog, 2014.

[5] Rechnungshöfe des Bundes und der Länder, Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IuK-Mindestanforderungen 2016), 2016.

Die Quoten stellen dar, wie viele der einzelnen abgefragten Maßnahmen zur Aufrechterhaltung und Erhöhung der Informationssicherheit am Ende der örtlichen Erhebungen bereits umgesetzt waren. Aus den gewonnenen Antworten bzw. Erkenntnissen wurde deutlich, welche Maßnahmen zur Informationssicherheit die Kommunen bereits ergriffen hatten und bei welchen Punkten noch Handlungsbedarf bestand.

Die Prüfung umfasste nicht, einzelne Sicherheitsmaßnahmen auf ihre technische Funktionalität oder Wirksamkeit zu untersuchen. Dies bleibt individuellen fachtechnischen Untersuchungen vorbehalten.

Besondere Aufmerksamkeit widmete die Prüfung den Themen Verfahrensbeschreibungen (vgl. Abschnitt 3.1) und Auftragsdatenverarbeitung (vgl. Abschnitt 3.4).

Für die Betrachtung der Verfahrensbeschreibungen erstellte die überörtliche Kommunalprüfung eine Liste mit Verfahren, mit denen in Kommunen üblicherweise personenbezogene Daten verarbeitet werden. Diese Liste glich die überörtliche Kommunalprüfung mit den in der Kommune tatsächlich eingesetzten Verfahren ab. In einem nächsten Schritt wurde überprüft, ob für die Verfahren, in denen personenbezogene Daten verarbeitet wurden, Verfahrensbeschreibungen vorlagen, die den Anforderungen des § 8 NDSG genügten.

Bei der Auftragsdatenverarbeitung prüfte die überörtliche Kommunalprüfung, ob dort, wo personenbezogene Daten durch Dritte verarbeitet wurden, dies auf der Grundlage eines entsprechenden Vertrags geschah. Es wurde ebenfalls betrachtet, ob sich die Kommunen der Einhaltung der technischen und organisatorischen Maßnahmen nach § 7 NDSG durch die Auftragnehmer versicherten.

Weiterhin erhob die überörtliche Kommunalprüfung, welche Kosten den Kommunen für die Wahrnehmung der Tätigkeit des Datenschutzbeauftragten entstanden (vgl. Abschnitt 3.7) und verglich die Kosten für die Wahrnehmung durch interne Datenschutzbeauftragte mit den Kosten für die Wahrnehmung durch externe Datenschutzbeauftragte. Basis des Vergleichs waren zum einen die intern entstehenden Kosten, die einheitlich nach dem KGSt-Standard „Kosten eines Arbeitsplatzes“[6] aus dem Jahr 2016 ermittelt wurden. Zum anderen waren die Kosten,

[6] Jahreswerte nach KGSt 2016/17; KGSt®-Bericht Nr. 7/2016.

die bei der Wahrnehmung durch einen externen Datenschutzbeauftragten entstanden, Teil des Vergleichs. Zu den Kosten des externen Datenschutzbeauftragten addierte die überörtliche Kommunalprüfung die Kosten des erforderlichen internen Datenschutzkoordinators. Dessen Kosten wurden ebenfalls einheitlich nach dem oben genannten KGSt-Standard ermittelt.

2 Kurzfassung der Prüfungsergebnisse

- Die überörtliche Kommunalprüfung untersuchte 2017 bei zehn Kommunen mit bis zu 33.000 Einwohnern mithilfe 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 die Bereiche Informationssicherheitsmanagement, Gebäudesicherheit, Zugang zu IT-Systemen, Auftragsdatenverarbeitung, Notfallmaßnahmen, Sensibilisierung und Schulung von Mitarbeitern und Datenschutzbeauftragte ab.

- Eine Leitlinie zur Informationssicherheit, in der für alle Mitarbeiter verständlich beschrieben war, welche Sicherheitsziele angestrebt werden und in welchem organisatorischen Rahmen diese umzusetzen sind, hatte zum Zeitpunkt der örtlichen Erhebungen mit der Stadt Georgsmarienhütte nur eine der zehn Kommunen eingeführt.

- Lediglich drei der zehn Kommunen verfügten über einen Notfallplan, der personenunabhängige Abläufe zur Bewältigung von Störungen im IT-Betrieb beschrieb.

- Verfahrensbeschreibungen nach § 8 NDSG, in denen datenverarbeitende Stellen, wie Fachbereiche, ihre Verfahren zur automatisierten Verarbeitung personenbezogener Daten darstellen, lagen nur in zwei Kommunen vollständig vor. In den übrigen acht Kommunen lagen die Verfahrensbeschreibungen nicht für alle Verfahren vor oder die Verfahrensbeschreibungen genügten nicht den Anforderungen des § 8 NDSG.

- IT-gestützte Prozesse und Systeme müssen sicher und zuverlässig funktionieren. Regelmäßige, ereignisunabhängige Tests sind wichtig, um präventiv Schwachstellen zu beseitigen und Risiken zu reduzieren. Nur zwei Kommunen testeten ereignisunabhängig ihre Notfallmaßnahmen.

- In Kommunen mit einem externen Datenschutzbeauftragten waren weniger Verstöße gegen datenschutzrechtliche Regeln festzustellen als in Kommunen mit einem internen Datenschutzbeauftragten.

3 Prüfungsfelder und -feststellungen

3.1 Informationssicherheitsmanagement

Mit Informationssicherheitsmanagement werden die Aufgaben bezeichnet, die erforderlich sind, um Informationssicherheit systematisch aufzubauen und umzusetzen.[7] Ein Informationssicherheitsmanagement ist in die Organisationsstrukturen und Geschäftsprozesse einer Kommune einzubetten. Es ist auf die örtlichen Anforderungen und Bedürfnisse individuell zuzuschneiden und kontinuierlich zu verbessern.[8]

Um eine bestmögliche Unterstützung kommunaler Verwaltungsprozesse durch den Einsatz von Informationstechnik zu erreichen, ist es unter Beachtung des Grundsatzes der Wirtschaftlichkeit (§ 110 Abs. 2 NKomVG) geboten, Rahmenwerke und Strukturen (Informationssicherheitsmanagementsysteme) zu entwickeln und fortlaufend bedarfsgerecht anzupassen.[9] Ein Informationssicherheitsmanagement sollte aus Sicht der überörtlichen Kommunalprüfung unter anderem folgende grundlegende Komponenten umfassen:

- Strategie und Leitlinie
- Verfahrensbeschreibungen
- Sicherungskonzept
- Notfallplan
- Regelung organisatorischer Maßnahmen
- Umgang mit mobilen Geräten/Datenträgern
- Sicherheitsrichtlinie

Mithilfe des Fragenkatalogs sowie einer gesonderten Erhebung zur Prüfung der Verfahrensbeschreibungen prüfte die überörtliche Kommunalprüfung, inwieweit das in den zehn einzelnen Kommunen bestehende Informationssicherheitsmanagement diese Komponenten abdeckte.

[7] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-1, Managementsysteme für Informationssicherheit (ISMS), S. 4.

[8] Deutscher Landkreistag (Hrsg.), Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, 2014, S. 6 ff.

[9] Rechnungshöfe des Bundes und der Länder, Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IuK-Mindestanforderungen 2016), 2016, S. 9.

Die nachstehende Abbildung zeigt, inwieweit die abgefragten Komponenten und -teile (ohne Sonderbetrachtung Verfahrensbeschreibungen) bereits im Informationssicherheitsmanagement der einzelnen Kommunen Berücksichtigung fanden.

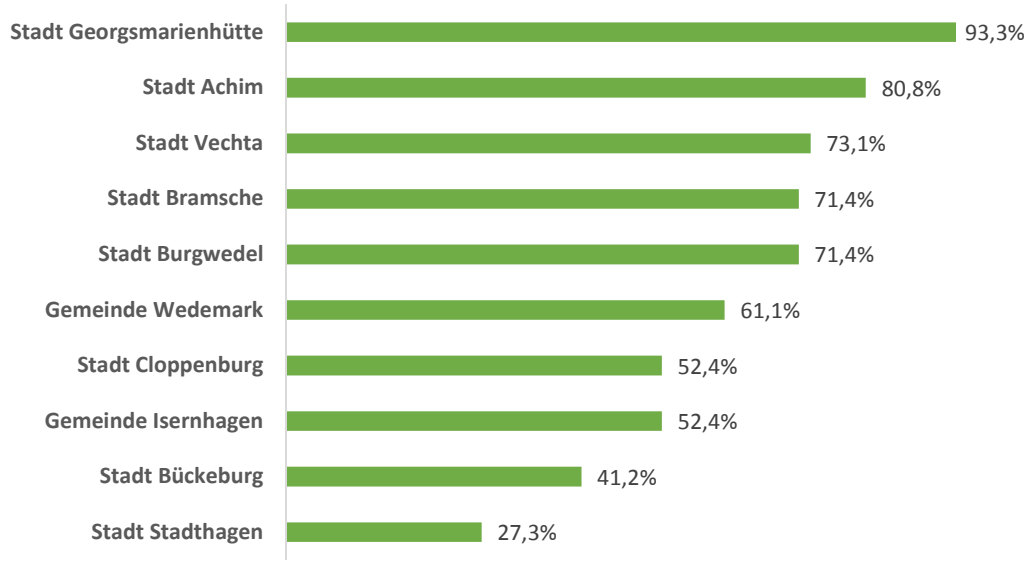


Abbildung 1: Quote Informationssicherheitsmanagement

Eine Leitlinie zur Informationssicherheit stellt die Grundlage zur Einführung eines Informationssicherheits-Managementsystems dar, die den Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit als Ziel festschreibt. In der Leitlinie wird für alle Mitarbeiter der Kommune verständlich beschrieben, welche Sicherheitsziele angestrebt werden und in welchem organisatorischen Rahmen diese umgesetzt werden sollen. Eine Leitlinie zur Informationssicherheit hatte zum Zeitpunkt der örtlichen Erhebungen mit der Stadt Georgsmarienhütte nur eine der zehn Kommunen eingeführt.

Ein Notfallplan legt personenunabhängige Abläufe zur Bewältigung von Störungen im IT-Betrieb fest. Er ist unumgänglich, um bei einem Ausfall von Systemen oder Anwendungen die Ausfallzeiten gering zu halten. Einen umfassenden Notfallplan hatten mit den Städten Achim, Georgsmarienhütte und Vechta nur drei Kommunen erstellt. Einzelne Regelungen, die Bestandteile eines umfassenden Notfallplans sind, lagen in allen Kommunen vor.

Die Kommunen setzten für ihre Aufgabenerledigung Softwarelösungen ein, in denen personenbezogene Daten automatisiert verarbeitet wurden. Sie haben für

diese Verfahren regelmäßig Verfahrensbeschreibungen[10] zu erstellen (§ 8 Satz 1 NDSG), in eine Übersicht (Verfahrensverzeichnis) aufzunehmen und ihrem behördlichen Datenschutzbeauftragten zuzuleiten, § 8 a Abs. 2 Satz 5 NDSG.

Die überörtliche Kommunalprüfung betrachtete in den Kommunen insgesamt 300 Verfahren, mit denen die Kommunen personenbezogene Daten automatisiert verarbeiteten.

Die nachstehende Abbildung zeigt, in welchem Umfang die erforderlichen Verfahrensbeschreibungen mit den nach § 8 NDSG erforderlichen Angaben vorlagen.

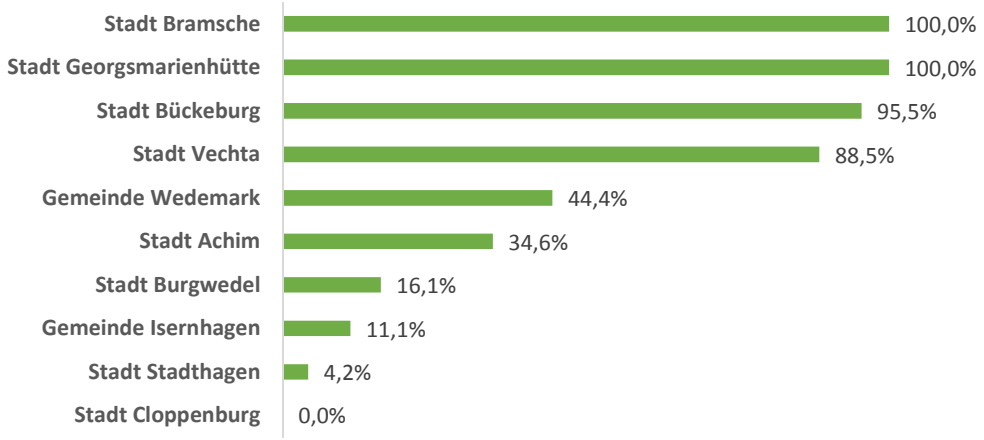


Abbildung 2: Quote Verfahrensbeschreibungen

Nur in zwei Kommunen, bei den Städten Bramsche und Georgsmarienhütte, lagen alle Verfahrensbeschreibungen vollständig vor. In den übrigen acht Kommunen lagen die Verfahrensbeschreibungen nicht für alle Verfahren vor oder die Verfahrensbeschreibungen genügten nicht den Anforderungen des § 8 NDSG. Die Stadt Cloppenburg hatte keine Verfahrensbeschreibungen.

Die Kommunen Achim, Bückeburg, Burgwedel, Cloppenburg, Isernhagen, Stadthagen, Vechta und Wedemark sind verpflichtet, ihre Verfahrensbeschrei-

[10] Ein Muster für eine Verfahrensbeschreibung, die die nach § 8 Satz 1 NDSG erforderlichen Angaben enthält, findet sich in Anlage 1 der Verwaltungsvorschriften zum Niedersächsischen Datenschutzgesetz (VV NDSG), gem. RdErl. des MI, der StK und der übr. Min. vom 26. Juni 2002, Nds. MBl. S. 640.

bungen gemäß § 8 Satz 1 NDSG zu erstellen bzw. zu ergänzen und ihrem behördlichen Datenschutzbeauftragten eine vollständige Übersicht über die automatisierten Verarbeitungen personenbezogener Daten zuzuleiten.

Mit den Städten Bramsche und Vechta ergriffen während dieser Prüfung bereits zwei Kommunen Maßnahmen, um ihr Informationssicherheitsmanagement zu verbessern.

3.2 Gebäudesicherheit

Gebäude schützen die Informationstechnik gegen natürliche Einflüsse oder von Menschen ausgehenden Gefahren. Ihre Art und ihre Beschaffenheit sind wichtige Beiträge zur Aufrechterhaltung und zur Erhöhung der Informationssicherheit.

Maßnahmen im Bereich der Gebäudesicherheit sollen Informationstechnik gegen physische Schäden aufgrund externer Einwirkungen, wie Feuer oder Wasser, sichern. Sie sollen ferner dafür sorgen, dass nur befugte Personen Zutritt zu schützenswerter Informationstechnik und zu vertraulichen Informationen haben. Aufgefächert auf die Bereiche

- Zutrittsmöglichkeiten
- Schlüsselvergabe
- Zusätzliche Schutzmaßnahmen
- Serverraum
- Lieferanten/Externe Dienstleister
- Brandschutzgeräte
- Brandmeldesystem
- Besucher

untersuchte die überörtliche Kommunalprüfung mithilfe des Fragenkatalogs, inwieweit die Kommunen Maßnahmen zur Gebäudesicherheit getroffen hatten.

Es ergab sich folgendes Bild:

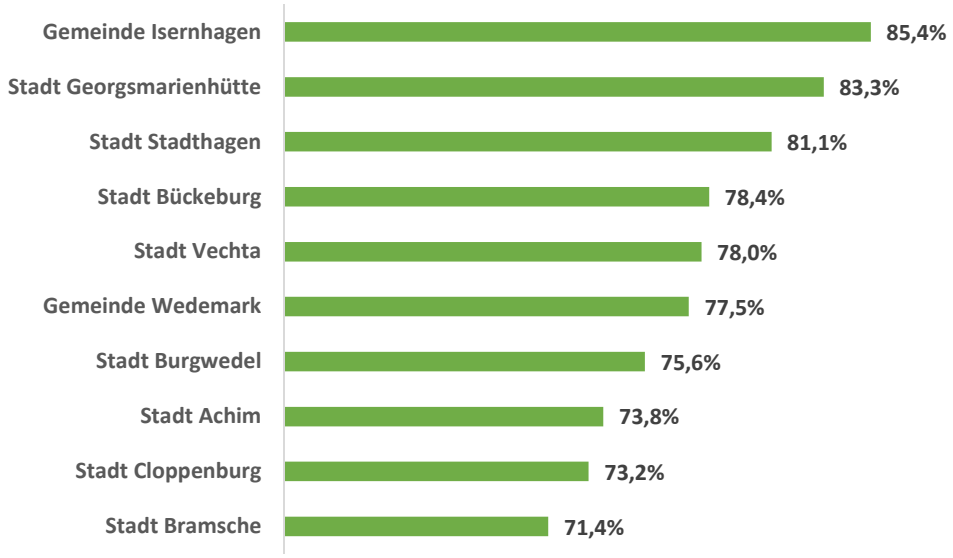


Abbildung 3: Quote Gebäudesicherheit

Für die Informationssicherheit stellt ein ungeregelter Zugang von Besuchern und Lieferanten eine Gefahr dar. Vertrauliche Informationen lassen sich schützen, indem verhindert oder zumindest erschwert wird, dass Gebäude von unbefugten Personen betreten werden.

Alle zehn Kommunen stellten durch angemessene Maßnahmen sicher, dass unbefugte Personen nicht in sensible Bereiche gelangen konnten. Zu den sensiblen Bereichen zählen etwa Räume, in denen schützenswerte informationstechnische Anlagen, beispielsweise Server, betrieben, oder in denen vertrauliche Informationen aufbewahrt werden. Ausnahmslos informierten die Kommunen ihre Mitarbeiter mithilfe von Anweisungen, das oder wie Büroräume beim Verlassen zu sichern sind. Acht Kommunen schützten ihre Gebäude ferner durch sicherheitstechnische Anlagen, wie Alarmanlagen oder Bewegungsmelder.

Es bestanden noch Handlungsbedarfe beim Schutz von Serverräumen. Lediglich fünf Kommunen sicherten ihre Serverräume durch Sicherheitstüren mit Widerstandsklassen. Bei den Kommunen Cloppenburg, Georgsmarienhütte, Isernhagen und Wedemark führten wasserführende Druckleitungen durch Serverräume. Angepasst an die örtlichen Gegebenheiten stellten die Kommunen Cloppenburg, Georgsmarienhütte und Isernhagen durch geeignete bauliche Maßnahmen sicher, dass sich das hieraus ergebende Risiko größtmöglich gemindert wurde. So

sicherte die Gemeinde Isernhagen die wasserführenden Leitungen beispielsweise durch eine zusätzliche Abmauerung in Verbindung mit einem wasserdichten Vorhang und einer Feuchtigkeitsmeldeanlage. Lediglich in der Gemeinde Wedemark waren die Server ungeschützt vor den druckführenden Leitungen.

Die Städte Bramsche, Burgwedel und Stadthagen leiteten bereits während der Prüfung Maßnahmen ein, um die Gebäudesicherheit zu erhöhen.

3.3 Zugang zu IT-Systemen

Erhalten unbefugte Personen Zugang zu IT-Systemen, besteht die Gefahr, dass sie nicht nur auf die eigentlichen Systeme, sondern auch auf die in den Systemen befindlichen Anwendungen und Daten zugreifen und diese manipulieren oder beschädigen können. Manipulationen oder Beschädigungen von IT-Systemen können zu großen Schäden führen.

Zugangs- und Zugriffsbeschränkungen sollen verhindern, dass IT-Systeme unberechtigt benutzt werden. Die nachstehende Abbildung zeigt, in welchem Umfang die Kommunen in den Bereichen

- Passwortsicherheit
- Geräteschutz
- Umgang mit Kennwörtern
- Erzwungener Login
- Manueller Logout
- Bildschirmschoner mit Kennwortabfrage
- Berechtigungen
- Zugriffsvergabe
- Umgang bei zeitweise Beschäftigten
- Systemprotokolle
- Zugriff, Änderung, Löschung
- Verschlüsselung/Signaturverfahren

Zugangs- und Zugriffsberechtigungen als organisatorische Maßnahmen einsetzten, um ihre IT-Systeme vor Zugriffen unbefugter Personen zu schützen:

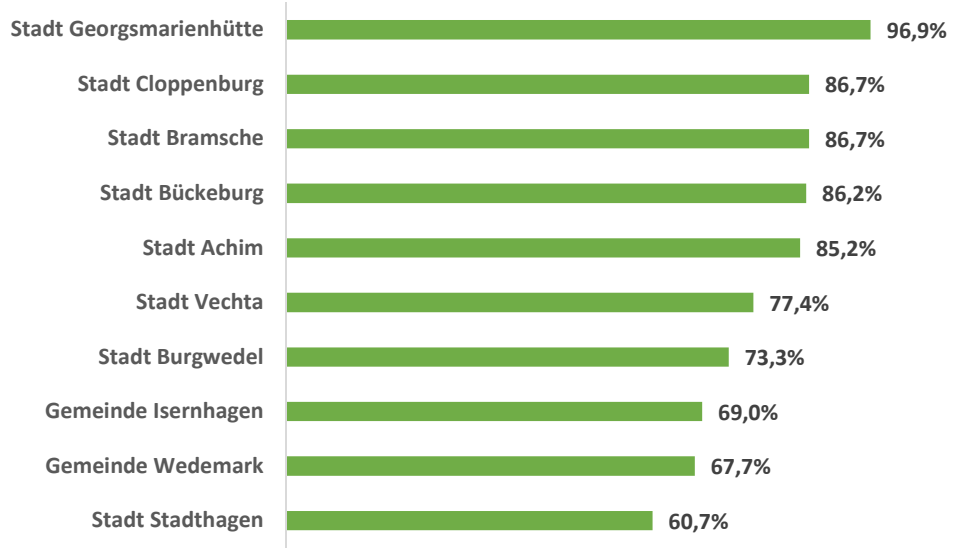


Abbildung 4: Quote Zugang zu IT-Systemen

In allen Kommunen mussten die Mitarbeiter sich an den IT-Systemen mit einem Passwort anmelden. Allerdings hatten nur neun Kommunen in einer Richtlinie festgelegt, wie ein als sicher einzuschätzendes Passwort zu gestalten ist.

In allen Kommunen gab es schriftliche Anweisungen, die IT-Systeme und -Geräte beim Verlassen des Arbeitsplatzes zu sperren oder diese wurden automatisch nach mehreren Minuten Inaktivität gesperrt. Einige Kommunen nutzten eine Kombination beider Möglichkeiten.

Über USB-Schnittstellen können IT-Systeme mit Schadprogrammen infiziert werden oder unbefugte Personen können sich an ungeschützten Systemen innerhalb kurzer Zeit infolge hoher Durchsatzraten mobiler Datenträger große Mengen an Daten aneignen. Acht Kommunen hatten die USB-Schnittstellen ihrer IT-Systeme deaktiviert oder setzten eine Software zur Verwaltung und Kontrolle der USB-Schnittstellen ein. Lediglich in zwei Kommunen konnten USB-Schnittstellen ungesichert genutzt werden.

Die Gemeinde Wedemark konnte bei Änderungen an ihren IT-Systemen nicht nachvollziehen, wer Änderungen vorgenommen hatte. Grund hierfür war, dass ein Administrationskonto von mehreren Mitarbeitern genutzt wurde.

Die überörtliche Kommunalprüfung empfiehlt den Kommunen – soweit noch nicht erfolgt –, geeignete organisatorische und technische Maßnahmen, wie das Aufstellen von Richtlinien für die Bildung von Passwörtern oder für die Nutzung von USB-Schnittstellen und die Einrichtung personenbezogener Administrationskonten, umzusetzen, um unbefugten Personen den Zugang zu ihren IT-Systemen zu erschweren.

Die Städte Bramsche, Stadthagen und Vechta ergriffen bereits während der Prüfung Maßnahmen, um unbefugten Personen den Zugang zu ihren IT-Systemen noch weiter zu erschweren.

3.4 Auftragsdatenverarbeitung

In der kommunalen Praxis werden regelmäßig Aufgaben von öffentlichen Stellen auf andere öffentliche oder nicht-öffentliche Stellen (beauftragte Stelle) übertragen, die mit der Verarbeitung personenbezogener Daten verbunden sind. So hatten beispielsweise einzelne Kommunen die Haltung und die Sicherung von Daten, wie Standesamtsdaten, auf hierauf spezialisierte Dienstleistungsunternehmen übertragen.

Eine Auftragsdatenverarbeitung liegt regelmäßig vor, wenn eine Kommune personenbezogene Daten durch eine von ihr beauftragte Stelle nach ihren Weisungen verarbeiten lässt. Die beauftragte Stelle erwirbt kein Eigentum an den von der Kommune zur Verfügung gestellten Daten. Sie darf keine eigenen Entscheidungen hinsichtlich der Verarbeitung der personenbezogenen Daten treffen. Die beauftragte Stelle wird vollkommen unselbstständig tätig. Verantwortlich für die Einhaltung der Vorschriften des Niedersächsischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz, zum Beispiel des Niedersächsischen Meldegesetzes (NMG) oder des Niedersächsischen Personalvertretungsgesetzes (NPersVG), bleibt allein die Kommune.[11]

Die Auftragsdatenverarbeitung ist abzugrenzen von der Übermittlung personenbezogener Daten nach §§ 11 bis 15 NDSG, bei der beauftragten Stellen Daten zur eigenverantwortlichen Nutzung, zum Beispiel zur Durchführung eines Forschungsauftrags, überlassen werden.

[11] Vgl. Wahlbrink, NDSG Kommentar 2014, § 6, S. 50 f.

Rechtsgrundlage für die Auftragsdatenverarbeitung sind §§ 6 ff. NDSG. Danach haben sich die Kommunen zu vergewissern, dass die beauftragten Stellen die von der Kommune erteilten Weisungen sowie die technischen und organisatorischen Maßnahmen nach § 7 NDSG beachten. Technische und organisatorische Maßnahmen sind alle Maßnahmen, die erforderlich sind, um eine den Vorschriften des Niedersächsischen Datenschutzgesetzes entsprechende Verarbeitung personenbezogener Daten sicherzustellen. Beispiele für technische und organisatorische Maßnahmen sind Zugangs-, Zugriffs- und Verfügbarkeitskontrollen. Der Aufwand für diese Kontrollen und der angestrebte Zweck müssen unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis stehen. Die Vereinbarungen mit den beauftragten Stellen über die Auftragsdatenverarbeitung und die Weisungen zu den Maßnahmen nach § 7 NDSG sind schriftlich festzuhalten.

In einem ersten Schritt wurde nachgefragt, ob die Kommunen personenbezogene Daten im Auftrag durch andere öffentliche oder nicht-öffentliche Stellen verarbeiten ließen. Alle zehn Kommunen hatten andere Stellen mit der Verarbeitung personenbezogener Daten beauftragt.

In einem zweiten Schritt wurde mithilfe des Fragenkatalogs untersucht, ob die Kommunen sich vergewisserten, ob die beauftragten Stellen die Gewähr für die Einhaltung der Maßnahmen nach § 7 NDSG bieten. Ferner betrachtete die überörtliche Kommunalprüfung, ob schriftliche Aufträge vorlagen und ob diese Aufträge Weisungen zu technischen und organisatorischen Maßnahmen nach § 7 NDSG enthielten. Insgesamt untersuchte die überörtliche Kommunalprüfung in den zehn geprüften Kommunen 84 Verfahren, bei denen eine Datenverarbeitung durch Dritte vorlag. Für 43 dieser Verfahren lagen Verträge über eine Auftragsdatenverarbeitung vor.

Zusammengefasst zeigte sich folgendes Bild:

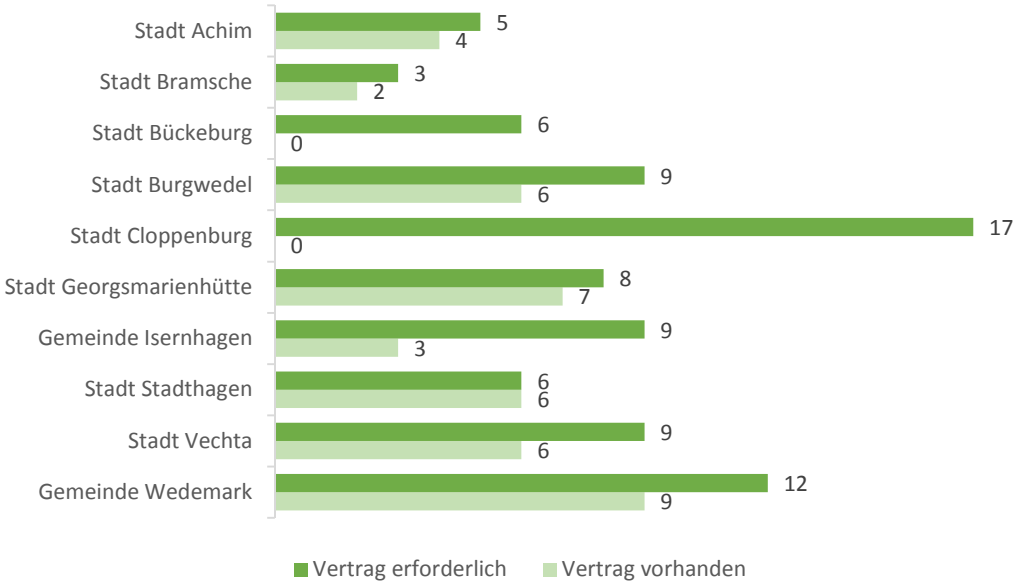


Abbildung 5: Auftragsdatenverarbeitung - Gegenüberstellung erforderliche und vorhandene Verträge

Lediglich die Stadt Stadthagen konnte für jedes Verfahren den entsprechenden Vertrag zur Auftragsdatenverarbeitung vorlegen. Sieben Kommunen konnten nicht für alle Verfahren die entsprechenden Verträge vorlegen. Mit Bückeburg und Cloppenburg konnten im Rahmen dieser Prüfung zwei Kommunen keine schriftlichen Verträge zur Auftragsdatenverarbeitung vorlegen.

Eine Auftragsdatenverarbeitung, die sich nicht auf das Niedersächsische Datenschutzgesetz, auf eine andere Rechtsvorschrift oder auf eine Einwilligung des Betroffenen stützen kann, ist unzulässig, § 4 Abs. 1 NDSG. Deshalb haben die Kommunen, die bisher Aufträge zur Auftragsdatenverarbeitung und Weisungen zur Umsetzung technisch organisatorischer Maßnahmen nach § 7 NDSG nicht schriftlich erteilt haben, dies unverzüglich nachzuholen.

Die Kommunen sollten ferner prüfen, inwieweit die Anforderungen der §§ 6 und 7 NDSG in den bestehenden Verträgen mit den beauftragten Stellen Berücksichtigung gefunden haben.[12] Die Kommunen haben im Rahmen der Auftragsdatenverarbeitung zu kontrollieren, ob die beauftragte Stelle die Weisungen der Kommunen einhält, § 6 Abs. 2 NDSG. Die überörtliche Kommunalprüfung empfiehlt

[12] Hilfestellungen zu datenschutzgerechter Auftragsdatenverarbeitung und zur Ausgestaltung der Verträge mit beauftragten Stellen finden sich beispielsweise auf der Internetseite der Landesbeauftragten für den Datenschutz Niedersachsen (www.lfd.niedersachsen.de) unter Themen/Auftragsdatenverarbeitung.

deshalb den Kommunen, regelmäßig Kontrollen zur Überprüfung der Einhaltung der von der Kommune erteilten Weisungen durchzuführen und zu dokumentieren.

Die Stadt Stadthagen konnte noch während der Prüfung die erforderlichen Verträge zur Auftragsdatenverarbeitung nachreichen.

3.5 Notfallmaßnahmen

IT-gestützte Prozesse und Systeme müssen sicher und zuverlässig funktionieren, da Störungen oder Ausfälle nicht unerhebliche Schäden nach sich ziehen können. Um einen Ausfall von IT-Systemen zu verhindern oder um bei einem Ausfall Schäden zu vermeiden, sind Notfallmaßnahmen zu planen. Meist zeigt sich erst im Fall einer Störung oder eines Ausfalls, ob die geplanten Notfallmaßnahmen greifen. Umso wichtiger ist es, regelmäßig ereignisunabhängige Tests durchzuführen, um präventiv Schwachstellen zu beseitigen.

Die überörtliche Kommunalprüfung prüfte, inwieweit die Kommunen Vorsorge für Notfälle ergriffen hatten und ob sie diese regelmäßig überprüften.

Inwieweit das in den einzelnen zehn Kommunen bestehende Notfallmanagement die Komponenten

- Firewall
- Virenschutz
- WLAN-Einsatz
- Technik
- Online-Datensicherung
- Recovery-Tests
- IT-Sicherheitsbeauftragter
- Unterbrechungsfreie Stromversorgung
- Überwachung/Monitoring
- Risikoanalyse
- Notfalltest

abdeckte, zeigt nachstehende Abbildung:

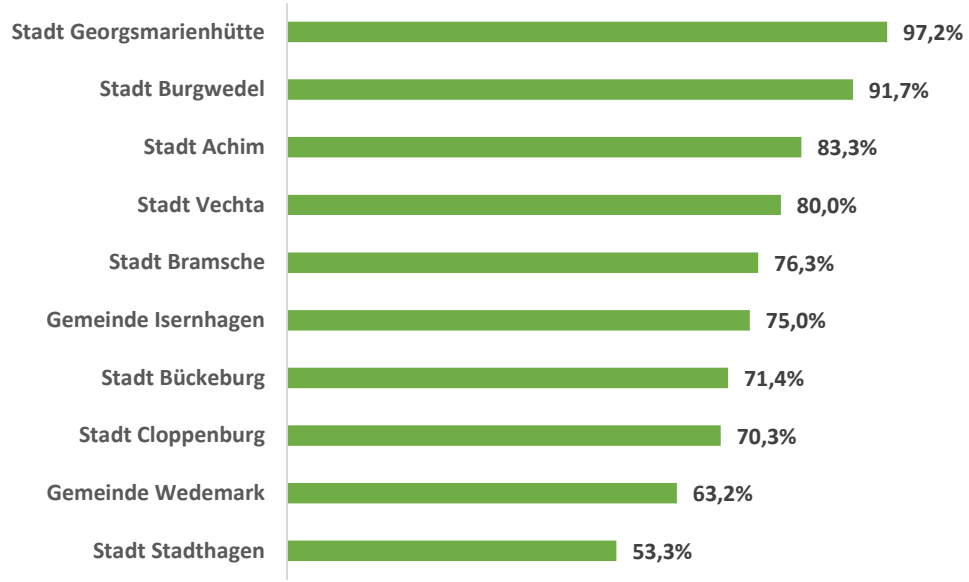


Abbildung 6: Quote Notfallmaßnahmen

Eine Firewall überprüft alle Daten, die das eigene interne Netzwerk (Intranet) verlassen oder aus einem externen Netzwerk (Internet) in das interne Netzwerk hineinwollen. Mit einer Firewall lässt sich der ein- und ausgehende Datenfluss kontrollieren und protokollieren, sperren oder freigeben. Alle geprüften Kommunen setzten eine Firewall ein, um die eigenen IT-Systeme vor Angriffen von außen zu schützen.

Eine unterbrechungsfreie Stromversorgung (USV) garantiert einerseits bei Netzausfall einen ununterbrochenen Betrieb der IT-Systeme und -Geräte und ermöglicht andererseits eine rechtzeitige Reaktion, wie eine Benachrichtigung eines Verantwortlichen oder ein geordnetes Herunterfahren eines elektronischen Systems ohne Datenverluste. Alle Kommunen dieser Prüfung verfügten über eine unterbrechungsfreie Stromversorgung und sicherten sich auf diese Weise gegen das Risiko eines Datenverlusts im Falle eines Stromausfalls ab.

Um die Wirksamkeit von Notfallmaßnahmen zu überprüfen, müssen diese ereignisunabhängig getestet werden. Nur zwei Kommunen testeten ereignisunabhängig ihre Notfallmaßnahmen.

Die überörtliche Kommunalprüfung empfiehlt allen Kommunen, ihre bestehenden Maßnahmen zur Notfallvorsorge zu überprüfen und erforderlichenfalls zu ergänzen, um (präventiv) Störungen und damit Schäden durch den Ausfall von Informationstechniken oder den Verlust von Daten zu vermeiden.

Die Städte Cloppenburg und Vechta ergriffen bereits während der Prüfung Maßnahmen, um ihr Notfallmanagement zu verbessern.

3.6 Sensibilisierung und Schulung von Mitarbeitern

Für den Schutz personenbezogener Daten reicht es regelmäßig nicht aus, sich auf technische Lösungen zu beschränken. Häufig stellen fehlende Kenntnisse oder mangelndes Problembewusstsein einzelner Mitarbeiter ein Risiko dar. Die Mitarbeiter benötigen die Fähigkeit, datenschutzrelevante Sachverhalte zu erkennen und schnell und kompetent darauf zu reagieren. Zu einem aktiven Bestandteil des Arbeitsalltags werden Datenschutz und -sicherheit nur dann, wenn alle Mitarbeiter über alle Hierarchieebenen einbezogen werden. Eine hohe Sicherheit lässt sich nur erreichen und halten, wenn Mitarbeiter regelmäßig für die Themen Datenschutz und -sicherheit sowie Fernmelde- und Datengeheimnis sensibilisiert werden.

Mithilfe des Fragenkatalogs wurden in diesem Prüffeld folgende Bereiche eingehender untersucht:

- Schulungen zu Datenschutz und -sicherheit
- Fernmelde- und Datengeheimnis
- Mitarbeiterwechsel
- Anzahl Schulungen

Die Auswertung dieser Bereiche zeigt zusammengefasst folgendes Bild:

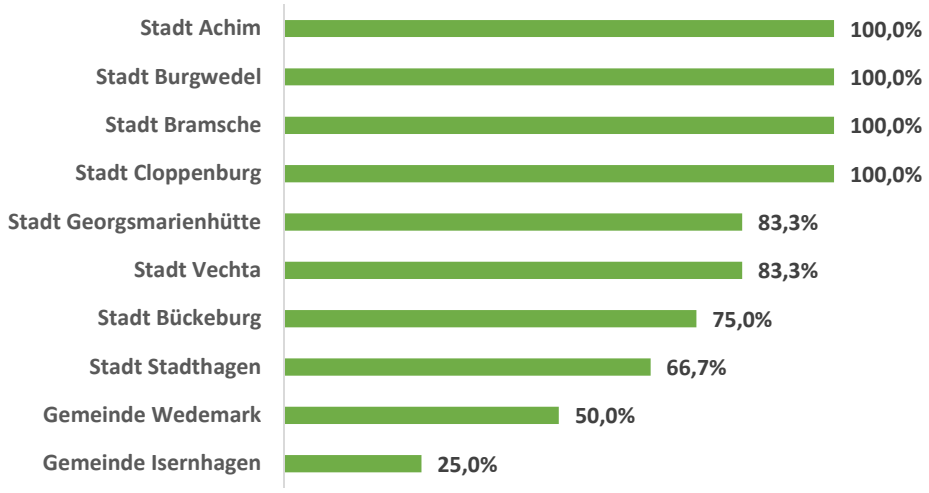


Abbildung 7: Quote Sensibilisierung und Schulung von Mitarbeitern

Gestattet eine Kommune ihren Mitarbeitern die private Nutzung kommunaler Kommunikationsanlagen, beispielsweise Telefon, E-Mail oder Internet, wird die Kommune zu einem sogenannten Diensteanbieter im Sinne des § 3 Nr. 6 TKG.[13] Die Kommune unterliegt damit den Pflichten des § 88 TKG. Danach fällt der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, unter das Fernmeldegeheimnis. Verpflichtet sind nicht nur Diensteanbieter selbst, sondern auch deren Mitarbeiter, die aufgrund ihrer Tätigkeit und Aufgabenstellung an der Erbringung der Telekommunikationsdienste mitwirken. Vom Fernmeldegeheimnis umfasst sind dabei nicht nur Telefonate und Telefaxe, sondern grundsätzlich auch die Internetverbindungen und die E-Mail-Kommunikation. Den betroffenen Mitarbeitern ist es insofern untersagt, sich über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen oder solche Informationen an Dritte weiterzugeben.

Die Gemeinden Isernhagen und Wedemark, die ihren Mitarbeitern die private Nutzung kommunaler Kommunikationsanlagen gestatteten, aber ihre Mitarbeiter mit Zugriff auf Verbindungsdaten, wie IT-Administratoren, nicht nach § 88 TKG

[13] Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Stand Januar 2016, Ziffer 2 b.

verpflichteten, haben dies nachzuholen. Die Städte Achim, Bramsche, Bückeburg und Stadthagen hatten die private Nutzung der dienstlichen Kommunikationsanlagen ausdrücklich untersagt.

§ 5 NDSG verpflichtet alle Personen mit dienstlichem Zugang zu personenbezogen Daten, diese Daten nur zu dienstlichen Zwecken zu verwenden. Alle kommunalen Mitarbeiter unterliegen bereits kraft Gesetz dem Datengeheimnis nach § 5 NDSG, sodass es grundsätzlich keiner besonderen Verpflichtung der Mitarbeiter auf § 5 NDSG bedarf. Da erfahrungsgemäß vielen Mitarbeitern diese Regelung nicht präsent ist, empfiehlt die Landesbeauftragte für den Datenschutz, die Mitarbeiter im Rahmen einer förmlichen Verpflichtung nach dem Verpflichtungsgesetz auch auf § 5 NDSG zu verweisen. Mit Ausnahme der Gemeinde Isernhagen folgten alle Kommunen dieser Empfehlung der Landesbeauftragten für den Datenschutz.

Alle Mitarbeiter sollten regelmäßig und systematisch zu Sicherheitsrisiken informiert und für Fragen der Informationssicherheit sensibilisiert werden. Solche Informationen können Hinweise auf Verhaltensfehler, Informationen über aktuelle Bedrohungen oder erkannte Schwachstellen sein. Die Informationsverbreitung kann beispielsweise per E-Mail, über ein vorhandenes Intranet oder das „Schwarze Brett“ geschehen.

Acht Kommunen informierten ihre Mitarbeiter regelmäßig über akute, den Datenschutz und die -sicherheit betreffende Gefahren. Die Gemeinde Wedemark sowie die Stadt Stadthagen sollten ebenfalls eine Informationsroutine etablieren und alle Mitarbeiter über aktuelle Bedrohungen informieren beziehungsweise alle Mitarbeiter unterrichten, woran sie eine Bedrohung erkennen und wie sie sich in einem solchen Fall zu verhalten haben.

Spezielle Schulungen zu den Themen Datenschutz und -sicherheit führten nur die Gemeinde Wedemark sowie die Städte Achim, Burgwedel, Cloppenburg und Georgsmarienhütte durch.

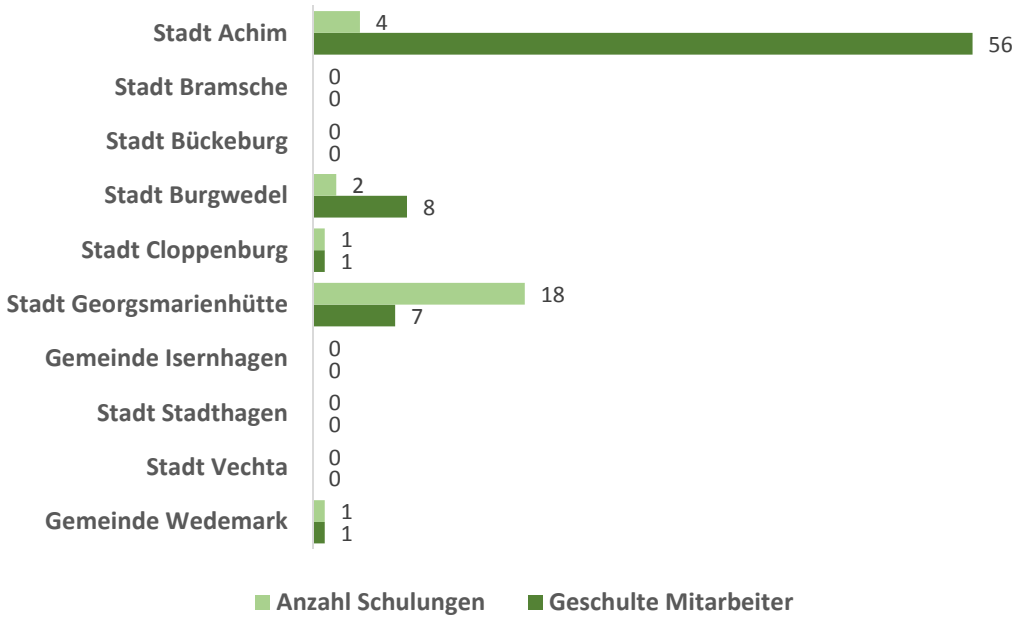


Abbildung 8: Anzahl durchgeführter Schulungen und Anzahl geschulter Mitarbeiter

Insgesamt schulten diese fünf Kommunen 73 Mitarbeiter in 26 Schulungen. Beachtenswert sind die unterschiedlichen Ansätze der Städte Achim und Georgsmarienhütte:

Während die Stadt Achim in vier Schulungen 56 Mitarbeiter schulte und somit auf eine flächendeckende Information und Sensibilisierung setzte, legte die Stadt Georgsmarienhütte den Schwerpunkt auf eine intensive Schulung ihrer IT-Mitarbeiter. Hier nahmen sieben Mitarbeiter an 18 Schulungen teil. Diese wirkten anschließend als Multiplikatoren.

Unabhängig vom gewählten Ansatz ist festzustellen, dass diese beiden Kommunen diejenigen mit den geringsten Handlungsbedarfen waren (vgl. Abschnitt 3.7).

Die überörtliche Kommunalprüfung empfiehlt allen Kommunen, ihre Mitarbeiter noch stärker für die Themen Informationssicherheit und Datenschutz zu sensibilisieren und zu diesen Themen bedarfsgerecht zu schulen. Permanente neue technologische und organisatorische Entwicklungen, die neben Verbesserungen

möglicherweise auch neue, zuvor nicht bekannte Risiken hervorbringen können, erfordern es, die Mitarbeiter regelmäßig über Änderungen und etwaige daraus resultierende Risiken zu unterrichten. Mitarbeiterschulungen sollten deshalb nicht nur einmalig, sondern regelmäßig in sinnvollen Abständen und zusätzlich anlassbezogen, zum Beispiel bei einem Arbeitsplatzwechsel eines Mitarbeiters, durchgeführt werden.

Mit den Städten Bramsche, Burgwedel, Cloppenburg, Georgsmarienhütte und Vechta ergriffen fünf Kommunen bereits während der Prüfung Maßnahmen, um ihre Mitarbeiter noch stärker zu sensibilisieren und noch besser zu schulen.

3.7 Datenschutzbeauftragte

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 S. 2 NDSG.

Datenschutzbeauftragte unterstützen die Kommunen bei der Sicherstellung des Datenschutzes. Sie haben auf die Einhaltung der datenschutzrechtlichen Vorschriften hinzuwirken. Datenschutzbeauftragte sind in der Ausübung ihrer Funktion weisungsfrei. Als Datenschutzbeauftragte dürfen Kommunen nur Personen bestellen, die die notwendige Sachkenntnis auf den Gebieten der Datenverarbeitung, der behördlichen Organisation und der einschlägigen Rechtsvorschriften haben sowie die erforderliche Zuverlässigkeit besitzen. Ferner dürfen Kommunen als Datenschutzbeauftragte nur Personen bestellen, die durch die Bestellung keinen Interessenkonflikten mit anderen dienstlichen Aufgaben ausgesetzt sind, § 8 a Abs. 2 NDSG.

Die überörtliche Kommunalprüfung prüfte, ob die Kommunen für den Datenschutz Beauftragte bestellt hatten. Die überörtliche Kommunalprüfung fragte die Beauftragten ergänzend, ob sie zusätzliche Schulungsbedarfe haben, ob ihnen für ihre Aufgaben ausreichende zeitliche und finanzielle Ressourcen zur Verfügung standen und ob möglicherweise Interessenkonflikte mit ihren übrigen in der Kommune wahrzunehmenden Aufgaben bestanden.

Zusammengefasst zeigte sich folgendes Bild:

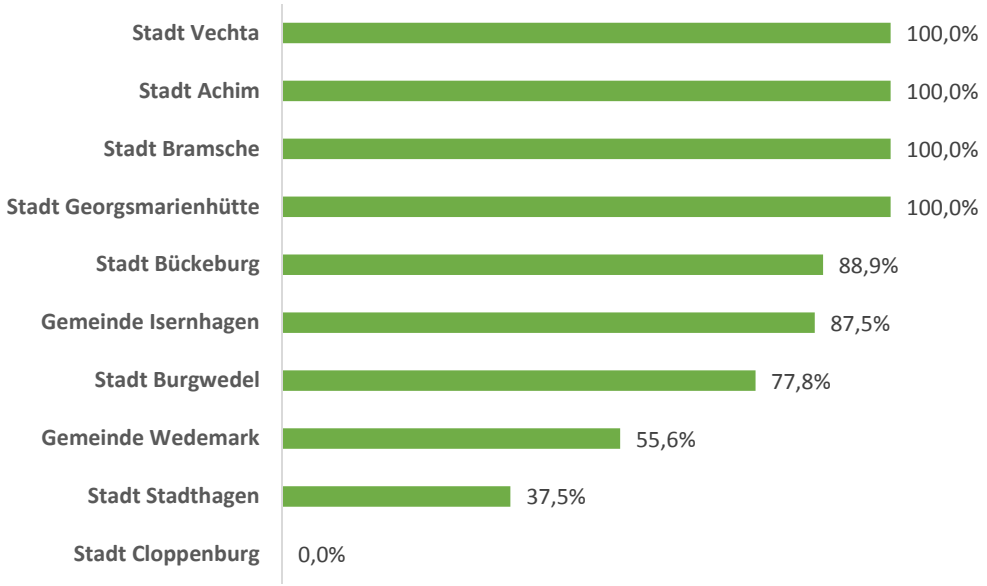


Abbildung 9: Quote Datenschutzbeauftragter

Die Kommunen Bramsche, Cloppenburg, Stadthagen und Wedemark hatten sich zum Zeitpunkt der Prüfung entschieden, die Aufgabe des Datenschutzbeauftragten durch eigene Mitarbeiter wahrnehmen zu lassen. In den übrigen sechs Kommunen waren Externe mit der Aufgabenwahrnehmung betraut.

Bei der Stadt Cloppenburg war zum Prüfungszeitpunkt keine Datenschutzbeauftragte bestellt. Die Datenschutzbeauftragte hatte die Stadtverwaltung zum 01.04.2017 verlassen. Seit Oktober 2017 nimmt eine neu eingestellte Juristin die Aufgabe wahr.

Die Kommunen haben die Beauftragten für den Datenschutz bei der Aufgabenerfüllung zu unterstützen, § 8 a Abs. 2 Satz 6 NDSG. Sie haben deshalb den Datenschutzbeauftragten angemessene zeitliche und finanzielle Ressourcen zur Verfügung zu stellen, damit diese ihre Aufgaben wirksam ausüben können.[14]

Ein interner Datenschutzbeauftragter gab an, weiteren Schulungsbedarf zu haben. Eine fachliche Schulung war bisher nicht wahrgenommen worden.

[14] Der Landesbeauftragte für den Datenschutz Niedersachsen (Hrsg.), Das Niedersächsische Datenschutzgesetz, Gesetzestext und Kommentar, 2014, S. 70; vgl. hierzu auch Die Landesbeauftragte für den Datenschutz Niedersachsen (Hrsg.) 22. Tätigkeitsbericht 2013 bis 2014, Hannover, 2015, S. 56.

In zwei Fällen schätzten die Datenschutzbeauftragten ihre zeitlichen und finanziellen Ressourcen als nicht ausreichend für ihre Tätigkeit ein. Die internen Datenschutzbeauftragten schätzten den zeitlichen Umfang ihrer Datenschutztätigkeit im Mittel auf wöchentlich ca. 4 Stunden ein. Auffällig ist hierbei der auf lediglich 0,4 Stunden geschätzte zeitliche Umfang bei der Stadt Stadthagen.

Erforderlich ist weiterhin, dass Kommunen die Empfehlungen ihrer Datenschutzbeauftragten zügiger umsetzen. Die überörtliche Kommunalprüfung stellte bei der Prüfung vereinzelt Handlungsfelder zur Verbesserung des Datenschutzes fest, die die Datenschutzbeauftragten bereits vor längerer Zeit identifiziert und in ihren Berichten kommuniziert hatten, die in den Kommunen aber weiterhin unbearbeitet waren. Beispielsweise wurden im Datenschutzbericht der Stadt Vechta fehlende Netzwerk- und Notfallpläne in den Rubriken „Umsetzungsstand“ und „Zeitplanung“ mit der Formulierung: „nach wie vor in Bearbeitung“ und „erneut verlängert auf IV/2016“ angemahnt. Zum Zeitpunkt dieser Prüfung lagen die geforderten Unterlagen immer noch nicht vor. Die Stadt hat diese Unterlagen erst nach Beendigung der örtlichen Erhebung der überörtlichen Kommunalprüfung nachgereicht. Der externe Datenschutzbeauftragte der Stadt Bückeburg mahnte im Januar 2017 die fehlenden Verträge zur Auftragsdatenverarbeitung mit hoher Priorität an. Zum Zeitpunkt der Prüfung durch die überörtliche Kommunalprüfung im August 2017 war dieser Mangel noch nicht abgestellt.

Positiv festzustellen war, dass es allen Kommunen mit einem internen Datenschutzbeauftragten gelungen war, Datenschutzbeauftrage zu bestellen, deren sonstige Tätigkeiten nicht zu Interessenkonflikten führten. Dies wäre beispielsweise der Fall, wenn sie in ihrer Haupttätigkeit als Beschäftigte im IT- oder Personalbereich ebenfalls mit der Verarbeitung personenbezogener Daten befasst wären. Grundsätzlich sollten daher Mitarbeiter, die zum Beispiel bei ihren sonstigen Aufgaben ändernd in IT-Verfahren eingreifen können oder mit der Verarbeitung personenbezogenen Daten befasst sind, deshalb nicht als Datenschutzbeauftragte bestellt werden.

Anhand des Fragebogens, den Antworten der Kommunen und den Untersuchungen vor Ort stellte die überörtliche Kommunalprüfung fest, an welchen Stellen noch Handlungsbedarfe bestanden beziehungsweise bestehen:

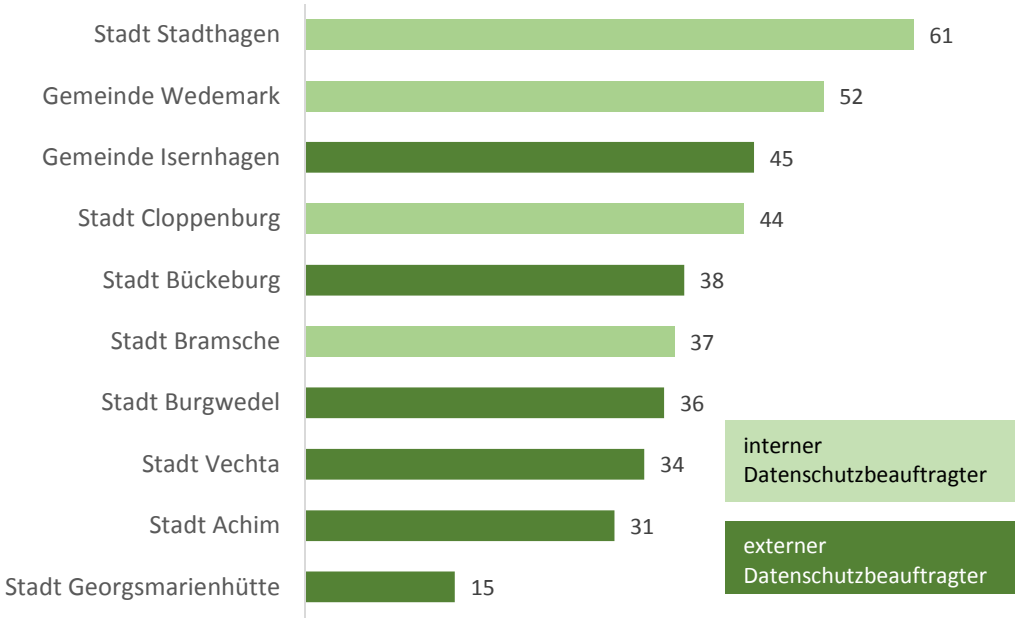


Abbildung 10: Handlungsbedarfe in den Kommunen

Über alle Kommunen stellte die überörtliche Kommunalprüfung im Mittel 39,3 Handlungsbedarfe fest.

In den Kommunen, in denen ein interner Datenschutzbeauftragter bestellt war, stellte die überörtliche Kommunalprüfung im Mittel eine um 34 % höhere Anzahl an Handlungsbedarfen fest, als in den Kommunen, in denen ein externer Datenschutzbeauftragter bestellt war.

Auffällig bei der Analyse ist die Stadt Stadthagen. Sie weist mit 61 Feststellungen die größte Zahl an Handlungsbedarfen auf. Damit weicht die Kommune 36 % vom Durchschnitt aller geprüften Kommunen ab. Vor dem Hintergrund des oben aufgezeigten geringen Zeitanteils für die Tätigkeit des Datenschutzbeauftragten bei der Stadt Stadthagen von 0,4 Stunden wöchentlich, empfiehlt die überörtliche Kommunalprüfung detailliert zu untersuchen, ob hier ein unmittelbarer Zusammenhang besteht und ob gegebenenfalls der Zeitanteil aufzustocken ist.

Zusammenfassend empfiehlt die überörtliche Kommunalprüfung den Kommunen zu prüfen, ob sie die teils komplexen, aufgrund der schnellen technologischen

Entwicklungen einem permanenten Wandel unterliegenden Aufgaben des Datenschutzes allein noch ordnungsgemäß wahrnehmen können. Vor allem kleinere Kommunen sollten für sich prüfen, 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. So könnten sich beispielsweise mehrere öffentliche Stellen einen Datenschutzbeauftragten teilen, solange dieser bei allen Stellen seinen Aufgaben als Datenschutzbeauftragter ausreichend nachkommen kann.

Denkbar ist im Bereich des Datenschutzes zum Beispiel eine interkommunale Zusammenarbeit. So hat die Stadt Georgsmarienhütte den Datenschutzbeauftragten der Stadt Bramsche im Jahr 2011 im Rahmen einer interkommunalen Zusammenarbeit auch zum Datenschutzbeauftragten der Stadt Georgsmarienhütte berufen. Der Datenschutzbeauftragte ist Bediensteter der Stadt Bramsche. Die Abrechnung für die Dienstleistung des Datenschutzbeauftragten für die Stadt Georgsmarienhütte erfolgt analog zur Erstattung von Aufwendungen gemäß der öffentlich-rechtlichen Vereinbarung über die gemeinsame Durchführung von Aufgaben der Rechnungsprüfung zwischen beiden Städten und wird jährlich nach tatsächlichem Aufwand abgerechnet.

Neben den festgestellten Unterschieden bei den Handlungsbedarfen untersuchte die überörtliche Kommunalprüfung weiterhin, ob die – in dieser Prüfung – zu besseren Ergebnissen führende Zusammenarbeit mit externen Datenschutzbeauftragten mit höheren Kosten verbunden war.

Hierfür erhob die überörtliche Kommunalprüfung die Eingruppierung und die zur Verfügung stehenden Zeitanteile der internen Datenschutzbeauftragten und ermittelte die jährlichen Kosten einheitlich nach dem KGSt-Standard „Kosten eines Arbeitsplatzes“[15] aus dem Jahr 2016.

Dem stellte die überörtliche Kommunalprüfung die Kosten gegenüber, die den Kommunen für die externen Datenschutzbeauftragten entstanden. Hierfür sah die überörtliche Kommunalprüfung die Verträge mit den Dienstanbietern und Rechnungen aus dem Jahr 2016 ein.

[15] Jahreswerte nach KGSt 2016/17; KGSt®-Bericht Nr. 7/2016.

Um einen angemessenen Vergleich herbeizuführen, addierte die überörtliche Kommunalprüfung zu den originären Kosten für die externen Datenschutzbeauftragten die in den Kommunen zudem anfallenden Kosten für Datenschutzkoordinatoren, die als Bindeglied zwischen Verwaltung und externem Datenschutzbeauftragten tätig sind.

Die Kosten der Datenschutzkoordinatoren ermittelte die überörtliche Kommunalprüfung gleichfalls wie die Kosten der internen Datenschutzbeauftragten nach dem KGST-Standard „Kosten eines Arbeitsplatzes“ aus dem Jahr 2016.

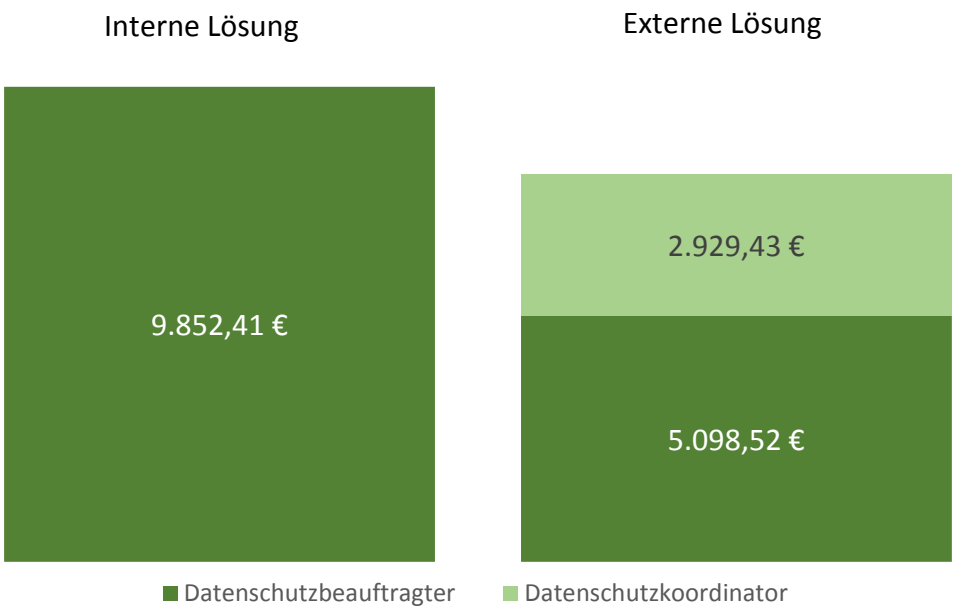


Abbildung 11: Jährliche Kosten für Datenschutzbeauftragte und -koordinatoren

Die überörtliche Kommunalprüfung stellte fest, dass die Aufwendungen bei der internen Wahrnehmung der Tätigkeit des behördlichen Datenschutzbeauftragten im Mittel bei gerundet 9.900 € lagen.

Demgegenüber wendeten Kommunen für die externe Wahrnehmung der Tätigkeit des behördlichen Datenschutzbeauftragen im Mittel gerundet nur 8.000 € auf, mithin etwa 18 % weniger.

Hieraus wird deutlich, dass die Hinzuziehung externen Sachverstands nicht zwingend mit höheren Aufwendungen einhergeht, sondern gegebenenfalls sogar die wirtschaftlichere Lösung darstellen kann.

4 Fazit und Empfehlungen

Informationssicherheit und Datenschutz nehmen mit zunehmender Digitalisierung einen immer höheren Stellenwert ein.

Die Ergebnisse dieser Prüfung können keine vollständige, abschließende Bestandsaufnahme zur Informationssicherheit einzelner Kommunen darstellen. Sie zeigen aber zusammengefasst, dass die Kommunen dem Thema Informationssicherheit einen noch höheren Stellenwert beimessen sollten. Vielfach sind vor allem organisatorische Maßnahmen zur Verbesserung der Informationssicherheit, wie die Sensibilisierung und Schulung von Mitarbeitern über bestehende Regelungen zur Risikominderung, zu ergreifen.

Maßnahmen zur Aufrechterhaltung und Erhöhung der Informationssicherheit können mit erheblichen Aufwendungen verbunden sein. Die Kommunen haben fortlaufend etwaige bestehende Risiken zu ermitteln und je nach ihrer Größe, ihrer Organisation, ihrem Sicherungsbedürfnis und ihrem finanziellen Handlungsrahmen abzuwägen, welche Maßnahmen in welcher Reihenfolge zu ergreifen sind. Werden Prioritäten falsch gesetzt und kommt es infolge dessen zu Schadensfällen, können die Aufwendungen um ein Vielfaches höher sein.

Aufgrund dieser Prüfungserkenntnisse empfiehlt die überörtliche Kommunalprüfung den Kommunen – soweit nicht bereits umgesetzt – unter Beachtung des Grundsatzes der Wirtschaftlichkeit

- Rahmenwerke und Richtlinien zur Informationssicherheit und zum Datenschutz zu entwickeln oder zu erweitern und fortlaufend anzupassen,
- mittelfristig ein an die Größe ihrer Kommune angepasstes Informationssicherheitsmanagementsystem 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 Datenverlust zu vermeiden,
- ihre Mitarbeiter noch stärker für die Themen Informationssicherheit und Datenschutz zu sensibilisieren und sie zu diesen Themen bedarfsgerecht zu schulen,

- zu prüfen, ob die häufig komplexen, einem fortlaufenden Wandel unterliegenden Aufgaben des Datenschutzes und der -sicherheit allein noch ordnungsgemäß abgebildet werden können, 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.
- bei der Beantwortung der Frage, inwieweit sich die Kommune für eine interne oder externe Wahrnehmung der Aufgaben des Datenschutzbeauftragten entscheidet, auch die Kostenseite in die Entscheidung mit einzubeziehen.

Sechs von zehn Kommunen wiesen bis zum Abschluss der örtlichen Erhebungen im August 2017 darauf hin, dass sie während der Erhebungen festgestellte Handlungsbedarfe bereits umgesetzt hatten oder im Begriff waren, diese umzusetzen. Der Mehrzahl der Kommunen war es somit möglich, einzelne Maßnahmen zur Verbesserung ihrer Informationssicherheit unmittelbar umzusetzen. Die übrigen Kommunen sollten ebenfalls prüfen, welche Maßnahmen kurzfristig umgesetzt werden können und welche Maßnahmen einer Vorbereitung bedürfen, um sie mittel- bis langfristig umsetzen zu können.

5 Stellungnahmen der Kommunen

Die Kommunen hatten bis zum 31. Januar 2018 Gelegenheit, zum Entwurf dieser Prüfungsmitteilung Stellung zu nehmen (§ 4 Abs. 1 Satz 3 NKPG).

Sechs von zehn Kommunen haben diese Gelegenheit genutzt.

In ihren Stellungnahmen führten die Kommunen detailliert aus, welche Maßnahmen sie zur Verbesserung der Informationssicherheit und des Datenschutzes aufgrund der identifizierten Handlungsfelder bereits erarbeitet und umgesetzt haben und welche noch geplant werden. So teilte eine Kommune mit, dass sie nunmehr einen externen Datenschutzbeauftragten berufen wolle. Zwei Kommunen informierten über inzwischen abgeschlossene Verträge zur Auftragsdatenverarbeitung. Eine Kommune kündigte den Umbau ihres Serverraums an, eine andere teilte die Anschaffung eines Programms zur Erstellung und Verwaltung von Verfahrensbeschreibungen mit.

Durchweg zeigten die eingegangen Stellungnahmen, dass sich die Kommunen aufgrund der Prüfungsergebnisse intensiv mit ihrer Informationssicherheit auseinandergesetzt, bestehende Handlungsbedarfe zielgerichtet abgestellt oder Maßnahmen hierzu ergriffen haben.

Im Auftrag

S t i e g e

Prüfgebiet	Prüfpunkt	Fragen
Informationssicherheitsmanagement		
	Strategie und Leitlinie	Gibt es eine behördenspezifische Leitlinie zur Informationssicherheit?
	Verfahrensverzeichnis	Gibt es für die zur Verarbeitung personenbezogener Daten eingesetzten IT-Anwendungen eine Verfahrensbeschreibung (§ 8 NDSG)?
	Sicherungskonzept	Gibt es ein dokumentiertes IT-Sicherungskonzept?
	Notfallplan	Existiert ein schriftlicher Notfallplan?
		Sind Netzwerkübersichten der eingesetzten Techniken und Systeme dokumentiert?
		Gibt es eine Leitungsübersicht (interne Verkabelung und externe Leitungen, inkl. Beschreibung der Patchfeld-Systematiken)?
		Gibt es eine Übersicht über externe Zulieferer (Strom, Wasser, Telekommunikation, Datenleitungen, Hardware, Software etc. mit Ansprechpartnern, Rufnummern, (Rahmen-) Vertragsdaten,
		Wird Ihre Hardware ganz oder teilweise durch Dritte betrieben oder betreut?
		Gibt es eine Übersicht über externe Dienstleister (z.B. für Installation, Wartung, Konfiguration, Support, Fehlerbehebung etc. mit Ansprechpartnern, Rufnummern,
		Gibt es ein Verzeichnis der im Einsatz befindlichen Hard- und Software sowohl für Server als auch für Arbeitsplätze?
		Gibt es eine Übersicht über auf den Geräten installierte Standardsoftware und darüber hinaus installierte Zusatzsoftware?
		Gibt es eine Klassifizierung der eingesetzten Systeme und Verfahren nach Dringlichkeit für eine Wiederherstellung?
	Regelung organisatorischer Maßnahmen	Bestehen Regelungen zur Nutzung des E-Mail-Accounts / Webzugangs zu geschäftlichen / privaten Zwecken?
		Gibt es Vertretungszugriffe statt Passwortweitergabe?
		Ist die Entsorgung von Daten in Papierform oder auf elektronischen Medien geregelt?
		Gibt es Anweisungen zum Verhalten bei Datenpannen und Sicherheitsverstößen?
	Umgang mit mobilen Geräten / Datenträgern	Sind bei dienstlichen Smartphones zusätzliche Sicherheitssperren aktiv? (z.B. PIN / Password! Keine Gesten, da zu unsicher.)
		Ist die Meldepflicht bei Verlust von mobilen Geräten bekannt gemacht worden?
	Sicherheitsrichtlinie	Ist den Mitarbeitern neben den detaillierten Richtlinien und Anweisungen eine zusammenfassende Sicherheitsrichtlinie bekannt gemacht worden?
Gebäudesicherheit		
	Zutrittsmöglichkeiten	Bleiben Türen zu Bereichen, die nicht dem Publikumsverkehr dienen, konsequent verschlossen?
	Besucher	Ist sichergestellt, dass Personen nicht in sensible Bereiche wie Verwaltung, IT oder Personal gelangen?
		Gibt es Anweisungen für Mitarbeiter, worauf sie zu achten haben und wie mit auffälligen Personen umzugehen ist?
	Schlüsselvergabe	Sind Ausgabe, Rücknahme, Tausch und Ersatz von Schlüsseln, Code-Karten, PINs nachvollziehbar dokumentiert und existieren hierfür feste Verfahrensweisen?
	Zusätzliche Schutzmaßnahmen	Gibt es besondere Gebäudesicherheitsmaßnahmen (Alarmsysteme etc.)?
	Serverraum	Gibt es gesonderte Serverräume?
		Ist sichergestellt, dass Netzwerkverteiler/Patch-Schränke stets verschlossen sind und nur ein beschränkter Mitarbeiterkreis Zugang hat?
		Ist sichergestellt, dass Serverschränke stets verschlossen sind und nur ein beschränkter Mitarbeiterkreis Zugang hat?
	Lieferanten/ Externe Dienstleister	Werden die getroffenen Schutzmaßnahmen bei Anlieferung und Abholung durch Dritte nicht unterbrochen?
		Dürfen sich Lieferanten und externe Dienstleister nur unter Aufsicht in den höheren Sicherheitszonen, z.B. nicht-öffentlichen Bereichen, bewegen?
		Werden die Identität des Externen und die Richtigkeit des Auftrags vor Zugriff auf Informationen (unabhängig ob elektronisch oder in Papierform) überprüft?
		Werden Zugriffe durch oder Übergaben an Dritte protokolliert?
	Brandschutzgeräte	Existieren Brandschutzgeräte im IT-Bereich / Serverraum?
		Sind Mitarbeiter in die Brandbekämpfung eingewiesen oder dafür speziell ausgebildet?
	Brandmeldesystem	Sind Brandmelder vorhanden?
		Ist die automatisierte Benachrichtigung der richtigen Ansprechpartner im Falle eines Auslösens sichergestellt?

Zugang zu IT-Systemen	
Passwortsicherheit	Muss ein Nutzer sowohl beim Login an seinem PC-Arbeitsplatz als auch in den einzelnen Verfahren ein sicheres Passwort eingeben?
Geräteschutz	Ist die Bootreihenfolge auf der Festplatte als erstes Medium eingestellt?
	Ist die Auswahl der Bootreihenfolge beim Systemstart abgeschaltet?
	Ist ein BIOS-Passwort gesetzt?
	Ist ein Schutz vor Gehäuseöffnung eingerichtet bzw. Warnmeldung aktiviert?
	Sind externe Anschlüsse z. B. USB-Ports, Kartenleser und Laufwerke grundsätzlich deaktiviert oder werden diese verwaltet?
Umgang mit Kennwörtern	Existieren personenbezogene Administrations-Accounts zwecks Nachvollziehbarkeit?
	Wird der eigentliche Administrations-Account „Admin“ nur im Notfall genutzt?
	Werden voreingestellte Admin-Passwörter (Auslieferungszustand) direkt bei der ersten Nutzung geändert?
	Sind alle wichtigen Kennwörter in einem besonders geschützten Passwortcontainer abgelegt
Erzwungener Login	Ist ohne Anmeldedaten ein System-Login oder der Zugriff auf relevante Verfahren ausgeschlossen?
Manueller Logout	Sind alle Mitarbeiter angewiesen, sich bei Verlassen des Arbeitsplatzes (auch für kurze Zeit) manuell vom System abzumelden?
Bildschirmschoner mit Kennwortabfrage	Startet nach spätestens 10 Minuten der Bildschirmschoner mit Kennwortabfrage automatisch?
Verschlüsselung / Signaturverfahren	Sind Dateien, Verzeichnisse und Laufwerke mit schutzbedürftigen Daten nach dem aktuellen Stand der Technik verschlüsselt?
	Kommen bei elektronischer Übertragung von Daten entsprechende Signatur- und Verschlüsselungsverfahren zum Einsatz?
Berechtigungen	Existieren Gruppen, mittels derer Nutzer ihre Zugriffsrechte zugeteilt bekommen?
	Wird auf die Nutzung von Einzelberechtigungen weitestgehend verzichtet?
	Wird das Berechtigungskonzept regelmäßig auf Aktualität überprüft?
Zugriffsvergabe	Gibt es festgeschriebene Anlässe aufgrund derer Zugriffsrechte vergeben und entzogen werden
Umgang bei zeitweisen Beschäftigungen	Ist der Rechteentzug für zeitweise Beschäftigungsverhältnisse oder bei Ausscheiden geregelt?
Systemprotokolle	Ist bekannt, welche Systemprotokolle aktiviert sind und was konkret aufgezeichnet wird (Login, Logout, Fehlversuche, Sicherheitsverstöße etc.)?
	Ist geregelt, was beim Feststellen von Verstößen konkret erfolgt?
Zugriff, Änderung, Löschung	Kann in den Systemen und Verfahren die datenschutzkonforme Protokollierung von Zugriffen auf Daten, deren Änderung und Löschung sichergestellt werden?
Auftragsdatenverarbeitung durch Externe	
Technische und organisatorische Maßnahmen	Werden personenbezogene Daten ganz oder teilweise durch Dritte verarbeitet?
Vereinbarung zur Auftragsdatenverarbeitung	Wurde eine der aktuellen Rechtslage entsprechende Vereinbarung mit dem Dienstleister vor Aufnahme der Zusammenarbeit geschlossen?
Notfallmaßnahmen	
Firewall	Wird eine dem Stand der Technik entsprechende Firewall-Lösung zum Schutz vor Zugriffen von außen eingesetzt?
Virenschutz	Werden Mitarbeiter über außerordentliche, aktuelle Bedrohungen informiert?
WLAN	Werden Rechner bzw. Endgeräte über WLAN eingebunden?
Technik	Ist mittels der eingesetzten Sicherungstechnik eine zeitnahe Datenwiederherstellung möglich?
	Bei Sicherung auf Wechselmedien: Werden diese regelmäßig ausgetauscht, um Ausfällen vorzubeugen?
Online Datensicherung	Wird eine Online-Datensicherung durchgeführt?
Recovery-Tests	Werden regelmäßig (mind. alle 3-6 Monate) Überprüfungen der Backups auf Funktionsfähigkeit durchgeführt?
IT-Sicherheitsbeauftragter	Existiert ein IT-Sicherheitsbeauftragter?
Unterbrechungsfreie Stromversorgung	Sind die Systeme vor Stromausfällen mittels unterbrechungsfreier Stromversorgung gesichert?
Überwachung / Monitoring	Sind im IT-Bereich Monitoring Systeme installiert?
	Werden bei Alarm SMS oder E-Mail Nachrichten an vorbestimmte Empfänger versendet?
Risikoanalyse	Wurde analysiert, welche Risiken die Funktionsfähigkeit der Systeme bedrohen?
	Wurden Verfahren in kritische und weniger kritische Systeme klassifiziert?
	Wurde die maximal tolerierbare Ausfallzeit von Systemen und Verfahren festgelegt?
	Wurde innerhalb der vergangenen 12 Monate eine Risikoanalyse durchgeführt?
Notfalltest	Werden die Notfallmaßnahmen regelmäßig getestet und mit den Mitarbeitern Notfallübungen abgehalten?

Sensibilisierung und Schulung von Mitarbeitern

Sensibilierung	Werden Mitarbeiter für die Themen Datenschutz und Datensicherheit sensibilisiert?
	Wie viele Schulungen zu den Themen Datenschutz und Datensicherheit wurden 2016 hausintern durchgeführt?
	Wie viele Mitarbeiter wurden zu den Themen Datenschutz und Datensicherheit 2016 hausintern geschult?
	Wie viele Schulungen zu den Themen Datenschutz und Datensicherheit wurden 2016 extern durchgeführt?
	Wie viele Mitarbeiter wurden zu den Themen Datenschutz und Datensicherheit 2016 extern geschult?
Daten- und Fernmeldegeheimnis	Sind nachweislich alle Mitarbeiter schriftlich auf das Datengeheimnis nach § 5 NDSG verpflichtet worden?
	Wurden Mitarbeiter mit Außenkontakt (Bürgerbüro, Telefonzentrale, Ansprechpartner für Bürger etc.) sowie Mitarbeiter mit regelmäßigem Zugriff auf Verbindungsdaten (z.B. IT-Mitarbeiter) auf

Datenschutzbeauftragter

Bestellung	Wurde ein Datenschutzbeauftragter bestellt?
Ausgliederung	Wird die Aufgabe des Datenschutzbeauftragen von einem externen Anbieter wahrgenommen?

Kommune	Stadt Georgsmarienhütte

Zeilenbeschriftungen	relevante Aspekte	berücksichtigte Aspekte	in %	Durchschnitt aller Kommunen in %
Informationssicherheitsmanagement	**30**	**28**	**93,33%**	**64,57%**
Notfallplan	13	13	100,00%	64,21%
Regelung organisatorischer Maßnahmen	5	5	100,00%	74,42%
Sicherheitsrichtlinie	1	1	100,00%	20,00%
Sicherungskonzept	5	5	100,00%	71,43%
Strategie und Leitlinie	4	2	50,00%	15,38%
Umgang mit mobilen Geräten / Datenträgern	2	2	100,00%	85,00%
Gebäudesicherheit	**42**	**35**	**83,33%**	**77,72%**
Besucher	2	2	100,00%	55,00%
Brandmeldesystem	3	3	100,00%	93,33%
Brandschutzgeräte	5	5	100,00%	94,00%
Lieferanten/ Externe Dienstleister	4	4	100,00%	100,00%
Schlüsselvergabe	1	1	100,00%	100,00%
Serverraum	19	13	68,42%	75,27%
Zusätzliche Schutzmaßnahmen	6	5	83,33%	50,00%
Zutrittsmöglichkeiten	2	2	100,00%	72,22%
Zugang zu IT-Systemen	**32**	**31**	**96,88%**	**79,12%**
Berechtigungen	3	3	100,00%	86,67%
Bildschirmschoner mit Kennwortabfrage	1	1	100,00%	70,00%
Erzwungener Login	1	1	100,00%	100,00%
Geräteschutz	5	5	100,00%	78,26%
Manueller Logout	2	2	100,00%	90,00%
Passwortsicherheit	4	4	100,00%	94,87%
Systemprotokolle	4	4	100,00%	54,29%
Umgang bei zeitweisen Beschäftigungen	1	1	100,00%	90,00%
Umgang mit Kennwörtern	4	4	100,00%	97,50%
Verschlüsselung / Signaturverfahren	3	2	66,67%	56,52%
Zugriff, Änderung, Löschung	2	2	100,00%	28,57%
Zugriffsvergabe	2	2	100,00%	85,00%
Notfallmaßnahmen	**36**	**35**	**97,22%**	**76,52%**
Firewall	2	2	100,00%	95,00%
IT-Sicherheitsbeauftragter	1	0	0,00%	28,57%
Notfalltest	1	1	100,00%	20,00%
Online Datensicherung			entfällt	0,00%
Recovery-Tests	5	5	100,00%	86,36%
Risikoanalyse	4	4	100,00%	30,00%
Technik	5	5	100,00%	98,00%
Überwachung / Monitoring	10	10	100,00%	77,55%
Unterbrechungsfreie Stromversorgung	5	5	100,00%	83,33%
Virenschutz	3	3	100,00%	100,00%
WLAN	0	0	entfällt	87,50%
Sensibilisierung und Schulung von Mitarbeitern	**6**	**5**	**83,33%**	**81,25%**
Daten- und Fernmeldegeheimnis	4	4	100,00%	90,32%
Sensibilierung	2	1	50,00%	64,71%
Datenschutzbeauftragter	**8**	**8**	**100,00%**	**81,01%**
Bestellung	2	2	100,00%	94,74%
Fachkunde	1	1	100,00%	88,89%
Interessenkonflikte	1	1	100,00%	100,00%
Kosten	0	0	entfällt	57,14%
Ressourcen	1	1	100,00%	77,78%
Tätigkeit	3	3	100,00%	69,23%
Gesamtergebnis	**154**	**142**	**92,21%**	**75,94%**