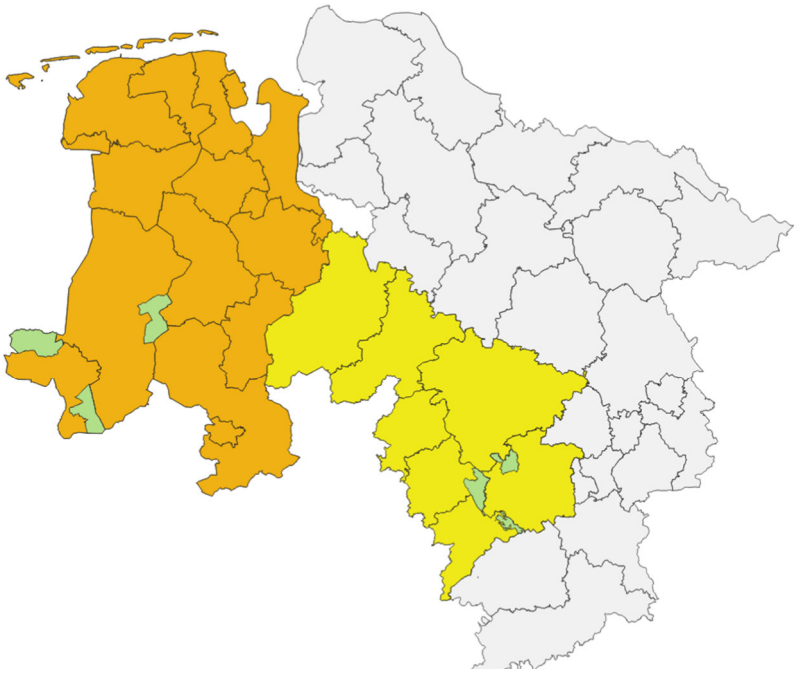
Die Präsidentin des
Niedersächsischen Landesrechnungshofs

- Überörtliche Kommunalprüfung -

Prüfungsmitteilung

Prüfungsreihe Informationssicherheit
Vertiefungsthema Notfallmanagement



Übersandt an

- Flecken Delligsen
  Flecken Salzhemmendorf
  Gemeinde Nordstemmen
  Samtgemeinde Emlichheim
  Samtgemeinde Herzlake
  Samtgemeinde Schüttorf
- deren Kommunalaufsichtsbehörden

Hildesheim, 27.04.2022

Az.: 10712/6.2-2/2021

Niedersachsen

Inhaltsverzeichnis

Abbildungsverzeichnis

Anlagenverzeichnis

Anlage 1	Fragenkatalog der überörtlichen Kommunalprüfung
Anlage 2	Berechnung Ausfallkosten Personal

Quellenhinweis

Die Karte des Deckblattes basiert auf den Geodaten des Landesamtes für Geoinformation und Landesvermessung Niedersachsen, *©2021* LGLN

1 Prüfungsanlass und Durchführung der Prüfung

Tz. 1 Die überörtliche Kommunalprüfung verfolgt bereits seit mehreren Jahren einen Prüfungsschwerpunkt in den Bereichen Informationstechnologie, Informationssicherheit und Datenschutz. Ziel dieser Prüfungen war und ist es, die Kommunen für die vorgenannten Bereiche zu sensibilisieren, sowohl wiederholt auftretende Schwachstellen aber auch Good Practice Lösungen zu identifizieren und letztlich über den Kommunalbericht zu veröffentlichen. Die bisher durchgeführten Prüfungen[1] zeigten auf, dass es für die Kommunen eine große Herausforderung darstellt, ein IT-Sicherheitsniveau herzustellen, welches alle Schutz- und Gewährleistungsziele der Informationssicherheit und des Datenschutzes[2] erfüllt. In den geprüften Kommunen bestand in allen Prüfungsfeldern ein wesentlicher Nachhol- bzw. Handlungsbedarf. Die Stellungnahmen der Kommunen zu den durchgeführten Prüfungen bestätigten die hohe Praxisrelevanz.

Tz. 2 Cyberattacken und Cyberkriminalität haben auch gegenüber Kommunen zugenommen. Durch Trojaner wurden bundesweit bereits etliche Verwaltungen teils für Wochen bis zur Arbeitsunfähigkeit hin beeinträchtigt. Nach einer Recherche des Bayerischen Rundfunks gemeinsam mit "Zeit online" aus dem Jahr 2021 betraf dies in den vergangenen sechs Jahren mehr als 100 Behörden, Kommunalverwaltungen und andere öffentliche Stellen.[3] Bei der Beantwortung einer kleinen Anfrage führt die niedersächsische Landesregierung im September 2021 aus, dass Ransomware[4] nutzende Cyberkriminelle bei der Auswahl ihrer Opfer nicht nach den Kategorien Verwaltung, Wirtschaft oder kritischen Infrastrukturen unterscheiden, sondern nach leicht anzugreifenden sowie kurz- bis mittelfristig finanziell lohnenden Zielen.[5] Dabei

---

1 Die Präsidentin des Niedersächsischen Landesrechnungshofs: IT-Sicherheit in Kommunen (Az.: 6.2-10712-111/3-16, Kommunalbericht 2017, Kapitel 5.10); Informationssicherheit in Kommunen (Az.: 6.2-10712-111/3-17, Kommunalbericht 2018, Kapitel 5.7); Verzeichnis von Verarbeitungstätigkeiten und Auftragsverarbeitung (Az.: 10712/6.2-3-2018/2, Kommunalbericht 2019, Kapitel 5.8); Informationssicherheitsmanagementsysteme und Sensibilisierung von Mitarbeiterinnen und Mitarbeitern (Az.: 6.2-10712-111/4-19, Kommunalbericht 2020, Kapitel 5.4).

2
- Vertraulichkeit (Zugang zu Informationen nur für Befugte),
- Integrität (Unversehrtheit und Korrektheit von Informationen),
- Verfügbarkeit (Informationen bei Bedarf bereitstellen),
- Transparenz (Ein Verfahren erfüllt prüfbar die datenschutzrechtlichen Anforderungen),
- Nichtverkettbarkeit (Daten dürfen nur für einen bestimmten Zweck verwendet werden),
- Intervenierbarkeit (ein personenbezogenes Verfahren muss geändert werden können).

3 Bayerischer Rundfunk, Zahlreiche Fälle von digitaler Erpressung in deutschen Behörden, 29.06.2021. https://www.br.de/nachrichten/deutschland-welt/hacker-angriffe-digitale-erpressung-in-deutschen-behoerden,SbduLPs
Siehe dazu auch das Interview des Deutschlandfunk Kultur mit Vera Linß aus dem BR-Rechercheteam: Wenn Hacker die Hochzeit verhindern, 03.07.2021 (Text und Audio-Beitrag, ca. 10 min.).
https://www.deutschlandfunkkultur.de/erpressung-von-behoerden-wenn-hacker-die-hochzeit-verhindern-100.html.

4 Ransomware ist Schadsoftware, die den Zugriff auf Daten einer Organisation verhindern kann, indem sie sie verschlüsselt. Die kriminellen Betreiber verlangen üblicherweise Geld, um den Zugang zu den Daten wiederherzustellen.

5 Kleine Anfrage zur kurzfristigen schriftlichen Beantwortung gemäß § 46 Abs. 2 GO LT mit Antwort der Landesregierung, Drucksache 18/9951.

steht die Cyberattacke auf die Stadtverwaltung Neustadt am Rübenberge beispielhaft für eine neue Dimension der Bedrohung. Vor Ort bedeutete der Trojanerbefall analoges Arbeiten, Improvisieren und Verschieben.[6] Die Verwaltung benötigte Monate, bis der Großteil wieder im Normalbetrieb arbeiten konnte. Insgesamt wurden 500.000 Daten verschlüsselt, die nicht mehr verfügbar waren.[7] Allein die ungeplanten Mehrausgaben für den IT-Neuaufbau wurden auf 100.000 bis 150.000 Euro geschätzt.

Tz. 3 Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) werden in Einzelfällen bis zu achtstellige Lösegelder gefordert.[8]

Tz. 4 Cyberkriminelle und potentielle Angriffsziele befinden sich hinsichtlich der technischen Einwirkungsmöglichkeiten einerseits und der technischen aber auch organisatorischen Abwehrmaßnahmen andererseits in einem Wettlauf. Für die Kommunen ergibt sich damit zwingend die Notwendigkeit, den Schutz von Computernetzwerken und Daten fortwährend zu verbessern und die Beschäftigten bestmöglich zu sensibilisieren und zu schulen.

1.1 Prüfungsgegenstand und -systematik

Tz. 5 Die steigenden Anforderungen an die IT-Sicherheit stellen insbesondere kleinere Kommunen vor große Herausforderungen. Dies gilt auch für die Zielsetzung, ein Mindestniveau in der Informationssicherheit zu erreichen. Die überörtliche Kommunalprüfung unterstützt mit ihren Erkenntnissen die Kommunen bei der Umsetzung der notwendigen Maßnahmen und gibt gerade kleinen Kommunen nützliche Orientierung.

Tz. 6 Für die Absicherung der IT-Infrastruktur sowie der Prozesse speziell in Kommunalverwaltungen hat die Arbeitsgruppe „Modernisierung IT-Grundschutz“, an der Vertreterinnen und Vertreter aus Kommunen und Zweckverbänden teilgenommen haben, bereits 2018 mit Unterstützung durch die kommunalen Spitzenverbände das

---

6 Hannoversche Allgemeine Zeitung, 12.9.2019.

7 https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Neustadt-spuert-noch-immer-Folgen-von-Cyberangrif,neustadt336.html, aufgerufen am 06.01.2021.

8 Was Emotet anrichtet – und welche Lehren die Opfer daraus ziehen; https://www.heise.de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html, aufgerufen am 25.02.2021.

IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung erstellt. Dieses Profil definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umgesetzt werden sollten, um sich nach Einschätzung der Arbeitsgruppe nicht des Vorwurfs eines grob fahrlässigen Verstoßes gegen die Grundsätze des rechtmäßigen Verwaltungshandelns nach Art. 20 Abs. 3 Grundgesetz (GG) auszusetzen.[9]

Tz. 7 Für die Beurteilung eines ganzheitlichen Mindestsicherheitsniveau in der Informationssicherheit hat die überörtliche Kommunalprüfung auf Grundlage des o.g. IT-Grundschutz-Profils, insbesondere die BSI Standards 200-1 bis 200-4[10] sowie das Informations-Sicherheitsmanagement Systems in 12 Schritten (ISIS12)[11,12] herangezogen.

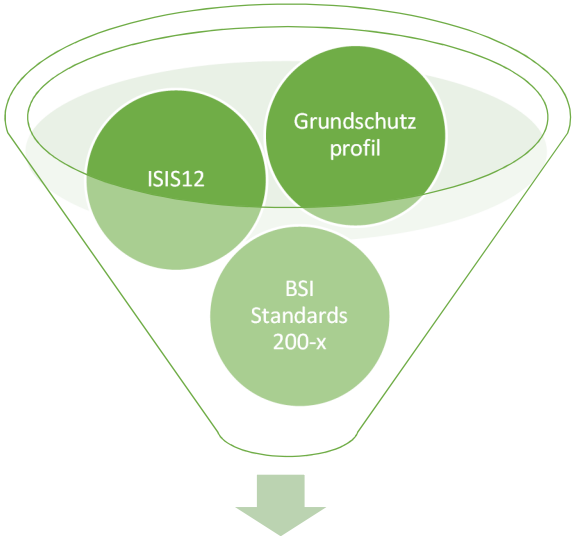


Abbildung 1 - Grundlagen des Fragenkatalogs der überörtlichen Kommunalprüfung

Tz. 8 Nach Sichtung und Würdigung der o.g. Standards (Tz. 7) hat die überörtliche Kommunalprüfung einen Fragenkatalog zum IT-Basis Check (Anlage 1) mit folgenden für die Kommunen relevanten Prüffeldern erarbeitet:

- Sicherheitsmanagement

---

9 Arbeitsgruppe „Modernisierung IT-Grundschutz“, IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, 2019, S. 4 ff.

10 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html.

11. www.isis12.de.

12. Die ISIS12 Vorgehensweise orientiert sich sehr stark an der BSI-Grundschutzmethodik; http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/16_Sitzung/05_Gutachten%20ISIS12.pdf?__blob=publicationFile&v=2.

- Konzeption und Vorgehensweise
- Infrastruktur
- Zugang zu IT-Systemen
- Notfallmaßnahmen
- Datenschutz-Grundverordnung (DSGVO)
- Schulungen und Sensibilisierungen der Beschäftigten

Tz. 9 Anhand der Antworten der geprüften Kommunen stellte die überörtliche Kommunalprüfung fest, in welchen der Prüffelder zur IT-Sicherheit noch Handlungsbedarfe bestanden. Diese Handlungsbedarfe wurden jeder Kommune bereits unmittelbar im Anschluss an die Erhebungen mitgeteilt. Den Kommunen war es somit möglich, einzelne Maßnahmen zur Verbesserung ihrer IT-Sicherheit unmittelbar nach Abschluss der Erhebungen umzusetzen.

Tz. 10 Der ausgefüllte und durch die überörtliche Kommunalprüfung ausgewertete Fragenkatalog, aus dem sich sämtliche Handlungsbedarfe ergeben, ist für jede einzelne Kommune jeweils als Anlage 1 beigefügt.

Tz. 11 Mit der vorliegenden Prüfung wurde aus dem Prüfgebiet Sicherheitsmanagement das Themenfeld Notfallmanagement (auch bekannt als Business Continuity Management) vertieft. Bei der Prüfung des Notfallmanagements ging die überörtliche Kommunalprüfung der Frage nach, inwieweit die Kommunen sich z. B. durch Pläne auf Notfälle und Krisen vorbereitet haben, damit die wichtigsten Geschäftsprozesse bei Ausfall oder auch nur kurzfristigen Unterbrechungen der IT-Infrastruktur zeitnah wiederaufgenommen werden können. Ziel der Kommunen muss sein, Schäden durch Notfälle oder Krisen sowohl in materieller als auch in immaterieller Hinsicht zu minimieren und die Aufgabenerledigung auch bei einem größeren Schadensereignis zu sichern.

Tz. 12 Ziel dieser Prüfung war nicht, vorgefundene Schutzmaßnahmen der einzelnen Bereiche auf ihre technische Funktionalität oder Wirksamkeit hin zu untersuchen. Dies bleibt fachtechnischen Untersuchungen vor Ort vorbehalten.[13]

Vorbemerkung zur Auswahl der geprüften Stellen

Tz. 13 Die Auswahl der Kommunen für diese Prüfung berücksichtigte vorrangig den für den Kommunalbericht 2022 vorgesehenen besonderen regionalen Schwerpunkt. Es sollten unter regionalen Aspekten besonders die statistischen Gebiete (NUTS-Ebenen 2) Hannover[14] und Weser-Ems[15] betrachtet werden. Diese Gebiete verfügen über eine hohe Anzahl von Kommunen mit einer zufriedenstellenden Finanz- und Verwaltungskraft. Es handelt sich um die beiden wirtschaftsstärkeren Regionen Niedersachsens, trotz des Gegensatzes von städtischer Struktur einerseits und ländlicher Prägung andererseits. Mit der regional abgegrenzten Betrachtung will die überörtliche Kommunalprüfung die höhere Vergleichbarkeit der Prüfungsergebnisse unterstützen, um den Kommunen ihre Standortbestimmung im differenzierten Vergleich zu erleichtern.

Tz. 14 Sofern die entscheidenden Prüfungskriterien nicht dagegensprachen, war diese regionale Betrachtung auch maßgeblich für die Auswahl der zu prüfenden Kommunen bei den für den Kommunalbericht 2022 vorgesehenen Prüfungen.

Tz. 15 Der Kommunalbericht 2023 und die für diesen Bericht vorgesehenen Prüfungsergebnisse werden sich schwerpunktmäßig mit den anderen beiden statistischen Gebieten Braunschweig[16] und Lüneburg[17] befassen. Damit wird sich für die Kommunalberichte 2022 und 2023 eine detaillierte Betrachtung des „westlichen“ und „östlichen“ Niedersachsens ergeben.

---

13 Solche Tests und Überprüfungen erfolgen durch die Kommune selbst oder beauftragte Dienstleister.

14 Regionsbereich Hannover, Landkreisbereiche Diepholz, Hameln-Pyrmont, Hildesheim, Holzminden, Nienburg/Weser und Schaumburg sowie die Landeshauptstadt Hannover.

15 Landkreisbereiche Ammerland, Aurich, Cloppenburg, Emsland, Friesland, Grafschaft Bentheim, Leer, Oldenburg, Osnabrück, Vechta, Wesermarsch und Wittmund sowie die Städte Delmenhorst, Emden, Oldenburg, Osnabrück und Wilhelmshaven.

16 Landkreisbereiche Gifhorn, Göttingen, Goslar, Helmstedt, Northeim, Peine und Wolfenbüttel sowie die Städte Braunschweig, Salzgitter und Wolfsburg.

17 Landkreisbereiche Celle, Cuxhaven, Harburg, Heidekreis, Lüchow-Dannenberg, Lüneburg, Osterholz, Rotenburg (Wümme), Stade, Uelzen und Verden.

Tz. 16 Geprüft wurden sechs Kommunen mit einer Größe bis zu 16.000 Einwohnern[18]. In die Auswahl wurden bisher nicht oder nur selten geprüfte Kommunen miteinbezogen. Folgende Kommunen aus den statistischen Gebieten Weser-Ems und Leine-Weser wurden ausgewählt:

- Gemeinde Nordstemmen (12.095 Einwohner)
- Flecken Delligsen (7.854 Einwohner)
- Flecken Salzhemmendorf (9.113 Einwohner)
- Samtgemeinde Emlichheim (14.329 Einwohner)
- Samtgemeinde Herzlake (10.445 Einwohner)
- Samtgemeinde Schüttorf (15.664 Einwohner)

Tz. 17 Die Ergebnisse der Prüfung sollen in erster Linie den geprüften, aber auch – über den Kommunalbericht 2022 – allen niedersächsischen Kommunen als Ansatz für notwendigen Maßnahmen zur Erlangung eines Mindestsicherheitsniveaus dienen.

1.2 Rechtliche Vorgaben

Tz. 18 Die Kommunen sind verpflichtet, ihre IT-Systeme und Verwaltungsvorgänge durch technische, personelle und organisatorische Maßnahmen ausreichend abzusichern. Diese Verpflichtung ergibt sich aus dem Grundsatz des rechtmäßigen Verwaltungshandelns nach Art. 20 Abs. 3 GG sowie unmittelbaren datenschutzrechtlichen Anforderungen zum Schutz personenbezogener Daten, wie Art. 24 Abs. 1 und Art. 25 DSGVO.

Tz. 19 Die Zuständigkeit und Verantwortung für die Sicherheit der IT-Systeme liegt als Geschäft der laufenden Verwaltung nach § 85 Abs. 1 S. 1 Nr. 7 Niedersächsisches Kommunalverfassungsgesetz (NKomVG) bei den Hauptverwaltungsbeamtinnen bzw. Hauptverwaltungsbeamten. Diese haben alle erforderlichen Maßnahmen zu

[18] Landesamt für Statistik Niedersachsen, Bevölkerung und Katasterfläche in Niedersachsen, Stand: 30.06.2018.

ergreifen, um einen wirksamen Schutz zu gewährleisten. Die überörtliche Kommunalprüfung empfiehlt, sich hierbei an den unter Kapitel 1.1 genannten Standards auszurichten. Es sind nach den örtlichen Bedürfnissen der Schutz der eingesetzten Soft- und Hardware, eine ausreichende Aufklärung der Mitarbeiter sowie der Schutz personenbezogener Daten sicherzustellen und ein Informationssicherheitsmanagementsystem einzurichten. Unterstützende Hinweise zu den erforderlichen Maßnahmen gibt die überörtliche Kommunalprüfung bereits in ihren Kommunalberichten der Jahre 2016 bis 2020.[19]

1.3 Stellungnahmen der Kommunen

Tz. 20 Während der Prüfung signalisierten die geprüften Kommunen bereits, dass sie die jeweils festgestellten Prüfungsergebnisse teilen.

Tz. 21 Die Kommunen hatten bis zum 31. März 2022 Gelegenheit, zum Entwurf dieser Prüfungsmitteilung Stellung zu nehmen (§ 4 Abs. 1 Satz 3 Niedersächsisches Kommunalprüfungsgesetz).

Tz. 22 Der Flecken Salzhemmendorf und die Samtgemeinde Emlichheim gaben keine Stellungnahme ab.

Tz. 23 Der Flecken Delligsen teilte schriftlich mit, dass die Prüfungsmitteilung die Situation ausführlich darstelle und zu einer deutlichen Sensibilisierung im Bereich des Notfallmanagements im Hinblick auf die IT-Sicherheit beigetragen habe.

Tz. 24 Die Gemeinde Nordstemmen sowie die Samtgemeinden Herzlake und Schüttorf machten von dem Angebot Gebrauch, den Entwurf der Prüfungsmitteilung in einem gemeinsamen Gespräch zu erörtern. Sie führten aus, welche Maßnahmen sie zur Verbesserung der Informationssicherheit aufgrund der identifizierten Handlungsfelder bereits erarbeitet und umgesetzt haben und welche noch geplant sind. So wurden beispielsweise die Nutzung der privaten mobilen Geräte schriftlich geregelt, die

[19] Die Präsidentin des Niedersächsischen Landesrechnungshofs: Beschaffung von IT-Hardware (Kommunalbericht 2016, Kapitel 5.13); IT-Sicherheit in Kommunen (Kommunalbericht 2017, Kapitel 5.10); Informationssicherheit in Kommunen (Kommunalbericht 2018, Kapitel 5.7); Verzeichnis von Verarbeitungstätigkeiten und Auftragsverarbeitung (Kommunalbericht 2019, Kapitel 5.8); Informationssicherheitsmanagementsysteme und Sensibilisierung von Beschäftigten (Kommunalbericht 2020, Kapitel 5.4); Software-Lizenzmanagement (Kommunalbericht 2021, Kapitel 5.7).

Einrichtung eines Brandmeldesystems beauftragt, eine komplette Übersicht der eingesetzten Programme inkl. aller Zugriffsrechte erstellt sowie eine regelmäßige Online-Unterweisung der Mitarbeitenden zum Datenschutz veranlasst.

2 Zusammenfassung der wesentlichen Inhalte

Tz. 25 Cyberangriffe auf Kommunen haben bereits Schäden in Millionenhöhe verursacht. In den geprüften Kommunen müsste im Falle eines Cyberangriffs allein mit Personalausfallkosten in sechsstelliger Höhe gerechnet werden. (Tz. 49) Je nach Einzelfall sind weitere beträchtliche Schadenspositionen zu erwarten. (Tz. 40)

Tz. 26 Die nachfolgende Abbildung zeigt, dass bei allen Prüfgebieten Handlungsbedarfe in den Kommunen bestanden. Im Wesentlichen lagen diese in den Bereichen Notfallmanagement, Sicherheitsmanagement sowie Konzepte und Vorgehensweisen. Hierbei handelte es sich durchgehend um Bereiche, in denen es um Strategien, Ziele, Leitlinien und Dokumentationen geht.

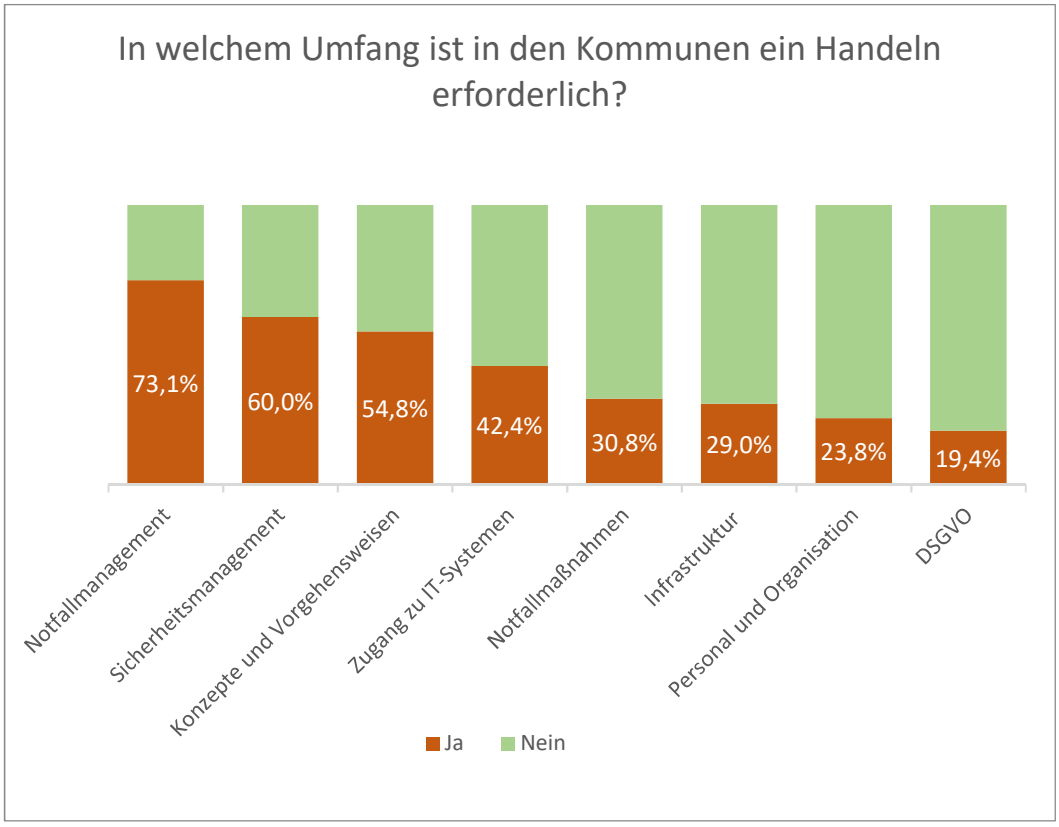


Abbildung 2 - Umfang Handlungsbedarfe in den Kommunen

Nachstehend werden die Handlungsbedarfe in den einzelnen Prüfgebieten differenziert dargestellt.

IT-Basis-Check

Tz. 27 Keine der geprüften Kommunen verfügte über eine behördenspezifische Leitlinie zur Informationssicherheit, in der die Stellenwerte der Informationsverarbeitung, die Zielerreichung, die Verantwortlichkeiten sowie eine organisatorische Einbindung beschrieben waren. (Tz. 57)

Tz. 28 Lediglich zwei von sechs Kommunen hatten IT-Sicherheitsbeauftragte benannt. (Tz. 61)

Tz. 29 Nur eine der geprüften Kommunen hatte ein dokumentiertes IT-Sicherungskonzept, in dem Sicherungsrhythmus und -art, die Bedeutung der Verfahren und Daten sowie die Verantwortlichkeit beschrieben waren. (Tz. 64)

Tz. 30 Externe Anschlüsse wie z. B. USB-Ports, Kartenleser und Laufwerke waren nur in einer Kommune grundsätzlich deaktiviert bzw. wurden aktiv verwaltet. (Tz. 72)

Tz. 31 In der Hälfte der Kommunen fehlten schriftliche Richtlinien dazu, wie ein sicheres Passwort in Bezug auf Mindestlänge, Zusammensetzung oder Geltungsdauer auszugestalten ist. In einer Kommune war es für die Nutzer nicht erforderlich, beim Login in allen einzelnen Fachverfahren ein sicheres Passwort einzugeben. (Tz. 72)

Tz. 32 Ein Formular (Papierform oder elektronisch), auf dem alle relevanten Informationen und Arbeitsschritte wie z. B. die Anforderung, Grund, Prüfung, Freigabe, Bestätigung der Umsetzung für die Zugriffsvergabe festgehalten werden, existierte in keiner der geprüften Kommunen. (Tz. 72)

Tz. 33 Alle Kommunen boten die Möglichkeit von Home-Office/Telearbeit an. Zwei Kommune hatten allerdings keine Dienstanweisung zu Home-Office/Telearbeit erlassen. In fünf Kommunen wurden hierbei auch private Computer der Beschäftigten eingesetzt; dabei fehlte es an den notwendigen Regelungen. (Tz. 72)

Tz. 34 Alle Kommunen hatten Virenschutzmaßnahmen sowie Firewall-Lösungen installiert und informierten die Beschäftigten über außerordentliche, aktuelle Bedrohungen. (Tz. 78)

Tz. 35 Keine Kommune testete die ergriffenen Notfallmaßnahmen regelmäßig. (Tz. 80)

Vertiefungsthema Notfallmanagement

Tz. 36 Zum Abschluss der Erhebungen hatte keine der geprüften Kommunen eine Risikoanalyse erstellt, in der z. B. überprüft wurde, welche Risiken die Funktionsfähigkeit der Systeme bedrohen. (Tz. 97) Nur eine Kommune hatte die eingesetzten Verfahren in kritische und weniger kritische Systeme klassifiziert, d. h. unterschieden nach Eintrittswahrscheinlichkeit und potentiell eintretendem Schaden. (Tz. 98)

Tz. 37 Keine der geprüften Kommunen hatte einen IT-Notfallplan erstellt, in dem alle notwendigen Handlungsabläufe nachvollziehbar dokumentiert sind, so dass z. B. auch externe Fachleute, die nicht an der Erstellung beteiligt waren, bei einem Notfall unmittelbar tätig werden können. (Tz. 105) Notfallübungen wurde ebenfalls noch nicht durchgeführt. (Tz. 119)

3 Kosten durch Cyberangriffe

Tz. 38 Vielfach ist den Kommunen nicht bekannt, welche Schäden durch Cyberangriffe entstehen und welche Kosten damit verbunden sein können. Laut einer Studie von Nexthink[20] nehmen die Kosten, die Unternehmen durch IT-Störereignisse entstehen, mit alarmierender Geschwindigkeit zu. So betrugen die geschätzten jährlichen Kosten für Ausfallzeiten 2019 im Durchschnitt rund 719.000 Euro je Unternehmen. Im Jahr 2018 hatten sie noch bei rund 467.000 Euro gelegen. Auch die geschätzten durchschnittlichen Kosten für Datenverluste erhöhten sich 2019 auf rund 900.000 Euro. 2018 betrugen diese noch etwa 883.000 Euro.

Tz. 39 Das BSI führt im Jahresbericht 2021[21] aus, dass von der Entdeckung einer Infektion mit einer Ransomware bis zur Bereinigung der Systeme und vollständigen Wiederherstellung der Arbeitsfähigkeit durchschnittlich 23 Tage vergehen.

Tz. 40 Vor diesem Hintergrund hat die überörtliche Kommunalprüfung im Rahmen der Prüfung die möglichen Ausfallkosten bei den Kommunen erfragt. Zu den möglichen, zum Teil erheblichen Folgen eines IT-Ausfalls zählen insbesondere:

a) Kosten für Produktivitätsausfall/Personalkosten
b) Kosten für die Fehlersuche
c) Kosten externer Hilfe (technisch und juristisch)

---

[20] https://www.storage-insider.de/it-ausfaelle-und-datenverluste-kosten-millionen-a-935534/, aufgerufen am 19.01.2022.

[21] Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2021, S.14.

d) Kosten für die Fehlerbeseitigung (Hardware, Software, Personalkosten)
e) Einnahmeausfälle
f) Reputationsverlust

Tz. 41 Häufig sahen sich angegriffene Kommunen mit Lösegeldforderungen von bis zu siebenstelligen Summen konfrontiert, damit die Daten wieder entschlüsselt werden.[22] Bei den geprüften Kommunen war das nicht der Fall.

Tz. 42 Bei der Ermittlung potentieller Schadenhöhen ist es nach Auffassung des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom)[23] nicht möglich, konkrete Zahlen zu nennen, da die jeweilige Schadenshöhe auch immer vom Angriff und dem konkreten Unternehmen bzw. der konkreten Behörde selbst abhängt. Hierbei seien so viele Faktoren zu berücksichtigen, dass nur eine Einzelfallanalyse entsprechende Schäden zuverlässig bezifferbar macht. Insbesondere seien die Kosten zu den Buchstaben b) bis f) schwer fassbar, da sie von Art und Umfang des „Notfalls“ abhängig seien.

Tz. 43 Konkrete Zahlen zu den Kosten der Buchstaben b) bis f) sind in bisher bekannten Fällen von Cyberangriffen auf Kommunen nicht bekannt gegeben worden.

Tz. 44 Der Landkreis Anhalt-Bitterfeld schätzte drei Monate nach dem Cyberangriff die Kosten bereits im hohen sechsstelligen Bereich und prognostizierte eine weitere Steigerung, weil die Arbeiten noch Monate dauern würden.[24] Insgesamt rechnet der Landkreis mit einem Kostenblock von etwa zwei Millionen Euro im Zusammenhang mit dem Cyberangriff.[25]

Tz. 45 Die Größenordnung möglicher Personalausfallkosten (Buchstabe a) kann hingegen abgeschätzt werden, da sie vom prozentualen Zeitanteil der IT-Einbindung des jeweiligen Arbeitsplatzes abhängig ist.

Tz. 46 Vor diesem Hintergrund und in Anbetracht der Feststellung, dass keine der geprüften Kommunen im Vorfeld der Prüfung Berechnungen über die Folgekosten eines

---

22 Neue Deister Zeitung, 13.9.2021, Seite 3.

23 Leitfaden Kosten eines Cyber-Schadensfalles, 2016 S. 4; https://www.bitkom.org/Bitkom/Publikationen/Welche-Kosten-entstehen-bei-einem-Cyberangriff.html.

24 https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/bitterfeld/cyberangriff-landkreis-katastrophenfall-geld-land-100.html, aufgerufen am 19.01.2022.

25 https://www.egovernment-computing.de/anhalt-bitterfeld-will-vorreiter-bei-cyber-sicherheit-werden-a-1085191/, aufgerufen am 10.01.2022.

Cyberangriffs durchgeführt hatte, hat die überörtliche Kommunalprüfung zur Ermittlung der möglichen Personalausfallkosten (= Produktivverluste) die Zeitanteile und vergütungsrechtlichen Eingruppierungen von Arbeitsplätzen mit IT-abhängigen Tätigkeiten bei den Kommunen abgefragt (Anlage 2).

Tz. 47 Auch wenn die Bezifferung zu erwartender Produktivverluste nur einen Aspekt von mehreren (Tz. 40) darstellt, ist sie aus Sicht der überörtlichen Kommunalprüfung geeignet, den Kommunen einen Eindruck davon zu vermitteln, in welcher Höhe Schäden durch Cyberangriffe insgesamt eintreten können. Zugleich wird greifbar, wie essentiell die im Rahmen der Prüfung untersuchten Abwehrmaßnahmen sein können.

Tz. 48 Auf der Basis von KGSt Personalkostensätzen wurden die potentiellen Personalausfallkosten berechnet. Bei den Produktivverlusten sind die betroffene Anzahl an Vollzeitäquivalenten sowie der Grad der Technisierung bzw. die IT-Abhängigkeit der Arbeitsabläufe beeinflussende Faktoren. Für die Berechnung der Produktivverluste hat die überörtliche Kommunalprüfung je Besoldungsgruppe/Eingruppierung die von den Kommunen übermittelten Vollzeitäquivalente mit dem prozentualen Grad der IT-Abhängigkeit der Arbeitsplätze und den entsprechende KGSt-Personalkostensätzen multipliziert und je Kommune zusammengefasst (Anlage 2). Betroffen wären von rd. 18,8 vollzeitäquivalente Stellen in Delligsen bis zu 51,08 vollzeitäquivalente Stellen in der Samtgemeinde Schüttorf.

Tz. 49 Vor diesem Hintergrund ergäben sich in den Kommunen durch einen Cyberangriff folgende Produktivverluste je Tag:

Kommune:	Einwohner	Ausfallkosten je Tag
Salzhemmendorf	9.113	4.327,63 €
Delligsen	7.854	4.937,55 €
Herzlake	10.445	7.589,63 €
Emlichheim	14.329	10.495,92 €
Nordstemmen	12.095	12.584,76 €
Schüttorf	15.664	13.087,95 €

Abbildung 3 - Ausfallkosten je Tag

Die Abbildung 3 zeigt auch, dass die Produktivverluste eines IT-Ausfalls nicht zwingend linear mit der Größe der Kommune (i. S. von Einwohneranzahl) im Zusammenhang stehen.

Tz. 50 Unter Berücksichtigung einer vom BSI angenommenen durchschnittlichen Ausfallzeit von 23 Tagen von der Entdeckung einer Infektion mit einer Ransomware bis zur Bereinigung der Systeme und kompletten Wiederherstellung der Arbeitsfähigkeit (Tz. 39) müsste bei einem vollständigen Ausfall der IT in den betrachteten Kommunen mit Produktivverlusten in folgender Höhe gerechnet werden:

Kommune:	Einwohner	Ø 23 Tage Ausfall
Salzhemmendorf	9.113	99.535,49 €
Delligsen	7.854	113.563,72 €
Herzlake	10.445	174.561,48 €
Emlichheim	14.329	241.406,16 €
Nordstemmen	12.095	289.449,44 €
Schüttorf	15.664	301.022,85 €

Abbildung 4 - Ausfallkosten bei einem durchschnittlichem Cyberangriff

Tz. 51 Nicht berücksichtigt sind bei diesen Prognoserechnungen die höchst individuellen Kosten für die Fehlersuche, externe technische und juristische Hilfe, die Fehlerbeseitigung an Hard- und Software, Einnahmeausfälle durch fehlende Lastschriften, notwendige Liquiditätskredite oder ggf. eintretende Reputationsverluste.

Tz. 52 Darüber hinaus ist im Vorfeld z. B. der Verlust digitalisierter technischer Zeichnungen aller Art nicht bezifferbar. Diese konnten in bisher bekannten Fällen nur teilweise durch Sicherungen in Planungs- und Architekturbüros wiederhergestellt werden. Nur noch physisch vorhandene Zeichnungen mussten manuell erneut digitalisiert werden, was zusätzlich einen erheblichen zeitlichen, personellen und finanziellen Aufwand darstellte.

4 Prüfungsergebnisse IT-Basis Check

Tz. 53 Als einzige der geprüften Kommunen hatte die Gemeinde Nordstemmen den Betrieb ihrer IT-Infrastruktur als Cloud Lösung einem zertifizierten Rechenzentrum[26] übertragen. Dadurch wurden alle technischen Anforderungen vom Rechenzentrum abgedeckt. Die Gemeinde Nordstemmen beschäftigte nur noch Koordinatoren, die den Betrieb mit dem Rechenzentrum abstimmten. Es gab bei der Gemeinde Nordstemmen keinen Serverraum mehr, da die Gemeinde Nordstemmen vollständig über ein Glasfaserkabel an das Rechenzentrum angeschlossen war. Insofern waren

[26] IT-Dienstleistungen für öffentliche Verwaltungen (ISO/IEC 27001:2013).

bei der Gemeinde Nordstemmen nur noch verwaltungsorganisatorische Maßnahmen, wie Dokumentationen, Einbindung der Beschäftigten oder Handlungsanweisungen Gegenstand der Prüfung.

4.1 Sicherheitsmanagement

Tz. 54 Als (Informations-)Sicherheitsmanagement wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen, kontinuierlich umzusetzen und zu dokumentieren.[27]

Tz. 55 Eine solche Dokumentation ist die Leitlinie zur Informationssicherheit[28]. Sie ist das Grundsatzdokument, um den Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit in einer Kommune festzulegen. Die Entwicklung der Leitlinie muss von der Leitung der Kommune als Geschäft der laufenden Verwaltung angestoßen und aktiv begleitet werden (Tz. 19). Die Leitlinie sollte Aussagen zu folgenden Punkten enthalten:

- Geltungsbereich,
- Bedeutung der Informationssicherheit für die Verwaltung,
- Verantwortung der Leitung, sowohl für die Initiierung des Sicherheitsprozesses als auch für dessen kontinuierlichen Verbesserung,
- Hinweis auf die einschlägigen Gesetze und Regelwerke sowie
- Festlegung der Organisationsstruktur für Informationssicherheit sowie die Aufgaben der verschiedenen Sicherheitsverantwortlichen.

Tz. 56 Gegenstand dieser Prüfung waren insbesondere die Fragen, ob die Kommunen ein Informationssicherheitsmanagement inkl. einer Leitlinie zur Informationssicherheit erstellt und ihr Personal in diesen Prozess eingebunden hatten.

---

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI); IT-Grundschutz | ISMS.1 Sicherheitsmanagement Stand Februar 2020.

[28] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS).

Tz. 57 Keine der geprüften Kommunen hatte eine behördenspezifische Leitlinie zur Informationssicherheit erstellt, in der der Stellenwert der Informationsverarbeitung, Ziele, Verantwortlichkeiten sowie eine organisatorische Einbindung beschrieben waren. Insoweit bestätigt sich das Ergebnis der Prüfung „Informationssicherheitsmanagementsysteme und Sensibilisierung von Beschäftigten“, die bereits bei anderen Kommunen stattgefunden hatte.

Tz. 58 Um dem stetig wachsenden Stellenwert der Informationssicherheit innerhalb der Verwaltung zu gerecht zu werden, empfiehlt die überörtliche Kommunalprüfung, eine Leitlinie mit oben genannten Inhalten zu erstellen, allen betroffenen Mitarbeitenden bekannt zugegeben und kontinuierlich zu aktualisieren. Die überörtliche Kommunalprüfung wiederholt somit auch ihre Empfehlung aus der o.g. Prüfung. Hilfestellung bei der Erstellung einer Leitlinie zur Informationssicherheit kann ein Muster des BSI geben.[29]

Tz. 59 Weiterhin wurde nach der Bestellung von Informationssicherheitsbeauftragten gefragt.

Tz. 60 Informationssicherheitsbeauftragte sind für alle Belange der Informationssicherheit in der Kommune zuständig.[30] Die Position kann intern oder extern besetzt werden. Intern sind Informationssicherheitsbeauftragte in der Regel in einer Stabsstelle angesiedelt. Die Kernaufgaben der Informationssicherheitsbeauftragten sind:

- den Informationssicherheitsprozess zu steuern und zu koordinieren,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung eines Sicherheitskonzepts, eines Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit anzufertigen,
- den Realisierungsplan für die Sicherheitsmaßnahmen zu erstellen und deren Umsetzung zu initiieren und zu überprüfen,

[29] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A01_Sicherheitsleitlinie.pdf?__blob=publicationFile&v=1.

[30] Bundesamt für Sicherheit in der Informationstechnik (BSI), Umsetzungshinweise zum Baustein ISMS.1 Sicherheitsmanagement; ISMS.1.M4 Benennung eines Informationssicherheitsbeauftragten.

- der Leitungsebene über den Status Quo der Informationssicherheit zu berichten,

- sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen den einzelnen Bereichen sicherzustellen,

- sicherheitsrelevante Zwischenfälle zu untersuchen sowie Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu steuern.[31]

Tz. 61 Nur zwei von sechs Kommunen hatten IT-Sicherheitsbeauftragte benannt. Die Samtgemeinde Emlichheim entschied sich für eine interne, die Samtgemeinde Schüttorf für eine externe Lösung. In beiden Fällen gaben die geprüften Kommunen an, dass die bzw. der IT-Sicherheitsbeauftragte sowohl über das notwendige Fachwissen als auch über ausreichende zeitliche Ressourcen für die Erledigung der Aufgaben verfügte.

Tz. 62 Obwohl keine gesetzliche Pflicht zur Bestellung eines Informationssicherheitsbeauftragten besteht (die Ausnahme bilden sogenannte KRITIS-Unternehmen[32]), empfiehlt die überörtliche Kommunalprüfung, diese Aufgabe intern oder extern durch geeignete Personen wahrnehmen zu lassen.

4.2 Konzeption und Vorgehensweise

Tz. 63 In diesem Prüfbereich wurde betrachtet, ob und inwieweit ein funktionierendes Managementsystem für Informationssicherheit (ISMS) eingerichtet und implementiert war. Es wurde u.a. geprüft, ob bei den Kommunen Regelungen zur physikalischen IT-Sicherheit (Gebäudesicherheit, Schutz bei technischem Versagen usw.) bestehen. Weiter wurde untersucht, ob in den Kommunen Regelungen zur technischen und organisatorischen IT-Sicherheit, wie etwa Schutzkonzepte gegen Schadsoftware, Notfallpläne, Vertretungsregelungen, Datensicherungskonzepte, Identitäts- und Berechtigungsmanagement, sowie Regelungen zu redundanten Systemen[33] vorhanden waren.

---

31 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI Standard 200-2 IT-Grundschutz-Methodik, 2017, S. 41.

32 KRITIS steht für kritische Infrastrukturen und umfasst solche Versorgungsdienstleister, bei deren Beeinträchtigung mit besonders schwerwiegenden Folgen für Wirtschaft, Staat und Gesellschaft zu rechnen ist. Einzelheiten sind der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz zu entnehmen.

33 Bei technischen Systemen versteht man unter Redundanz die bewusste Mehrfachauslegung von technischen Bestandteilen. Die bei normaler Funktion überflüssigen Bestandteile sind als Ersatz für ausfallende Komponenten gedacht. Sehr verbreitet ist die Verdopplung z.B. von Netzteilen in zentralen Netzwerkgeräten oder Servern.

Tz. 64 Die folgende Abbildung zeigt, dass in allen Kommunen noch Handlungsbedarfe auf dem Weg zur Erstellung eines funktionierendes Managementsystem für Informationssicherheit (ISMS) bestehen. Während einige Kommunen bereits Grundlagen, wie ein Sicherungskonzept oder konzeptionelle Regelungen zur Nutzung der IT Infrastruktur hatten, hatte die Samtgemeinde Herzlake auf diesem Gebiet bisher keine Regelungen getroffen.

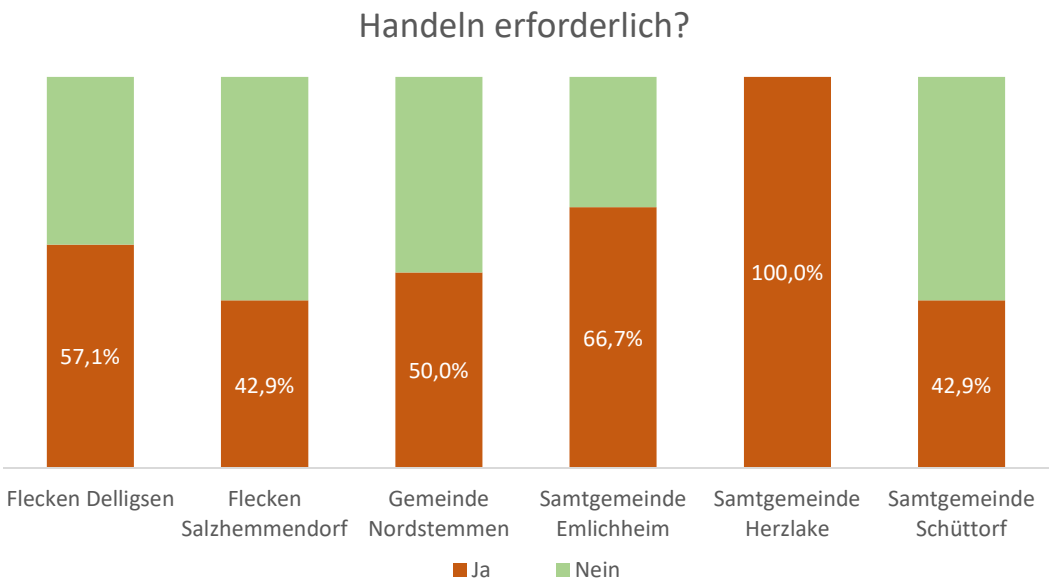


Abbildung 5 - Handlungsbedarf Prüfgebiet Konzept und Vorgehensweise

- Nur der Flecken Salzhemmendorf hatte ein dokumentiertes IT-Sicherungskonzept, in dem der Sicherungsrhythmus, die Sicherungsart, die Bedeutung der Verfahren und Daten oder die Verantwortlichkeit beschrieben waren. Die Gemeinde Nordstemmen hatte den kompletten technischen IT-Betrieb inkl. der Datensicherung an einen Dienstleister ausgelagert und musste daher selbst keine Regelungen zur Datensicherung erlassen. (Tz. 53)

- Vier der geprüften Kommunen gaben an, die Nutzung des E-Mail-Accounts und des Webzugangs zu dienstlichen oder privaten Zwecken geregelt zu haben. In der Gemeinde Nordstemmen sowie der Samtgemeinde Herzlake fehlten die erforderlichen Regelungen. Damit fehlen bereits wichtige Grundlagen, um die missbräuchliche Nutzung der IT Systeme zu verhindern. (Tz. 63)

Tz. 65 Über weitere Handlungsbedarfe und somit Empfehlungen der überörtlichen Kommunalprüfung wurden die einzelnen Kommunen bereits im Anschluss an die Erhebung durch Übersendung des ausgewerteten Fragenkatalogs (Anlage 1) informiert.

4.3 Infrastruktur

Tz. 66 Ein weiterer, wesentlicher Gesichtspunkt der IT-Sicherheit liegt darin, unberechtigte Personen frühzeitig und effektiv am Zutritt zu IT-sicherheitsrelevanter Infrastruktur einschließlich den Serverräumen zu hindern. Deshalb wurden Aspekte wie allgemeine Zutrittsmöglichkeiten, besondere Erfordernisse an Serverräume, Umgang mit Dienstleistern sowie Besucherinnen und Besuchern ebenso erfragt wie Brandschutzaspekte.

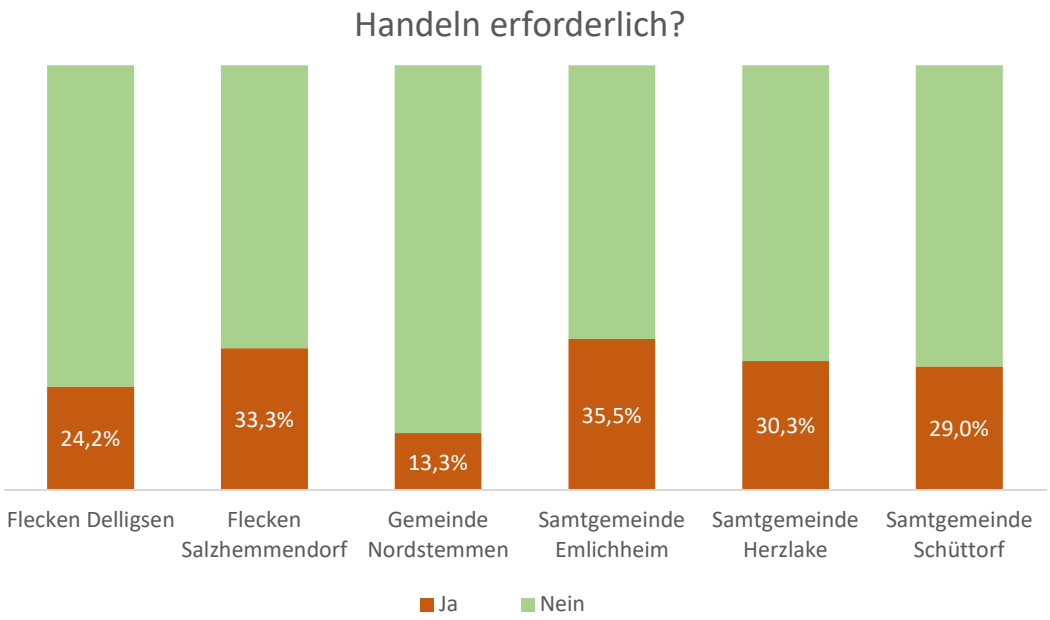


Abbildung 6 - Handlungsbedarf Prüfgebiet Infrastruktur

Tz. 67 Vorstehende Abbildung 6 zeigt, dass die von der überörtlichen Kommunalprüfung erfragten Prüfpunkte überwiegend erfüllt wurden. Die wenigsten Handlungsnotwendigkeiten ergaben sich bei der Gemeinde Nordstemmen. Der dortige Handlungsbedarf bezieht sich auf das Brandmeldesystem für das gesamte Gebäude und hat aber durch die ausgelagerte IT-Infrastruktur (Tz. 53) nur mittelbar Einfluss auf die originäre Sicherheit der dortigen IT-Infrastruktur.

Tz. 68 Die Schwerpunkte der festgestellten Handlungsbedarfe in den verbleibenden fünf Kommunen lagen im Bereich der Serverräume, dem Umgang mit Besucherinnen

und Besuchern, Lieferanten sowie der Brandmeldesysteme. Hier wurde im Wesentlichen folgendes vorgefunden:

- Im Flecken Delligsen führten Wasser Zu- oder Ableitungen durch den Serverraum. Allerdings war in diesem Fall das Risiko durch einen installierten Wassermelder reduziert worden.

- Lediglich die Samtgemeinde Herzlake hatte einen fensterlosen Serverraum. Von den verbleibenden vier Kommunen waren die Fenster nur im Flecken Delligsen alarmgesichert.

- Keine der Kommunen hatte für den Serverraum eine Videoüberwachung oder eine Alarmierung für eine Zeitüberschreitung der Türöffnung eingerichtet.

- Nur die Gemeinde Nordstemmen hatte ihre Beschäftigten schriftlich darauf hingewiesen, worauf sie bei Besucherkontakt zu achten haben und wie mit auffälligen Personen umzugehen ist.

- Alle Kommunen gaben an, dass externe Dienstleister sich nur unter Aufsicht in den höheren Sicherheitszonen, wie Personalabteilungen oder Technikbereiche, bewegen dürfen. Nur die Gemeinde Nordstemmen dokumentierte dies, um so Anwesenheiten und Tätigkeiten Externer nachvollziehen zu können, sollten im Nachgang Störungen auftreten.

Tz. 69 Detaillierte Hinweise zur Ausgestaltung eines Serverraums bietet z. B. der Grundschutzbaustein INF.2 „Rechenzentrum sowie Serverraum“ des BSI Grundschutz Kompendiums.[34]

Tz. 70 Über die Handlungsbedarfe und somit die Empfehlungen der überörtlichen Kommunalprüfung wurden die einzelne Kommune bereits im Anschluss an die Erhebung durch Übersendung des ausgewerteten Fragenkatalogs (Anlage 1) informiert.

[34] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/10_INF_Infrastruktur/INF_2_Rechenzentrum_sowie_Serverraum_Edition_2022.pdf?__blob=publicationFile&v=3#download=1.

4.4 Zugang zu IT-Systemen

Tz. 71 Bezüglich des Zugangs zu IT-Systemen wurde beleuchtet, welche Maßnahmen die Kommunen ergriffen haben, um einen unbefugten Zugriff auf die EDV-Systemen mit geeigneten Maßnahmen zu verhindern. So wurde geprüft, ob und wie eine ordnungsgemäße IT-Administration inklusive Passwortsicherheit gewährleistet und Zugriffsrechte gehandhabt wurden.

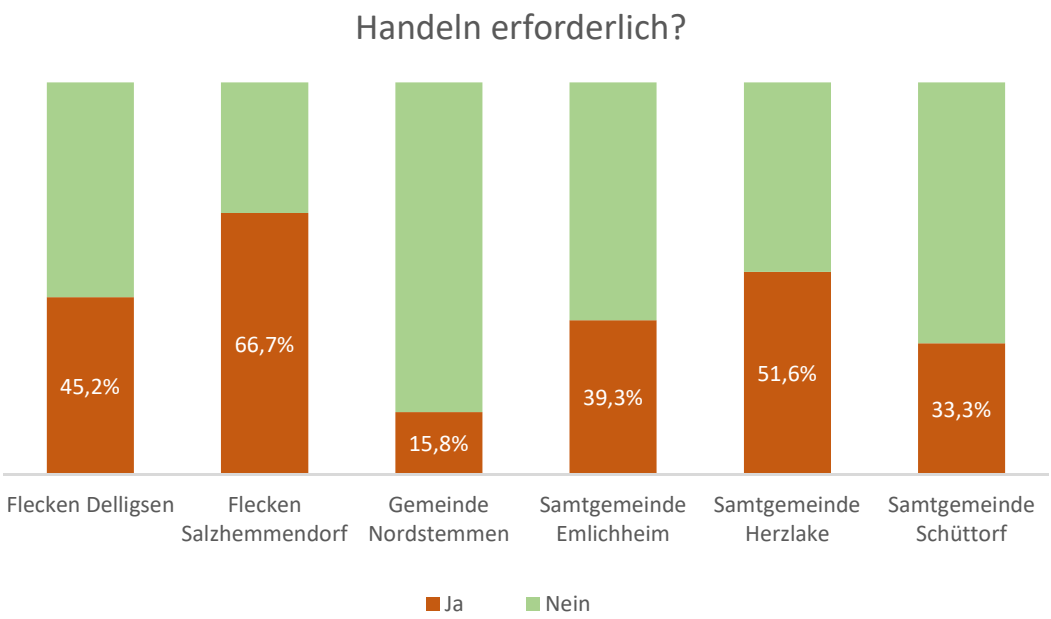


Abbildung 7 - Handlungsbedarf Prüfgebiet Zugang zu IT-Systemen

Tz. 72 Wie die Abbildung 7 zeigt, hatten die Kommunen überwiegend Maßnahmen ergriffen, um einen unbefugten Zugang zu den EDV-Systemen zu verhindern. Gleichwohl gab es in allen Kommunen noch Handlungsbedarfe, wie die nachfolgenden Beispiele aufzeigen:

- Nur die Gemeinde Nordstemmen hatte externe Anschlüsse wie USB-Ports, Kartenleser und Laufwerke grundsätzlich deaktiviert bzw. aktiv verwaltet.

- Ein Formular (Papierform oder elektronisch), auf dem alle relevanten Informationen und Arbeitsschritte wie z. B. die Anforderung, Grund, Prüfung, Freigabe, Bestätigung der Umsetzung für die Zugriffsvergabe festgehalten werden, existierte in keiner der geprüften Kommunen. Die überörtliche Kommunalprüfung empfiehlt, einen strukturierten Ablaufplan für Veränderungen beim Personal zu erstellen.

- Nur in der Hälfte der Kommunen existierten schriftliche Richtlinien, wie ein sicheres Passwort in Bezug auf Mindestlänge, Zusammensetzung und Geltungsdauer auszugestalten ist.

- Alle Kommunen boten die Möglichkeit von Home-Office/Telearbeit an. Zwei Kommunen hatten allerdings keine Dienstanweisung zu Home-Office/Telearbeit erlassen. In fünf Kommunen wurden hierbei auch private Computer der Beschäftigten eingesetzt. Sofern private Computer für dienstliche Zwecke eingesetzt werden, müssen einige Punkte, unter anderem lizenzrechtliche Fragen berücksichtigt werden. So darf privat angeschaffte Software je nach den lizenzrechtlichen Bestimmungen eventuell nicht dienstlich genutzt werden. Zudem werden sensible Daten auf Endgeräten verarbeitet, die häufig nicht so gut abgesichert werden können wie auf Arbeitsplatzrechnern. Da durch die Kommune nicht direkt auf die privaten Geräte zugegriffen werden kann, muss durch entsprechende Regelungen sichergestellt werden, dass Beschäftigte

  - aktuelle Virenschutz-Programme einsetzen,
  - alle Sicherheitsupdates zeitnah einspielen,
  - ihr Endgerät ausschließlich allein nutzen,
  - alle lokal gespeicherten Daten verschlüsseln.

  Darüber hinaus sollten sich die Beschäftigten verpflichten, den Dienstherrn umgehend zu informieren, wenn sie ein Gerät verloren haben.[35]

Tz. 73 Insbesondere für die Nutzung von Telearbeitsplätzen ist eine stringente IT-Administration ebenso erforderlich wie eine dokumentierte Vergabe von Zugriffsrechten und eine durchgehende Passwortsicherheit. Des Weiteren sind ergänzende organisatorische Absprachen zwischen den Beschäftigten und der Kommune angezeigt, wie Handlungsanweisungen für den Fall, dass sicherheitsrelevante Vorkommnisse am Telearbeitsplatz eintreten. Zudem muss für einen Fernzugriff von der Kommune ein

[35] Vgl. https://www.cio.de/a/ratschlaege-fuer-die-byod-policy,2906315, aufgerufen am 02.02.2022.

sicherer Remote-Zugang eingerichtet werden, z. B. kryptografisch abgesicherte Zugänge via VPN (Virtual Private Networks).[36]

Tz. 74 Über die Handlungsbedarfe und somit die Empfehlungen der überörtlichen Kommunalprüfung wurden die einzelnen Kommunen bereits im Anschluss an die Erhebung durch Übersendung des ausgewerteten Fragenkatalogs (Anlage 1) informiert.

4.5 Notfallmaßnahmen

Tz. 75 Notfallmaßnahmen sind Handlungen der IT-Verantwortlichen, die den Normalbetrieb absichern. In der IT sollen primär die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sichergestellt werden. Störungsbedingte Ausfallzeiten im Normalbetrieb sollen durch geeignete Notfallmaßnahmen minimiert und im Rahmen der allgemeinen Aufbauorganisation abgewickelt werden.

Tz. 76 Von besonderer Bedeutung ist u.a., ob eine dem Stand der Technik entsprechende Firewall-Lösung zum Schutz vor Zugriffen von außen eingesetzt und ob die Systeme vor Stromausfällen mittels unterbrechungsfreier Stromversorgung (USV) gesichert sind. Weiterhin wurde geprüft, ob und inwieweit ein Monitoring System[37] vorhanden ist. Ein Monitoring-System hat den Vorteil, dass das gesamte Netzwerk in Echtzeit und aus einer Hand überwacht werden kann, bei Störungen unterschiedlichster Art (Feuer, Wasser, Einbruch, fehlerhafte Backups usw.) rechtzeitig alarmiert und die Ursache deutlicher schneller erkennt. Oft kann ein Problem behoben werden, bevor eine Störung bei den Nutzerinnen und Nutzern bemerkbar wird.

Tz. 77 Notfallmaßnahmen sollten zudem regelmäßig und ereignisunabhängig getestet werden. Es sollten darüber hinaus Notfallübungen mit den Mitarbeitenden durchgeführt werden.

---

[36] Eine VPN-Verbindung bietet die abgesicherte Möglichkeit, von außen auf ein bestehendes Netzwerk, hier einer Kommune, zuzugreifen.

[37] Beim IT-Monitoring handelt es sich um die laufende Überwachung der Funktionalität von Hardware, Vorgängen und Prozessen in der entsprechenden Systemumgebung. Dabei wird überwacht, ob alle beobachteten Komponenten störungsfrei laufen.

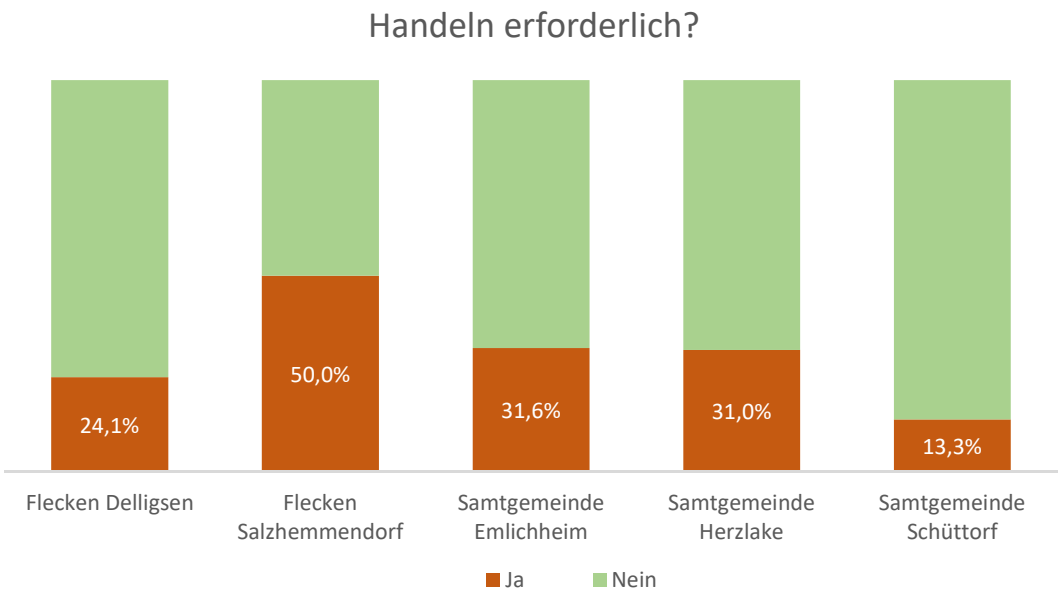


Abbildung 8 - Handlungsbedarf Prüfgebiet Notfallmaßnahmen

Tz. 78 Vorstehende Abbildung 8 zeigt, dass alle Kommunen Vorkehrungen im Sinne einer Notfallvorsorge getroffen hatten. Gut aufgestellt waren die Kommunen in den Bereichen Firewall, Virenschutz und WLAN. Handlungsbedarfe ergaben sich aus Sicht der überörtlichen Kommunalprüfung überwiegend in den Bereichen Monitoring, USV und bei der Durchführung von Notfalltests.

Tz. 79 In dieser Betrachtung wurde die Gemeinde Nordstemmen nicht berücksichtigt, da sie die technischen Notfallmaßnahmen durch die vollständige Auslagerung des IT-Betriebs auf ein zertifiziertes Rechenzentrum übertragen hatte. (Tz. 53)

Tz. 80 Die verbleibenden Kommunen zeigten ein heterogenes Bild:

- Die Kommunen hatten noch nicht für alle geeigneten Bereiche Monitoring-Systeme eingesetzt. So wurden die USV-Systeme nicht regelmäßig gewartet und/oder meldeten auftretende Störungen – im einfachsten Fall automatisch per E-Mail oder SMS – nicht an die hierfür zuständigen Ansprechpersonen.

- Keine der Kommunen hatte mit den Mitarbeitenden Notfallübungen durchgeführt.

Tz. 81 Über weitere Handlungsbedarfe und somit Empfehlungen der überörtlichen Kommunalprüfung wurden die einzelnen Kommunen bereits im Anschluss an die Erhebung durch Übersendung des ausgewerteten Fragenkatalogs (Anlage 1) informiert.

Tz. 82 Die überörtliche Kommunalprüfung empfiehlt allen Kommunen, insbesondere anhand der o. g. Punkte 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.

4.6 Datenschutzgrundverordnung (DSGVO)

Tz. 83 Die Regelungen der DSGVO dienen dem Schutz personenbezogener Daten. Mithilfe der DSGVO sollen innerhalb der EU ein weitestgehend einheitliches Datenschutzrecht geschaffen und die Rechte der Betroffenen deutlich gestärkt werden. Auch die Kommunen haben hierbei konkrete Vorgaben einzuhalten. Neben der grundsätzlichen Frage, ob Datenschutzbeauftragte bestellt worden sind, wurde geprüft, ob die Kommunen alle gesetzlich vorgesehenen Maßnahmen zur Verarbeitung personenbezogener Daten getroffen haben, wenn diese Verarbeitung durch externe Dienstleister durchgeführt wird (Auftragsverarbeitung). Ebenso wurde betrachtet, ob die Kommunen sichergestellt hatten, dass auch die Auftragsverarbeiter alle technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes bei der Verarbeitung getroffenen hatten und ob das Auskunftsrecht Betroffener organisiert war.

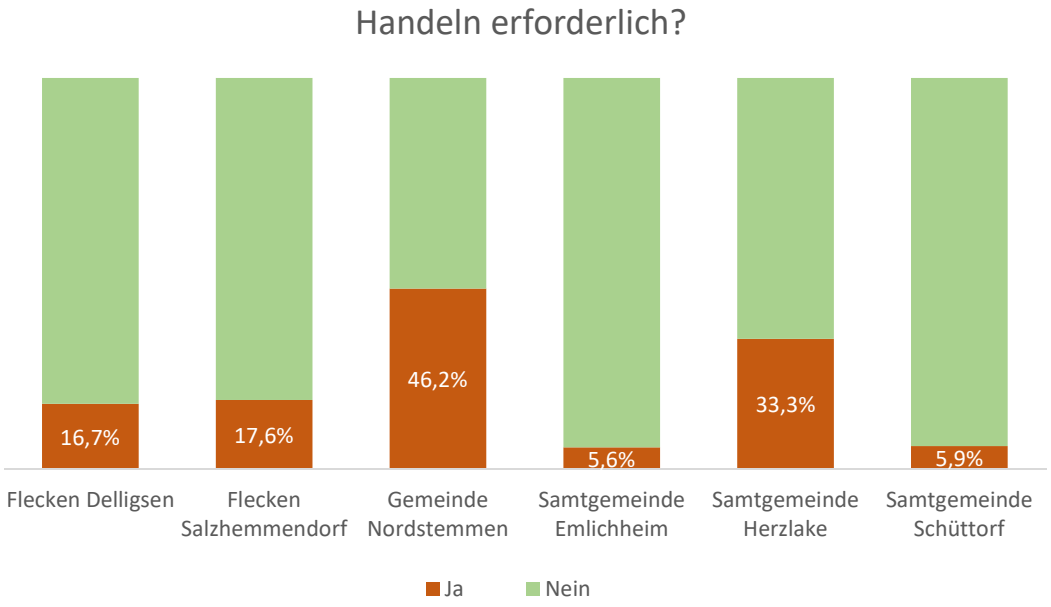


Abbildung 9 - Handlungsbedarf Prüfgebiet DSGVO

Tz. 84 Die Kommunen hatten die Vorgaben der DSGVO überwiegend bereits berücksichtigt und die erforderlichen Maßnahmen umgesetzt. So hatten z. B. alle geprüften Kommunen schriftlich Datenschutzbeauftragte bestellt. Alle Kommunen entschieden sich dabei für eine externe Beauftragung. Gleichwohl bestanden zum Abschluss der örtlichen Erhebungen noch Handlungsbedarfe:

- Alle Kommunen hatten durchgängig mit allen Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DSGVO abgeschlossen. Allerdings hatten drei Kommunen vor Vertragsabschluss das Datenschutz- und Datensicherheitsniveau der externen Dienstleister nicht geprüft.

- Die Gemeinde Nordstemmen verfügte nicht über ein gem. Art. 30 DSGVO vorgeschriebenes Verzeichnis der Verarbeitungstätigkeiten.

- Über einen schriftlich festgelegten Prozess, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DSGVO zeitnah und vollständig erfüllen zu können, verfügten nur die Samtgemeinde Schüttorf und der Flecken Delligsen. Diese beiden Kommunen hatten auch einen Prozess eingeführt, der die internen Zuständigkeiten regelte.

Tz. 85 Die Kommunen sollten die noch nicht erfüllten Vorgaben der DSGVO unverzüglich umsetzen und damit ihren Verpflichtungen zum Schutz personenbezogener Daten nachkommen.

Tz. 86 Über die Handlungsbedarfe und somit die Empfehlungen der überörtlichen Kommunalprüfung wurden die einzelne Kommune bereits im Anschluss an die Erhebung durch Übersendung des ausgewerteten Fragenkatalogs (Anlage 1) informiert.

4.7 Schulungen und Sensibilisierungen der Beschäftigten

Tz. 87 Trotz der in den letzten Jahren stetig gestiegenen Berichterstattung über Cyberangriffe und Datenpannen[38] scheint allgemein das Bewusstsein (sog. Awareness) für die heute existierenden Cybergefahren noch immer nicht in dem Maße vorhanden zu sein, wie es die bestehenden Risiken erfordern. Auch für Kommunen bedeutet fehlende Sensibilität der Beschäftigten in Bezug auf IT-Sicherheit ein gesteigertes

[38] Eine Datenpanne ist ein Vorfall, bei dem Unberechtigte Zugriff auf eine Datensammlung erhalten oder Daten unerwünscht abhandenkommen.

Risiko, Opfer einer Cyberattacke zu werden. Zudem ist nicht jeder IT-Notfall leicht zu erkennen. Noch schwerer ist die Beurteilung, ob es sich um eine Fehlfunktion oder um einen Cyberangriff handelt.

Tz. 88 Die überörtliche Kommunalprüfung betrachtete daher, ob die Mitarbeiterinnen und Mitarbeiter für die Themen Datenschutz und Datensicherheit sensibilisiert wurden und ob regelmäßig (mindestens alle zwei Jahre) Auffrischungsschulungen durchgeführt wurden.

Tz. 89 Alle Kommunen gaben an, ihr Personal für die Themen Datenschutz und Datensicherheit zu sensibilisieren. In der Regel haben die Kommunen alle zwei Jahre Auffrischungsschulungen hierzu durchgeführt.

Tz. 90 Die überörtliche Kommunalprüfung begrüßt ausdrücklich, dass die Kommunen weitestgehend ihre Beschäftigten schulen. Sie empfiehlt mit Blick auf die Bedeutung von Datenschutz und Datensicherheit darüber hinaus, organisatorische Regelungen zu treffen, die die Durchführung und Überwachung dieser Schulungsmaßnahmen verbindlich regeln. Dies kann beispielsweise in Form eines Sensibilisierungs- und Schulungskonzepts mit folgenden Inhalten erfolgen:

- Verantwortlichkeit für die Durchführung von Schulungen- und Sensibilisierungsmaßnahmen sowie deren Überwachung,
- Aufnahme des Ist-Stands und Ableitung des Soll-Zustands,
- Schulungsplanung, Methoden und Medien,
- Zielgruppen (zum Beispiel Führungskräfte, Verwaltungsbeschäftigte, IT-Beschäftigte) sowie
- risikobehaftete Themen (zum Beispiel Passwort, E-Mail, mobile Datenträger).[39]

Tz. 91 Schulungen und Sensibilisierungsmaßnahmen in der Kommune bieten sich als Rahmen an, um beispielsweise auch die IT-Notfallkarte einzuführen.

[39] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Umsetzungshinweise zum Grundschutz Kompendium, Baustein ORP.3 Sensibilisierung und Schulung.

Tz. 92 Die IT-Notfallkarte[40] ist das 2019 eingeführte Hinweisschild für den IT-Bereich, analog zum bekannten Format „Verhalten im Brandfall“. Beschäftigten in den Kommunen werden hiermit wichtige Verhaltenshinweise bei IT-Notfällen aller Art an die Hand gegeben. Die aufgeführten Handlungsanweisungen ermöglichen es den Beschäftigten, vom ersten Moment an die richtigen Entscheidungen treffen zu können. Die Notfallkarte sollte an zentralen Orten, wie Fluren, Büros oder direkt an den IT-Arbeitsplätzen platziert werden. Sie erzeugt dadurch einen unmittelbaren Beitrag zur Awareness in der Kommune.

5 Vertiefende Betrachtung IT-Notfallmanagement

Tz. 93 Über die Notfallmaßnahmen hinaus (vgl. Kapitel 4.5), die störungsbedingte Ausfallzeiten im Normalbetrieb minimieren, soll das Notfallmanagement sicherstellen, dass eine Behörde ihren Betrieb in allen IT-Notfalllagen aufrechterhalten kann und weiterhin die Geschäfts- und Handlungsfähigkeit gegeben ist. Notfallmanagement ist also ein systematischer, an den Geschäftsprozessen orientierter Ansatz zur Vorsorge gegen Notfälle und Krisen. Es zielt darauf ab, solche Ausnahmesituationen, wenn schon nicht zu verhindern, so doch in ihren Schadensauswirkungen zu begrenzen. Dazu gehört es, organisatorische Strukturen aufzubauen sowie Konzepte zu entwickeln und umzusetzen, die eine rasche Reaktion auf Notfälle und die Fortsetzung zumindest der wichtigsten Geschäftsprozesse ermöglichen.[41]

Tz. 94 Mit dem IT-Notfallmanagement plant die Kommune alle notwendigen Schritte und prüft im Vorfeld alle Vorgehensweisen, um im Notfall einen möglichst schadensbegrenzenden Ablauf zu gewährleisten. Hierfür sind Maßnahmen der Prävention bereits im Vorfeld zu ermitteln, vorzubereiten und zu üben. Wesentliche Punkte im IT-Notfallmanagement sind

- Risikoanalyse,
- Erstellung einer Richtlinie zum Notfallmanagement,
- Notfallplan,

[40] IT-Notfallkarte abzurufen unter: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/IT-Notfallkarte_DINA4.pdf;jsessionid=5946C49724498C689685D86309055D01.internet461?__blob=publicationFile&v=1.

[41] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI); Erläuterung BSI Webkurs Notfallmanagement; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Webkurs_Notfallmanagement.pdf;jsessionid=127838103B07FBDE0C7C572EE9604EEC.internet481?__blob=publicationFile&v=1, aufgerufen am 04.02.2022.

- Vorbereitung zur Behebung von Notfällen,
- Dokumentation von Notfällen zur späteren Auswertung sowie
- Durchführung von Notfallübungen.

5.1 Risikoanalyse

Tz. 95 Die Risikoanalyse identifiziert und bewertet die möglichen Risiken, denen die informationsverarbeitenden Systeme der Kommunen ausgesetzt sind oder die durch sie verursacht werden.

Tz. 96 Bei der Risikoanalyse werden zwei Phasen nacheinander durchlaufen:

a) Identifikation der Gefährdungen.
Die Nutzerinnen und Nutzer identifizieren potentielle Gefährdungen, die sich negativ auf ihre Geschäftsprozesse und -bereiche in ihrer Kommunalverwaltung auswirken können, die Funktionsfähigkeit der Systeme und die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) bedrohen. Auf dieser Basis sollten später die eingesetzten Verfahren in kritische und weniger kritische Systeme klassifiziert werden. Gefährdungen in diesem Sinne sind vielschichtig und reichen z. B. von Bedrohungen durch Feuer oder Naturkatastrophen bis hin zur Manipulation von Hard- und Software. Das BSI hat eine Übersicht über 47 elementare Gefährdungen erstellt.[42]

b) Risikoeinschätzung
Die festgestellten potenziellen Gefährdungen sind nunmehr in Bezug auf Eintrittshäufigkeit und Schadenshöhe durch geeignetes Fachpersonal (das können die vorgenannten Sicherheitsbeauftragten sein) nach den Kriterien Eintrittshäufigkeit[43] und Schadenshöhe[44] zu beurteilen.

---

[42] Bundesamt für Sicherheit in der Informationstechnik (BSI); BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz, S. 13 ff.

[43] Bundesamt für Sicherheit in der Informationstechnik (BSI); BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz, S. 27 f.

[44] Bundesamt für Sicherheit in der Informationstechnik (BSI); BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz, S. 26 f.

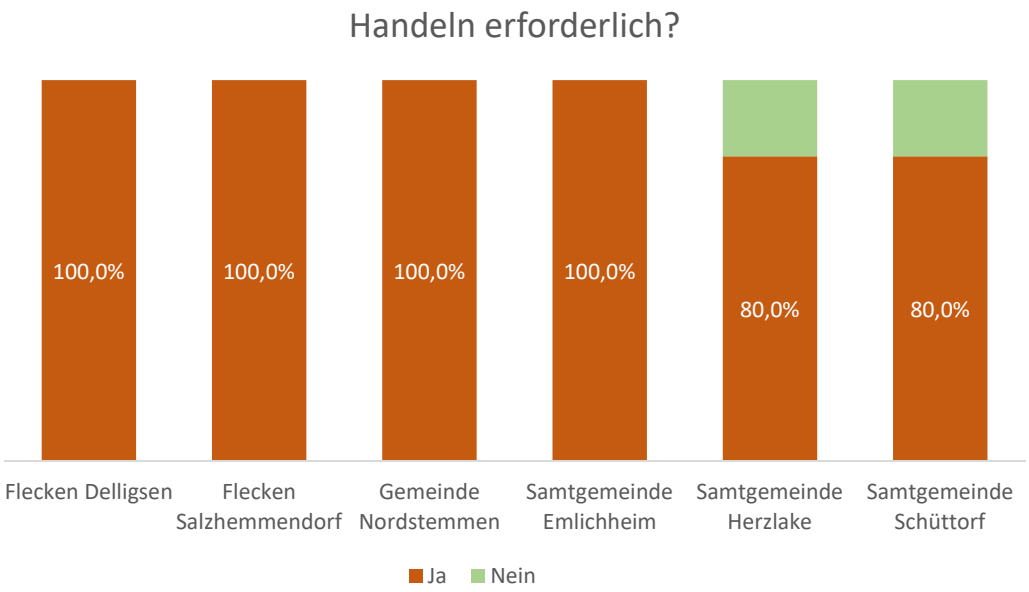


Abbildung 10 - Handlungsbedarf Prüfgebiet Risikoanalyse

Tz. 97 Keine der Kommune hat in den zwölf Monaten vor Abschluss der Erhebungen eine vollständige Risikoanalyse durchgeführt.

Tz. 98 Einzelne Aspekte wurden in verschiedenen Kommunen aufgegriffen. So hatte zum Beispiel die Samtgemeinde Schüttorf maximal tolerierbare Ausfallzeiten festgelegt. Die Samtgemeinde Herzlake hatte die eingesetzten Verfahren in kritische und weniger kritische Systeme klassifiziert.

5.2 Erstellung einer Richtlinie zum Notfallmanagement

Tz. 99 Eine Richtlinie zum Notfallmanagement sollte nach den örtlichen Gegebenheiten der Kommune kurz und übersichtlich die wesentlichen Aspekte des Umgangs mit einem IT-Notfall beschreiben. Hierzu zählen die Definition des Notfallmanagements, das gewählte Vorgehensmodell sowie der Geltungsbereich des Notfallmanagements.

Tz. 100 Bei der Entwicklung der Richtlinie ist es hilfreich, die wichtigsten Gruppen zu identifizieren, die Interessen am Notfallmanagement der Kommune haben und deren Anforderungen zu berücksichtigen. Zu diesen Gruppen gehören z. B. die Beschäftigten, Bürgerinnen und Bürger, Lieferanten aber auch Aufsichtsbehörden und Vertragspartner.

Tz. 101 Eine solche Richtlinie zum Notfallmanagement, in der die wesentlichen Aspekte des Umgangs mit einem IT-Notfall beschrieben werden, war in keiner der geprüften Kommunen vorhanden.

Tz. 102 Um auf Ausfälle in der Verfügbarkeit ihrer IT-Systeme angemessen reagieren zu können, sollten die Kommunen in einer Leitlinie zur Informationssicherheit oder im Notfallplan folgende Festlegungen dazu treffen,

- welche Ressourcen und Prozesse der Kommune kritisch sind,
- welche Maßnahmen präventiv erforderlich sind, damit Notfälle und Krisen möglichst unbeschadet überstanden werden können sowie
- insbesondere wie bei Unterbrechung wichtiger Prozesse der schnelle Wiederanlauf sichergestellt werden kann.

Eine solche Richtlinie inkl. der abgeleiteten Notfallanweisungen sollte fortwährend der aktuellen Bedrohungslage angepasst und regelmäßig, mindestens jährlich, aktualisiert werden.

5.3 Notfallplan

Tz. 103 Ein Notfallplan ist ein Leitfaden, der basierend auf der Richtlinie zum Notfallmanagement konkrete Handlungsanweisungen und zu ergreifende Maßnahmen bei IT-Notfällen definiert. Ein Notfallplan ist das zentrale Dokument, um auf IT-Notfälle angemessen und zügig reagieren zu können. Er hilft, ein etwaiges Schadensausmaß einzugrenzen und gezielt Gegenmaßnahmen unverzüglich ergreifen zu können. In einem Notfallplan werden

- Handlungsabläufe nachvollziehbar dokumentiert,
- Verantwortlichkeiten für die Wiederanlaufmaßnahmen vorgegeben,
- Netzwerkübersichten der eingesetzten Techniken und Systeme dokumentiert,
- Übersichten über externe Zulieferer für Strom, Wasser, Telekommunikation, Datenleitungen, Hardware, Software usw. und

- Verzeichnisse der im Einsatz befindlichen Hard- und Software,

vorgehalten.

Tz. 104 Konsequenterweise basiert ein Notfallplan auf einer vorab durchgeführten Risikoanalyse (Kapitel 5.1), wird allen Beschäftigten zur Kenntnis gegeben und anschließend an einem fest definierten Ort aufbewahrt.

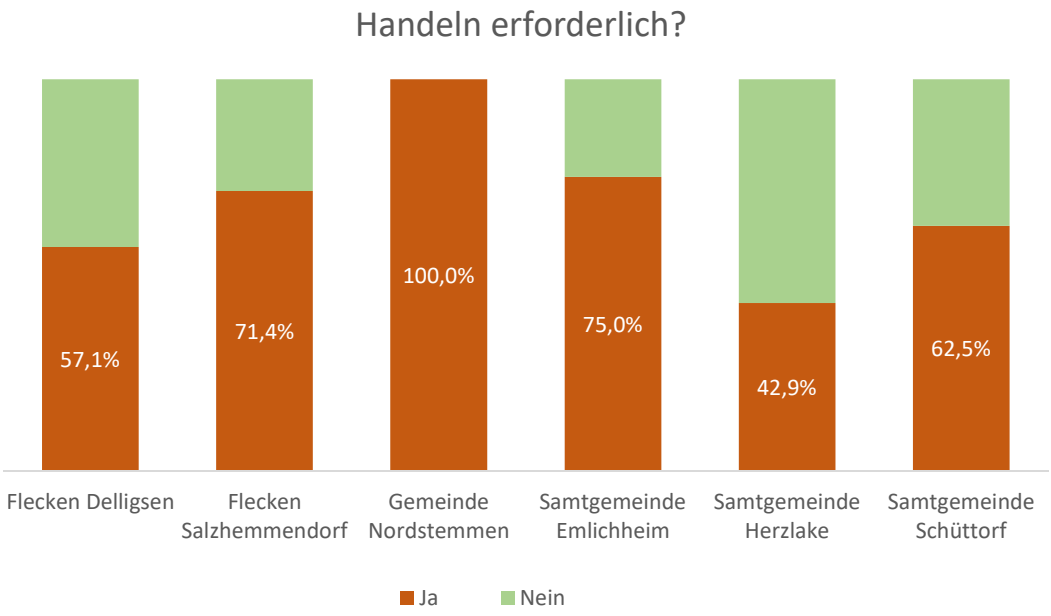


Abbildung 11 - Handlungsbedarf Prüfgebiet Notfallplan

Tz. 105 Einen solchen Notfallplan hatte keine der geprüften Kommunen verfasst.

Tz. 106 Allerdings hatten die drei Kommunen Samtgemeinden Emlichheim, Herzlake und Schüttorf Netzwerkübersichten der eingesetzten Techniken und Systeme dokumentiert. Zwei Kommunen (Flecken Delligsen und Salzhemmendorf) führten ein Verzeichnis der im Einsatz befindlichen Hard- und Software. Der Flecken Delligsen sowie die Samtgemeinden Herzlake und Schüttorf verfügten über eine Leitungsübersicht der internen Verkabelung und externen Leitungen sowie einer Beschreibung der Patchfeld-Systematiken.[45]

[45] Bei IT- und Kommunikationsnetzen sind alle Komponenten und Anschlüsse gekennzeichnet und werden über Verteilerschränke miteinander verbunden. Alle Kabel enden in Verteilerschränken als Anschluss in einem Patchfeld. Die konkreten Zusammenhänge werden in einer Netzwerkdokumentation erfasst und nachvollziehbar abgebildet. Über die Bezeichnung dieser Patchfelder können dann alle Verbindungen, wie z. B. von einem Arbeitsplatz zu einem Server, identifiziert werden.

Tz. 107 Diese bereits vorliegenden Bausteine sind eine gute Grundlage für die Erarbeitung eines umfassenden Notfallplans.

Tz. 108 Die übrigen Kommunen sollten ebenfalls vergleichbare Übersichten (Tz. 106) erstellen und zu einem zusammenfassenden Notfallplan verarbeiten.

5.4 Behebung von Notfällen

Tz. 109 Je besser vorbereitet eine Kommune auf einen IT-Notfall ist, desto handlungsfähiger ist sie und desto leichter kann sie mögliche Schäden begrenzen. Wichtig ist dabei insbesondere, dass alle für die Behebung des Notfalls wesentlichen Informationen, wie z. B. Passwörter und Angaben zu Lieferanten und Dienstleistern zentral zur Verfügung stehen. Ebenso sollten alle Backup-Medien für das Rücksichern der Daten unmittelbar zur Verfügung stehen.

Tz. 110 In dieser Betrachtung wurde die Gemeinde Nordstemmen nicht berücksichtigt, da sie die technischen Notfallmaßnahmen durch die vollständige Auslagerung des IT-Betriebs auf ein zertifiziertes Rechenzentrum ausgelagert hatte (Tz. 53).

Tz. 111 Die verbleibenden Kommunen gaben an, dass die Rücksicherungsmedien, wie z. B. Datenträgerdateien oder Bandlaufwerke, im Notfall zur Verfügung stehen und auch die wesentlichen Informationen zur Behebung des Notfalls vorhanden sind.

5.5 Dokumentation von Notfällen zur späteren Auswertung

Tz. 112 Alle dem Notfallplan zugrunde liegenden Geschäftsprozesse, technische Verfahren oder Bedrohungsszenarien unterliegen einem fortgesetzten Wandel. Das Notfallmanagement bleibt folglich nur dann aktuell, wenn regelmäßig geprüft wird, ob die eingeführten Konzepte, Maßnahmen und organisatorischen Regelungen noch angemessen und zeitgemäß sind.

Tz. 113 Insbesondere nach der Durchführung von Notfallmaßnahmen muss die Wirksamkeit analysiert und das Ergebnis dokumentiert werden, um die Reaktionsfähigkeit möglichst aktuell zu halten.

Tz. 114 Allerdings ist nicht jede Fehlfunktion von Hardware oder Software ein IT-Notfall, sondern vielfach lediglich eine Störung, die in der Regel im Tagesgeschäft behoben werden kann.

Tz. 115 Ein Notfall, also ein Schadensereignis, bei dem Prozesse oder Ressourcen einer Kommune nicht wie vorgesehen funktionieren und die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen nicht innerhalb einer geforderten Zeit wiederhergestellt werden konnte, lag bisher in keiner der geprüften Kommunen vor.

Tz. 116 Gleichwohl sollten sich alle Kommunen, idealerweise in einem Notfallplan, präventiv eine Dokumentation von Notfallereignissen auferlegen.

Tz. 117 So kann sichergestellt werden, dass geplante Maßnahmen:

- in der Praxis Wirkung entfaltet haben,
- Konzepte, Maßnahmen und organisatorischen Regelungen noch angemessen und aktuell sind,
- Beschäftigte, die eine Notfallfunktion haben, in der geplanten Funktion auch tatsächlich tätig werden und
- geplante Maßnahmen tatsächlich vollumfänglich benötigt wurden oder künftig effizienter gestaltet werden können.

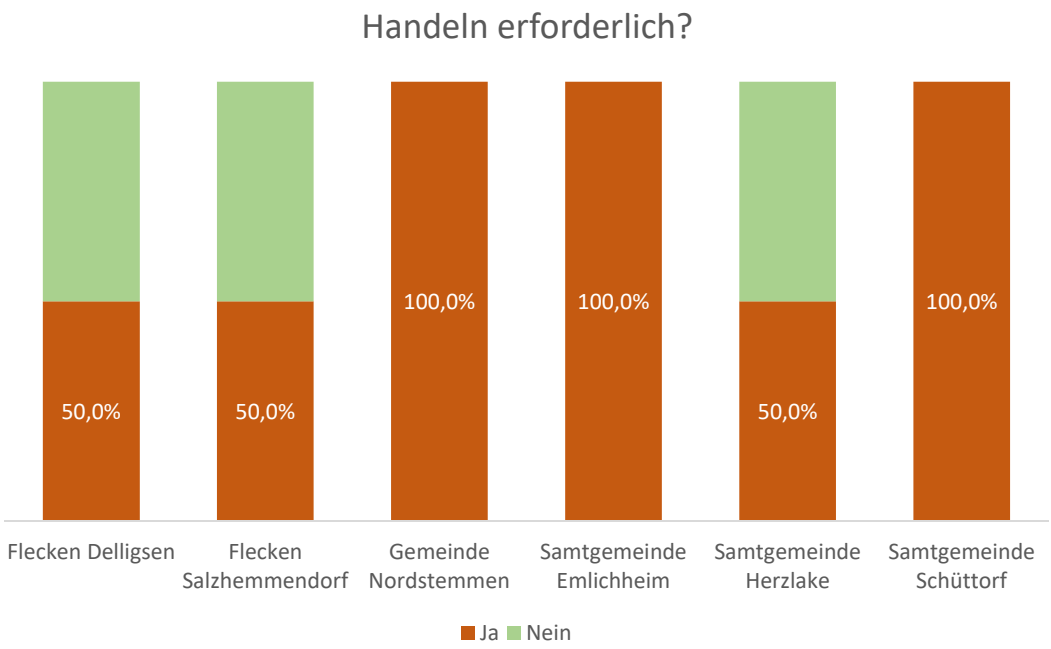
5.6 Durchführung von Notfallübungen

Tz. 118 Notfallübungen sind zentrale Elemente eines funktionierenden Notfallmanagements.

Mittels Notfallübungen werden Notfallpläne auf Aktualität und Effizienz getestet. Zudem sorgen sie bei den Beteiligten für eine Routine bei den umzusetzenden Maßnahmen. Selbst geringfügige Probleme können durch Notfallübungen ausfindig gemacht werden. Dazu zählen nicht aktuelle Ansprechpersonen, Telefonnummern sowie Kommunikations- und Schnittstellenprobleme. Denn selbst „kleinste“ Unstimmigkeiten können im Ereignisfall folgenschwere Auswirkungen haben (z. B. Warnmeldungen gehen ins Leere, weil eine neue Handynummer nicht eingepflegt wurde).

Während einer Übung auftretende Fehler und Unstimmigkeiten müssen in einer sorgfältigen Nachbereitung (vgl. Kapitel 5.5) erörtert und behoben werden.

Tz. 119 Gegenstand dieses Prüfpunkts war zum einen die Beantwortung der Frage, ob alle Beschäftigten wussten, was im Falle eines Notfalls zu tun ist („Wen alarmiere ich?"; „Was mache ich zuerst?") und zum anderen, ob das ggf. vorliegende theoretische



Wissen praktisch durch Notfallübungen überprüft wurde.

Abbildung 12 - Handlungsbedarf Prüfgebiet Notfallübung

Tz. 120 Die Gemeinde Nordstemmen sowie die Samtgemeinden Emlichheim und Schüttorf gaben an, ihre Beschäftigten nicht informiert zu haben, wie sie sich im Notfall zu verhalten haben. Notfallübungen wurden nicht durchgeführt. Die weiteren drei geprüften Kommunen erklärten, dass ihre Beschäftigten theoretisch wissen, was zu tun ist. Diese Kommunen führten bisher aber ebenfalls keine praktischen Notfallübungen durch.

Tz. 121 Den Kommunen wird empfohlen, die Inhalte der Notfallmaßnahmen in ihre Schulungs- und Sensibilisierungsmaßnahmen aufzunehmen und praktisch zu üben. Ein erster Schritt könnte die Einführung der „Notfallkarte" (Tz. 91) sein.

Tz. 122 Auch Kommunen, wie z. B. die Gemeinde Nordstemmen, die den technischen Betrieb ihrer IT-Infrastruktur auf einen Dienstleister ausgelagert haben, müssen be-

rücksichtigen, dass zur Vorbereitung auf Notfallszenarien auch die eigene Organisation vorbereitet werden muss. Hierfür müssen Abläufe geplant und die Beschäftigten entsprechend sensibilisiert und eingewiesen werden, damit die in Anspruch genommenen Dienstleister unmittelbar in die Bewältigung eines Vorfalls eingebunden werden können. Hierbei müssen alle verwaltungsorganisatorischen Maßnahmen, wie Dokumentationen, Einbindung der Beschäftigten oder Handlungsanweisungen innerhalb der Verwaltung einem Notfallmanagement genügen. Es genügt nicht, sich ausschließlich auf die Einhaltung der technischen und organisatorischen Maßnahmen beim beauftragten Dienstleister zu verlassen, da dieser nicht in die Arbeitsabläufe der Kommune vor Ort (Stichwort „Social Engineering“[46]) eingebunden ist.

Tz. 123 Um den praktischen Einstieg in ein IT-Notfallmanagement zu erleichtern, hat das BSI in einem „One-Pager“[47] eine Anleitung erstellt. Die dort aufgeführten Maßnahmen gliedern sich in die vier Phasen Vorbereitung, Bereitschaft, Bewältigung und Nachbereitung. Alle Punkte sind handlungsorientiert formuliert und unmittelbar umsetzbar.

6 Fazit

Tz. 124 Mit der vorliegenden Prüfung hat die überörtliche Kommunalprüfung an den Prüfungsschwerpunkt Informationstechnologie, Informationssicherheit und Datenschutz angeknüpft. Vertiefend wurde dabei das Notfallmanagement in kleineren Kommunen betrachtet. Dabei ist im Ergebnis festzustellen, dass im Gegensatz zu vorangegangenen Prüfungen in dieser Prüfung alle Kommunen einen externen Datenschutzbeauftragten bestellt hatten (vgl. Kommunalbericht 2018, Kapitel 5.7).[48] Außerdem hatten – bis auf eine – sämtliche geprüften Kommunen jetzt ein Verzeichnis der Verarbeitungstätigkeiten nach den Vorgaben der DSGVO erstellt. In der 2019 zu diesem Thema durchgeführten Prüfung[49] war dies nur bei zwei Dritteln der Fall.

---

[46] Beim Social Engineering geht es um die zwischenmenschliche Beeinflussung einer Person. Dabei versucht der Hacker das Vertrauen des Opfers zu gewinnen und ihn so zum Beispiel zur Preisgabe von vertraulichen Informationen oder zur Freigabe von Kreditkartendaten und Passwörtern zu bewegen.

[47] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/One-Pager_Einstieg_ins_IT-Notfallmanagement_KMU.pdf;jsessionid=F9453D3868536AFC13ED69B2916D621A.internet482?__blob=publicationFile&v=5.

[48] Nur vier von insgesamt zehn Kommunen hatten zum damaligen Zeitpunkt einen externen Datenschutzbeauftragten beauftragt. Fünf Kommunen bestellten einen internen Datenschutzbeauftragten, eine Kommune hatte zum Prüfungszeitpunkt gar keinen Datenschutzbeauftragten. Die Zahl der Handlungsbedarfe fiel in Kommunen mit einem internen Datenschutzbeauftragten im Mittel um 34 % höher aus als in Kommunen, die einen externen Datenschutzbeauftragten bestellt hatten. Zugleich waren die Aufwendungen bei der externen Wahrnehmung der Tätigkeit sogar etwa 19 % geringer.

[49] Die Präsidentin des Niedersächsischen Landesrechnungshofs, Prüfungsmitteilung „Verzeichnis von Verarbeitungstätigkeiten und Auftragsverarbeitung“ (Az.: 10712/6.2-3-2018/2).

Tz. 125 Trotz dieser positiven und begrüßenswerten Entwicklung brachte auch diese Prüfung weitere Handlungsbedarfe zu Tage. Diese liegen überwiegend in den Bereichen Sicherheitsmanagement sowie von Konzepten und Vorgehensweisen und dem Notfallmanagement. Es sind vor allem Strategien, Ziele, Leitlinien und Dokumentationen aufzuarbeiten und Notfallpläne aufzustellen. Auch die Sensibilisierung von Beschäftigten sollte verbindlich geregelt und durch organisatorische Regelungen begleitet werden.

Tz. 126 Die im Rahmen dieser Prüfung bezifferten Produktivverluste geben einen ersten Eindruck von den Schäden, die durch Cyberangriffe insgesamt entstehen können und zeigen aus Sicht der überörtlichen Kommunalprüfung einen deutlichen Praxisbezug der geprüften Themenbereiche auf.

Tz. 127 Vor diesem Hintergrund wird die überörtliche Kommunalprüfung auch im Jahr 2022 eine vergleichbare Prüfung durchführen.

Im Auftrag

Heike Fliess

Fragenkatalog der überörtlichen Kommunalprüfung

Fragen Nr.	Kommune	Prüfgebiet	Prüfpunkt	Fragen	Antwort	Handeln erforderlich?
1	**Samtgemeinde Herzlake**	Sicherheitsmanagement	Strategie und Leitlinie	Gibt es eine behördenspezifische Leitlinie zur Informationssicherheit?	Nein	**Ja**
2	**Samtgemeinde Herzlake**	Sicherheitsmanagement	Strategie und Leitlinie	Wurde diese von der Behördenleitung verabschiedet?	Trifft nicht zu	**Trifft nicht zu**
3	**Samtgemeinde Herzlake**	Sicherheitsmanagement	Strategie und Leitlinie	Wurde und wird die Leitlinie allen Mitarbeitern bekanntgegeben?	Trifft nicht zu	**Trifft nicht zu**
4	**Samtgemeinde Herzlake**	Sicherheitsmanagement	IT-Sicherheitsbeauftragter	Ist ein IT-Sicherheitsbeauftragter benannt?	Nein	
5	**Samtgemeinde Herzlake**	Sicherheitsmanagement	IT-Sicherheitsbeauftragter	Ist dieser vom Fachwissen her für die Aufgabe geeignet?	Trifft nicht zu	**Trifft nicht zu**
6	**Samtgemeinde Herzlake**	Sicherheitsmanagement	IT-Sicherheitsbeauftragter	Verfügt dieser über ausreichend zeitliche Ressourcen, um seine Aufgaben wahrnehmen zu können?	Trifft nicht zu	**Trifft nicht zu**
7	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Regelung organisatorischer Maßnahmen	Bestehen Regelungen zur Nutzung des E-Mail-Accounts / Webzugangs zu geschäftlichen / privaten Zwecken?	Nein	**Ja**
8	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Regelung organisatorischer Maßnahmen	Ist die Entsorgung von Daten geregelt (in Papierform oder auf elektronischen Medien)?	Nein	**Ja**
9	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Regelung organisatorischer Maßnahmen	Gibt es schriftliche Anweisungen zum Verhalten bei Datenpannen und Sicherheitsverstößen?	Nein	**Ja**
10	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Regelung organisatorischer Maßnahmen	Wurden die Regelungen innerhalb der letzten 24 Monate aktualisiert?	Trifft nicht zu	**Trifft nicht zu**
11	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Sicherungskonzept	Gibt es ein dokumentiertes IT-Sicherungskonzept?	Nein	**Ja**
12	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Sicherungskonzept	Ist im Sicherungskonzept die Wichtigkeit der Verfahren und Daten beschrieben?	Trifft nicht zu	**Trifft nicht zu**
13	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Sicherungskonzept	Ist im Sicherungskonzept die Sicherungsart geregelt?	Trifft nicht zu	**Trifft nicht zu**
14	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Sicherungskonzept	Ist im Sicherungskonzept der Sicherungsrhythmus vorgegeben?	Trifft nicht zu	**Trifft nicht zu**
15	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Sicherungskonzept	Sind im Sicherungskonzept Verantwortlichkeiten eindeutig geregelt?	Trifft nicht zu	**Trifft nicht zu**

16	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Umgang mit mobilen Geräten / Datenträgern	Gibt es schriftliche Regelungen zur Nutzung von dienstlichen mobilen Geräten?	Nein	**Ja**
17	**Samtgemeinde Herzlake**	Konzepte und Vorgehensweisen	Umgang mit mobilen Geräten / Datenträgern	Gibt es schriftliche Regelungen zur Nutzung von privaten mobilen Geräten zur dienstlichen Nutzung?	Nein	**Ja**
18	**Samtgemeinde Herzlake**	Infrastruktur	Schutzmaßnahmen	Gibt es besondere Gebäudesicherheitsmaßnahmen (z. B. Alarmsysteme)?	Nein	**Ja**
19	**Samtgemeinde Herzlake**	Infrastruktur	Zutrittsmöglichkeiten	Bleiben Türen zu Bereichen, die nicht dem Publikumsverkehr dienen, konsequent verschlossen?	Ja	**Nein**
20	**Samtgemeinde Herzlake**	Infrastruktur	Besucher	Ist sichergestellt, dass Unbefugte nicht in sensible Bereiche wie Verwaltung, IT oder Personal gelangen?	Nein	**Ja**
21	**Samtgemeinde Herzlake**	Infrastruktur	Besucher	Gibt es schriftliche Anweisungen für Beschäftigte, worauf sie zu achten haben und wie mit auffälligen Personen umzugehen ist?	Nein	**Ja**
22	**Samtgemeinde Herzlake**	Infrastruktur	Lieferanten/ Externe Dienstleister	Dürfen sich Lieferanten und externe Dienstleister nur unter Aufsicht in den höheren Sicherheitszonen, z.B. nichtöffentlichen Bereichen, bewegen?	Ja	**Nein**
23	**Samtgemeinde Herzlake**	Infrastruktur	Lieferanten/ Externe Dienstleister	Werden die Identität des Externen und die Richtigkeit des Auftrags vor Zugriff auf Informationen überprüft (unabhängig ob elektronisch oder in Papierform)?	Ja	**Nein**
24	**Samtgemeinde Herzlake**	Infrastruktur	Lieferanten/ Externe Dienstleister	Werden Zugriffe durch oder Übergaben an Dritte (z.B. Dienstleister, Landkreis o.ä.) protokolliert?	Nein	**Ja**
25	**Samtgemeinde Herzlake**	Infrastruktur	Brandmeldesystem	Sind Rauchmelder in allen Gebäuden vorhanden?	Ja	**Nein**
26	**Samtgemeinde Herzlake**	Infrastruktur	Brandmeldesystem	Wird das Brandmeldesystem regelmäßig geprüft und das Ergebnis dokumentiert?	Ja	**Nein**
27	**Samtgemeinde Herzlake**	Infrastruktur	Brandmeldesystem	Ist die automatisierte Benachrichtigung der richtigen Ansprechpartner im Falle eines Auslösens sichergestellt?	Nein	**Ja**
28	**Samtgemeinde Herzlake**	Infrastruktur	Brandschutzgeräte	Existieren deutliche und ausreichend viele Hinweisschilder auf die Standorte der Brandschutzgeräte? (Im Zweifel sind das mehr Hinweise als sie der Brandschutz rechtlich vorsieht.)	Ja	**Nein**
29	**Samtgemeinde Herzlake**	Infrastruktur	Brandschutzgeräte	Werden die Brandschutzgeräte regelmäßig gewartet / geprüft?	Ja	**Nein**
30	**Samtgemeinde Herzlake**	Infrastruktur	Brandschutzgeräte	Sind Mitarbeiter in die Brandbekämpfung eingewiesen oder dafür speziell ausgebildet?	Ja	**Nein**
31	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Existieren Brandschutzgeräte im IT-Bereich / Serverraum?	Ja	**Nein**
32	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Gibt es gesonderte Serverräume?	Ja	**Nein**

33	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Wurde auf eine gesonderte Kennzeichnung der Serverräume verzichtet? (Schilder wie „Serverraum“, „Technikraum“ oder „Zutritt nur für Befugte“ sind eine Einladung!)	Ja	**Nein**
34	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Liegt der Serverraum geschützt im Inneren des Gebäudes?	Ja	**Nein**
35	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Verfügt der Serverraum ausschließlich über eine Zugangstür?	Ja	**Nein**
36	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Ist der Serverraum ohne Fenster?	Ja	**Nein**
37	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Sind zum Serverraum Türen mit Schutzklasse verbaut? (z. B. aus Metall, Zargen, Sicherheitsschlösser, Aushebelschutz etc.)?	Ja	**Nein**
38	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Sind diese mit separaten Schlüsseln zu öffnen?	Ja	**Nein**
39	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Ist eine Alarmierungen für Glasbruch eingerichtet?	Nein	**Ja**
40	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Ist eine Alarmierung für eine Zeitüberschreitung der Türöffnung eingerichtet?	Nein	**Ja**
41	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Gibt es eine Videoüberwachung im Innenbereich des Serverraums?	Nein	**Ja**
42	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Liegt der Serverraum in einem eigenen Brandabschnittsbereich?	Ja	**Nein**
43	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Werden schwer brennbare Bodenbeläge verwendet?	Nein	**Ja**
44	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Sind Brand- und Wassermelder installiert und wird deren Funktion regelmäßig geprüft?	Nein	**Ja**
45	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Führen Wasser-Zu- und Ableitungen durch den Serverraum?	Nein	**Nein**
46	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Liegen über dem Serverraum wasserführende Räumen wie z.B Küche oder Sanitär?	Nein	**Nein**
47	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Wird der Serverraum zusätzlich als Lager (Papier, Putzmittel etc.) oder Archiv genutzt?	Nein	**Nein**
48	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Ist sichergestellt, dass **Netzwerkverteiler/Patch-Schränke** stets verschlossen sind und nur ein beschränkter Mitarbeiterkreis Zugang hat?	Ja	**Nein**
49	**Samtgemeinde Herzlake**	Infrastruktur	Serverraum	Ist sichergestellt, dass **Serverschränke** stets verschlossen sind und nur ein beschränkter Mitarbeiterkreis Zugang hat?	Ja	**Nein**

50	**Samtgemeinde Herzlake**	Infrastruktur	Schlüsselvergabe	Sind Ausgabe, Rücknahme, Tausch und Ersatz von Schlüsseln, Code-Karten, PINs nachvollziehbar dokumentiert und existieren hierfür feste Verfahrensweisen?	Ja	**Nein**
51	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Berechtigungen	Existieren Gruppen, mittels derer Nutzer ihre Zugriffsrechte zugeteilt bekommen?	Nein	**Ja**
52	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Berechtigungen	Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?	Nein	**Ja**
53	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Bildschirmschoner mit Kennwortabfrage	Ist nach spätestens 10 Minuten ein automatischer Start des Bildschirmschoners mit Kennwortabfrage eingerichtet?	Ja	**Nein**
54	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Geräteschutz	Ist die Bootreihenfolge auf der Festplatte als erstes Medium eingestellt?	Nein	**Ja**
55	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Geräteschutz	Ist die Auswahl der Bootreihenfolge beim Systemstart abgeschaltet?	Nein	**Ja**
56	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Geräteschutz	Ist ein BIOS-Passwort gesetzt?	Nein	**Ja**
57	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Geräteschutz	Ist ein Schutz vor Gehäuseöffnung eingerichtet bzw. Warnmeldung aktiviert?	Nein	**Ja**
58	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Geräteschutz	Sind externe Anschlüsse z. B. USB-Ports, Kartenleser und Laufwerke grundsätzlich deaktiviert oder werden diese aktiv verwaltet?	Nein	**Ja**
59	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Passwortsicherheit	Muss ein Nutzer beim Login an seinem PC-Arbeitsplatz ein sicheres Passwort eingeben?	Ja	**Nein**
60	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Passwortsicherheit	Muss ein Nutzer beim Login in allen einzelnen Fachverfahren ein sicheres Passwort eingeben?	Ja	**Nein**
61	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Passwortsicherheit	Existieren schriftliche Richtlinien, wie ein sicheres Passwort auszusehen hat (Mindestlänge, Zusammensetzung, Lebensdauer)?	Nein	**Ja**
62	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Passwortsicherheit	Werden diese Richtlinien durchgängig beim Login (Gruppenrichtlinie und in den Verfahren) technisch erzwungen?	Ja	**Nein**
63	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Passwortsicherheit	Sind die Mitarbeiter schriftlich angewiesen, die Richtlinien eigenverantwortlich einzuhalten, wenn es keinen technischen Zwang innerhalb des Verfahrens gibt?	Nein	**Ja**
64	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Umgang mit Kennwörtern	Existieren personenbezogene Administrations-Accounts zwecks Nachvollziehbarkeit?	Ja	**Nein**
65	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Umgang mit Kennwörtern	Wird der eigentliche Administrations-Account „Admin“ nur im Notfall genutzt?	Ja	**Nein**
66	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Umgang mit Kennwörtern	Werden voreingestellte Admin-Passwörter (Auslieferungszustand) direkt bei der ersten Nutzung geändert?	Ja	**Nein**

67	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Umgang mit Kennwörtern	Sind alle wichtigen Kennwörter in einem besonders geschützten Passwortcontainer abgelegt und in ausgedruckter Form im Datenschutz-Tresor hinterlegt?	Nein	**Ja**
68	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Zugriffsvergabe	Gibt es festgeschriebene Anlässe aufgrund derer Zugriffsrechte vergeben und entzogen werden? (z.B. bei Anforderung eines Arbeitsplatzes, Wechsel eines Mitarbeiters, Ausscheiden etc.)	Ja	**Nein**
69	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Zugriffsvergabe	Existiert hierfür ein Formular (Papierform oder elektronisch), auf dem alle relevanten Informationen und Arbeitsschritte festgehalten werden? (z. B. Anforderung, Grund, Prüfung, Freigabe, Bestätigung der Umsetzung)	Nein	**Ja**
70	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Manueller Logout	Sind alle Mitarbeiter schriftlich angewiesen, sich bei Verlassen des Arbeitsplatzes (auch für kurze Zeit) manuell vom System abzumelden?	Nein	**Ja**
71	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Umgang bei zeitweisen Beschäftigungen	Ist der Rechteentzug für zeitweise Beschäftigungsverhältnisse oder bei Ausscheiden geregelt?	Nein	**Ja**
72	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Zugriff, Änderung, Löschung	Kann in den Systemen die datenschutzkonforme Protokollierung von Zugriffen auf Daten, deren Änderung und Löschung sichergestellt werden?	Nein	**Ja**
73	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Zugriff, Änderung, Löschung	Kann in den Fachverfahren die datenschutzkonforme Protokollierung von Zugriffen auf Daten, deren Änderung und Löschung sichergestellt werden?	Ja	**Nein**
74	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Verschlüsselung / Signaturverfahren	Sind Dateien, Verzeichnisse und Laufwerke mit schutzbedürftigen Daten nach dem aktuellen Stand der Technik verschlüsselt?	Ja	**Nein**
75	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Verschlüsselung / Signaturverfahren	Sind mobile Datenträger (Sticks) und Geräte (Notebooks, Tablets, Smartphones) in die Verschlüsselung mit einbezogen?	Trifft nicht zu	**Trifft nicht zu**
76	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Verschlüsselung / Signaturverfahren	Kommen bei elektronischer Übertragung von Daten entsprechende Signatur- und Verschlüsselungsverfahren zum Einsatz?	Ja	**Nein**
77	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Telearbeit/Home Office	Wird die Möglichkeit von Home Office/Telearbeit angeboten?	Ja	**Nein**
78	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Telearbeit/Home Office	Haben Sie die Anzahl an Home Office-Arbeitsplätzen aufgrund der Corona Pandemie ausgeweitet?	Ja	**Nein**
79	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Telearbeit/Home Office	Werden hierfür dienstliche Computer genutzt?	Ja	**Nein**
80	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Telearbeit/Home Office	Werden hierfür private Computer genutzt?	Ja	**Nein**
81	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Telearbeit/Home Office	Werden Sie nach den gemachten Erfahrungen auch künftig Home Office anbieten?	Ja	
82	**Samtgemeinde Herzlake**	Zugang zu IT-Systemen	Telearbeit/Home Office	Haben Sie eine Dienstanweisung zu Home Office/Telearbeit erlassen?	Nein	**Ja**

83	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Firewall	Wird eine dem Stand der Technik entsprechende Firewall-Lösung zum Schutz vor Zugriffen von außen eingesetzt?	Ja	**Nein**
84	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Firewall	Sind die Funktionen der Firewall bekannt und dokumentiert?	Ja	**Nein**
85	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Virenschutz	Werden Mitarbeiter über außerordentliche, aktuelle Bedrohungen informiert?	Ja	**Nein**
86	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Virenschutz	Sind sowohl client- als auch serverseitig Virenschutzmaßnahmen installiert?	Ja	**Nein**
87	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Virenschutz	Werden Updates sowohl auf dem Server als auch auf Clients sichergestellt?	Ja	**Nein**
88	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Unterbrechungsfreie Stromversorgung	Sind die Systeme vor Stromausfällen mittels unterbrechungsfreier Stromversorgung gesichert?	Ja	**Nein**
89	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Unterbrechungsfreie Stromversorgung	Werden die USV regelmäßig gewartet (Akkuprüfung, Austausch)?	Ja	**Nein**
90	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Unterbrechungsfreie Stromversorgung	Werden diese Arbeiten protokolliert?	Ja	**Nein**
91	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Unterbrechungsfreie Stromversorgung	Melden die USV kritische Zustände nicht nur per Leuchtanzeige, sondern ebenfalls über Meldesysteme wie Email / SMS?	Nein	**Ja**
92	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Unterbrechungsfreie Stromversorgung	Werden intelligente USV Systeme eingesetzt, die entsprechende Notaktivitäten einleiten? (Information an Nutzer, Schließen der Datenbanken, Herunterfahren der Systeme etc.)	Ja	**Nein**
93	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Online Datensicherung	Wird eine Online-Datensicherung in eine Cloud oder auf einen externen Server durchgeführt?	Ja	
94	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Online Datensicherung	Sind die Datenübertragung und der Online-Speicher nach aktuellem Stand verschlüsselt?	Ja	**Nein**
95	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Online Datensicherung	Existiert eine genaue Beschreibung des Backups und der Recovery Maßnahmen für den Fall der Nichtverfügbarkeit der Verantwortlichen für das Backup?	Ja	**Nein**
96	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Recovery-Tests	Werden regelmäßig (mind. alle 3-6 Monate) **ereignisunabhängig** Überprüfungen der Backups auf Funktionsfähigkeit durchgeführt?	Nein	**Ja**
97	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Recovery-Tests	Wird das Ergebnis entsprechend dokumentiert?	Trifft nicht zu	**Trifft nicht zu**
98	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Recovery-Tests	Werden Fehlversuche analysiert und deren Ursache zeitnah abgestellt?	Trifft nicht zu	**Trifft nicht zu**
99	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Recovery-Tests	Wird die Fehleranalyse schriftlich dokumentiert?	Trifft nicht zu	**Trifft nicht zu**

100	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Technik	Ist mittels der eingesetzten Sicherungstechnik eine zeitnahe Datenwiederherstellung möglich?	Ja	**Nein**
101	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Technik	Bei Sicherung auf Wechselmedien: Werden diese regelmäßig ausgetauscht, um Ausfällen vorzubeugen?	Trifft nicht zu	**Trifft nicht zu**
102	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Technik	Werden die Sicherungsmedien (Tape, Wechselplatte, NAS) außerhalb des Serverraums gelagert?	Ja	**Nein**
103	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Technik	Werden diese in einem anderen Brandabschnitt gelagert?	Ja	**Nein**
104	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Technik	Ist ein Datensicherungstresor nach Norm S 60 (1 Std. Feuersicherheit für Datenträger) oder S 120 (2 Stunden Feuersicherheit für Datenträger) DIS vorhanden?	Nein	**Ja**
105	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Hat die IT-Abteilung Monitoring Systeme installiert?	Nein	**Ja**
106	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Sind im IT-Bereich Monitoring Systeme für Temperatur im Serverraum installiert?	Nein	**Ja**
107	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Sind im IT-Bereich Monitoring Systeme für Feuchtigkeit installiert?	Nein	**Ja**
108	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Sind im IT-Bereich Monitoring Systeme für unbefugter Zutritt / Einbruch eingerichtet?	Nein	**Ja**
109	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Sind im IT-Bereich Monitoring Systeme für fehlerhafte Backups eingerichtet?	Ja	**Nein**
110	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Sind im IT-Bereich Monitoring Systeme bei Verstößen gegen Sicherheitsrichtlinien (unbefugtes Verwenden von USB Sticks, unberechtigte Zugriffsversuche usw.) auf den Systemen eingerichtet?	Nein	**Ja**
111	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Werden bei Alarm eines der Monitoring Systeme SMS oder E-Mail Nachrichten an vorbestimmte Empfänger versendet?	Ja	**Nein**
112	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Sind die Empfänger aktuell oder laufen die Meldungen eventuell ins Leere?	Ja	**Nein**
113	**Samtgemeinde Herzlake**	Notfallmaßnahmen	Überwachung / Monitoring	Sind die informierten Mitarbeiter geschult und eingewiesen, was im Meldefall zu tun ist?	Ja	**Nein**
114	**Samtgemeinde Herzlake**	Notfallmaßnahmen	WLAN	Werden Rechner bzw. Endgeräte über WLAN eingebunden?	Ja	
115	**Samtgemeinde Herzlake**	Notfallmaßnahmen	WLAN	Sofern WLAN eingesetzt wird: Existiert ein Plan über alle WLAN Zugangspunkte / Hotspots?	Ja	**Nein**
116	**Samtgemeinde Herzlake**	Notfallmaßnahmen	WLAN	Sofern WLAN eingesetzt wird: Wird auf sichere Verschlüsselung WPA/WPA2/WPA3 geachtet?	Ja	**Nein**

117	Samtgemeinde Herzlake	Notfallmaßnahmen	Notfalltest	Werden die Notfallmaßnahmen regelmäßig getestet und mit den Mitarbeitern Notfallübungen abgehalten?	Nein	Ja
118	Samtgemeinde Herzlake	DSGVO	Datenschutzbeauftragter	Wurde ein Datenschutzbeauftragter bestellt?	extern	extern
119	Samtgemeinde Herzlake	DSGVO	Datenschutzbeauftragter	Wurde der Datenschutzbeauftragte schriftlich bestellt?	Ja	Nein
120	Samtgemeinde Herzlake	DSGVO	Datenschutzbeauftragter	Wenn ja, ist er gemäß dem Art. 37 Abs. 8 DSGVO der zuständigen Aufsichtsbehörde gemeldet?	Ja	Nein
121	Samtgemeinde Herzlake	DSGVO	Datenschutzbeauftragter	Verfügt der Datenschutzbeauftragte über entsprechende Fachkunde?	Ja	Nein
122	Samtgemeinde Herzlake	DSGVO	Datenschutzbeauftragter	Ist der Datenschutzbeauftragte im Unternehmen bekannt (Intranet, Newsletter, Organigramm etc.)?	Ja	Nein
123	Samtgemeinde Herzlake	DSGVO	Auskunftsrechte Betroffener	Gibt es einen schriftlich festgelegten Prozess, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DSGVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DSGVO)?	Nein	Ja
124	Samtgemeinde Herzlake	DSGVO	Auskunftsrechte Betroffener	Ist dieser Prozess allen Mitarbeitern bekannt?	Trifft nicht zu	Trifft nicht zu
125	Samtgemeinde Herzlake	DSGVO	Auskunftsrechte Betroffener	Wurde in diesem Prozess eine zentrale Anlaufstelle festgelegt?	Trifft nicht zu	Trifft nicht zu
126	Samtgemeinde Herzlake	DSGVO	Auskunftsrechte Betroffener	Wurde die Datenschutzerklärung der Website entsprechend ergänzt?	Ja	Nein
127	Samtgemeinde Herzlake	DSGVO	Datenschutzverletzungen (Art. 33, 34 DSGVO)	Ist sichergestellt, dass Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden (Art. 33 DSGVO)?	Ja	Nein
128	Samtgemeinde Herzlake	DSGVO	Datenschutzverletzungen (Art. 33, 34 DSGVO)	Haben Sie einen Prozess aufgesetzt, wie mit solchen Verletzungen intern umzugehen ist?	Nein	Ja
129	Samtgemeinde Herzlake	DSGVO	Datenschutzverletzungen (Art. 33, 34 DSGVO)	Haben Sie schriftlich festgelegt, welche Person, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert?	Nein	Ja
130	Samtgemeinde Herzlake	DSGVO	Auftragsverarbeitung	Sind externe Dienstleister zur Erledigung von Arbeiten (Auftragsverarbeiter, wie Rechenzentren, Landkreis o.ä.) eingebunden?	Ja	Nein
131	Samtgemeinde Herzlake	DSGVO	Auftragsverarbeitung	Wenn ja, gibt es eine zentrale Übersicht über die Auftragsverarbeiter?	Ja	Nein
132	Samtgemeinde Herzlake	DSGVO	Auftragsverarbeitung	Haben Sie mit allen Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DSGVO abgeschlossen?	Ja	Nein
133	Samtgemeinde Herzlake	DSGVO	Auftragsverarbeitung	Wurde das Datenschutz- und Datensicherheitsniveau der externen Dienstleister vor Vertragsabschluss geprüft?	Nein	Ja

134	Samtgemeinde Herzlake	DSGVO	Technische und organisatorische Maßnahmen	Wurden die Prüfungen des externen Dienstleisters und die Ergebnisse schriftlich dokumentiert?	Trifft nicht zu	Trifft nicht zu
135	Samtgemeinde Herzlake	DSGVO	Verzeichnis der Verarbeitungstätigkeiten	Gibt es ein Verzeichnis der Verarbeitungstätigkeiten (VVT) gem. Art. 30 DSGVO?	Ja	Nein
136	Samtgemeinde Herzlake	DSGVO	Verzeichnis der Verarbeitungstätigkeiten	Ist dieses Verzeichnis aktuell und vollständig?	Nein	Ja
137	Samtgemeinde Herzlake	Personal und Organisation	Sensibilisierung	Werden Mitarbeiter für die Themen Datenschutz und Datensicherheit sensibilisiert?	Ja	Nein
138	Samtgemeinde Herzlake	Personal und Organisation	Sensibilisierung	Finden regelmäßig, spätestens alle zwei Jahre, Schulungen zur Auffrischung statt?	Ja	Nein
139	Samtgemeinde Herzlake	Personal und Organisation	Daten- und Fernmeldegeheimnis	Wurden Mitarbeiter mit Außenkontakt (Bürgerbüro, Telefonzentrale, Ansprechpartner für Bürger etc.) sowie Mitarbeiter mit regelmäßigem Zugriff auf Verbindungsdaten (z.B. IT-Mitarbeiter) auf das Fernmeldegeheimnis nach § 88 TKG verpflichtet?	Ja	Nein
140	Samtgemeinde Herzlake	Personal und Organisation	Daten- und Fernmeldegeheimnis	Ist dies in Schriftform erfolgt?	Nein	Ja
141	Samtgemeinde Herzlake	Notfallmanagement	Risikoanalyse	Haben Sie eine Vorstellung, was ein vollständiger Ausfall Ihrer IT pro Tag an Kosten verursacht?	Nein	Ja
142	Samtgemeinde Herzlake	Notfallmanagement	Risikoanalyse	Haben Sie Berechnungen oder Prognosen über die Kosten eines IT Ausfalls erstellt?	Nein	Ja
143	Samtgemeinde Herzlake	Notfallmanagement	Risikoanalyse	Wurde innerhalb der vergangenen 12 Monate eine Risikoanalyse durchgeführt?	Nein	Ja
144	Samtgemeinde Herzlake	Notfallmanagement	Risikoanalyse	Wurden Verfahren in kritische und weniger kritische Systeme klassifiziert?	Ja	Nein
145	Samtgemeinde Herzlake	Notfallmanagement	Risikoanalyse	Wurde die maximal tolerierbare Ausfallzeit von Systemen und Verfahren festgelegt?	Nein	Ja
146	Samtgemeinde Herzlake	Notfallmanagement	Risikoanalyse	Wurde analysiert, welche Risiken die Funktionsfähigkeit der Systeme bedrohen?	Nein	Ja
147	Samtgemeinde Herzlake	Notfallmanagement	Erstellung einer Richtlinie zum Notfallmanagement	Ist ein aktuelles IT-Notfallhandbuch mit konkreten Handlungsanweisungen vorhanden?	Nein	Ja
148	Samtgemeinde Herzlake	Notfallmanagement	Erstellung einer Richtlinie zum Notfallmanagement	Wurden Ihre Notfallanweisungen (z.B. IT-Notfallhandbuch o. ä.) innerhalb der letzten 12 Monate aktualisiert?	Trifft nicht zu	Trifft nicht zu
149	Samtgemeinde Herzlake	Notfallmanagement	Maßnahmenkatalog zum Notfallmanagement	Ist sichergestellt, dass ein aktuelles Notfallhandbuch im IT-Notfall unmittelbar vorliegt (z. B. Alarmierungs- und Meldewege)?	Trifft nicht zu	Trifft nicht zu
150	Samtgemeinde Herzlake	Notfallmanagement	Maßnahmenkatalog zum Notfallmanagement	Haben Sie Dienstleister verpflichtet, die Sie bei IT-Notfällen geeignet und zeitgerecht unterstützen können?	Ja	Nein

151	**Samtgemeinde Herzlake**	Notfallmanagement	Maßnahmenkatalog zum Notfallmanagement	Haben Sie eine Liste mit allen Ansprechpartnern und haben mit diesen Vorabsprachen (z.B. Erreichbarkeit, Verfügbarkeit) getroffen?	Ja	**Nein**
152	**Samtgemeinde Herzlake**	Notfallmanagement	Maßnahmenkatalog zum Notfallmanagement	Haben Sie Regeln zur Kommunikation nach innen und außen festgelegt? (Eine erfolgreiche Presse- und Öffentlichkeitsarbeit während eines IT-Notfalls kann einen evtl. Imageschaden erheblich begrenzen.)	Nein	**Ja**
153	**Samtgemeinde Herzlake**	Notfallmanagement	Maßnahmenkatalog zum Notfallmanagement	Haben Sie IT-Notfall-Szenarien (z. B. IT-Ausfälle, Cyber-Angriffe, etc.) praktisch durchgeführt?	Nein	**Ja**
154	**Samtgemeinde Herzlake**	Notfallmanagement	Maßnahmenkatalog zum Notfallmanagement	Haben Sie Ihre IT-Infrastruktur auf Angreifbarkeit prüfen (Penetrationstest) lassen?	Nein	**Ja**
155	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Existiert ein schriftlicher Notfallplan?	Nein	**Ja**
156	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Basiert der Notfallplan auf einer Risikoanalyse?	Trifft nicht zu	**Trifft nicht zu**
157	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Ist dieser Notfallplan den Mitarbeitern bekannt gemacht?	Trifft nicht zu	**Trifft nicht zu**
158	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Wird dieser Notfallplan an einem fest definierten Ort aufbewahrt?	Trifft nicht zu	**Trifft nicht zu**
159	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Sind alle notwendigen Handlungsabläufe nachvollziehbar dokumentiert, sodass auch z.B. externe Kräfte oder Personen, die nicht an der Erstellung beteiligt waren, tätig werden können?	Trifft nicht zu	**Trifft nicht zu**
160	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Sind im Notfallplan die Verantwortlichkeiten für die Wiederanlaufmaßnahmen vorgegeben, um eine reibungs- und konfliktlose Umsetzung zu gewährleisten?	Trifft nicht zu	**Trifft nicht zu**
161	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Sind Netzwerkübersichten der eingesetzten Techniken und Systeme dokumentiert?	Ja	**Nein**
162	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Gibt es eine Leitungsübersicht (interne Verkabelung und externe Leitungen, inkl. Beschreibung der Patchfeld-Systematiken)?	Ja	**Nein**
163	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Gibt es eine Übersicht über externe Zulieferer? (Strom, Wasser, Telekommunikation, Datenleitungen, Hardware, Software etc. mit Ansprechpartnern, Rufnummern, (Rahmen-) Vertragsdaten, Leistungsbeschreibung in Kurzform)?	Ja	**Nein**
164	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Wird **Ihre** Hardware ganz oder teilweise durch Dritte betrieben oder betreut? (Nicht Auftragsverarbeitung)	Nein	
165	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Gibt es eine Übersicht über externe Dienstleister? (z.B. für Installation, Wartung, Konfiguration, Support, Fehlerbehebung etc. mit Ansprechpartnern, Rufnummern, Vertragsdaten/Leistungsbeschreibung)?	Ja	**Nein**

166	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Gibt es ein Verzeichnis der im Einsatz befindlichen Hard- und Software sowohl für Server als auch für Arbeitsplätze?	Nein	**Ja**
167	**Samtgemeinde Herzlake**	Notfallmanagement	Notfallplan	Gibt es eine Übersicht über auf allen Geräten installierte Software?	Nein	**Ja**
168	**Samtgemeinde Herzlake**	Notfallmanagement	Behebung von Notfällen	Stehen alle Informationen (z. B. Passwörter und Lieferanteninformationen) im Falle eines Notfalles zentral zur Verfügung?	Ja	**Nein**
169	**Samtgemeinde Herzlake**	Notfallmanagement	Behebung von Notfällen	Stehen die Backup-Medien für das Rücksichern der Daten zur Verfügung?	Ja	**Nein**
170	**Samtgemeinde Herzlake**	Notfallmanagement	Dokumentation von Notfällen zur späteren Auswertung	Wurden bisherige Notfälle für die anschließende Analyse dokumentiert?	Trifft nicht zu	**Trifft nicht zu**
171	**Samtgemeinde Herzlake**	Notfallmanagement	Durchführung von Notfallübungen	Wurden in der Organisation Notfallübungen durchgeführt?	Nein	**Ja**
172	**Samtgemeinde Herzlake**	Notfallmanagement	Durchführung von Notfallübungen	Wissen die Mitarbeiter, wer im Falle eines Notfalles zu alarmieren ist und welche Maßnahmen zuerst zu ergreifen sind?	Ja	**Nein**

Berechnung Ausfallkosten Personal Samtgemeinde Herzlake

Allgemeine Verwaltung

BesG/EG-Gruppen	Anzahl Clients	Anzahl VZÄ	% Zeitanteil mit IuK Technik	Ø P-Kosten gem. KGSt [1]	Kosten Ausfall je Stunde	Kosten Ausfall je Tag	Kosten Ausfall je Woche	Jahr
EG 1-4 und vergl. BesG A1-A5	0,00	0,00	0,00	46.566,67 €	0,00 €	0,00 €	0,00 €	0,00 €
EG 5-9a und vergl. BesG A6 bis A9	23	21,3	75%	60.950,00 €	598,08 €	4.784,65 €	23.923,25 €	973.676,25 €
EG 9b - 12 und vergl. BesG A9 bis A 13	9	8,1	75%	79.036,36 €	294,93 €	2.359,44 €	11.797,20 €	480.145,91 €
> EG 12 und vergl. BesG >A 13	2	1,0	75%	120.890,00 €	55,69 €	445,54 €	2.227,70 €	90.667,50 €

Sozial- und Erziehungs-dienst

S-Gruppen	Anzahl Clients	Antahl VZÄ	% Zeitanteil mit IuK Technik	Ø P-Kosten gem. KGSt [1]	Kosten Ausfall je Stunde	Kosten Ausfall je Tag	Kosten Ausfall je Woche	Jahr
S 2 - S 8b	0,00	0,00	0,00	57.400,00 €	0,00 €	0,00 €	0,00 €	0,00 €
S 9	0,00	0,00	0,00	67.300,00 €	0,00 €	0,00 €	0,00 €	0,00 €
S 11a - S 18	0,00	0,00	0,00	76.880,00 €	0,00 €	0,00 €	0,00 €	0,00 €

[1]Eigenen Berechnung: Mittelwert auf Basis KGSt Bericht Nr. 07/2020 - Kosten eines Arbeitsplatzes 2020/2021