# Kommunaler Notbetrieb

Jens Lange
Silberbornstraße 53
34134 Kassel
0561 770722
post@kommunaler-notbetrieb.de
https://kommunaler-notbetrieb.de

Jens Lange | Silberbornstraße 53 | 34134 Kassel

An
Herrn Claus Christian Claussen
Vorsitzender des Wirtschafts- und Digitalisierungsausschusses

per E-Mail an: wirtschaftsausschuss@landtag.ltsh.de

Datum: 21. März 2024

**Bericht über die Cybersicherheit unserer Infrastruktur**
Bericht der Landesregierung
Drucksache 20/1584

Schleswig-Holsteinischer Landtag
Umdruck 20/2966

# Schriftliche Stellungnahme zur Anhörung

## Anlass

Der Wirtschafts- und Digitalisierungsausschuss des Schleswig-Holsteinischen Landtags hat mich mit Schreiben vom 28. Februar 2024 um eine schriftliche Stellungnahme zu dem *„Bericht über die Cybersicherheit unserer Infrastruktur“* (nachfolgend „Bericht“ genannt) der Landesregierung (Drucksache 20/1584) gebeten. Dem komme ich hiermit gerne nach.

## Vorbemerkung

Ich bin im Rahmen meines privaten Projektes *„Kommunaler Notbetrieb“* vom Wirtschafts- und Digitalisierungsausschuss des Schleswig-Holsteinischen Landtags für eine Stellungnahme angefragt worden. Auf der Webseite Kommunaler-Notbetrieb.de sammle ich öffentliche Informationen und Meldungen über IT-Sicherheitsvorfälle in Kommunalverwaltungen. Ich weise darauf hin, dass ich hauptberuflich als Informationssicherheitsbeauftragter der Stadtverwaltung Kassel tätig bin, diese Stellungnahme aber nicht in dieser Funktion verfasst habe. Mit meiner beruflichen Expertise, den Erkenntnissen des Projektes *„Kommunaler Notbetrieb“* und als Mitglied diverser Arbeitsgruppen der kommunalen Spitzenverbände (z. B. AG kommunale Basis-Absicherung, AG BCM Länder/Kommunen, AG Handreichung Informationssicherheitsleitlinie) werde ich meine Betrachtung des Berichts ausschließlich auf die kommunalen Aspekte fokussieren.

## Cybersicherheit vs. IT-Sicherheit vs. Informationssicherheit

Auf Antrag der Fraktion des SSW hat der Schleswig-Holsteinische Landtag die Landesregierung aufgefordert, einen *„Bericht zur Cybersicherheit unserer Infrastruktur“* vorzulegen. Cybersicherheit ist neben der IT-Sicherheit ein Schlüsselbegriff der Informationssicherheit. Das Verständnis der Bedeutung und der Unterschiede zwischen diesen Schlüsselbegriffen ist wichtig. Cybersicherheit konzentriert sich auf den Schutz von Daten und Systemen in vernetzten virtuellen Räumen (Cyberraum), insbesondere vor Bedrohungen aus dem Internet. IT-Sicherheit hat ein breiteres Ziel und umfasst den Schutz aller Informationstechnologien (Hardware, Software, Daten) vor jeglichen Formen von Bedrohungen, sowohl intern als auch extern. Informationssicherheit ist der umfassendste Bereich, der den Schutz aller Arten von Informationen (digital und physisch) vor unbefugtem Zugriff, Verlust oder Beschädigung anstrebt. Obwohl sich ihre spezifischen Schwerpunkte unterscheiden, verfolgen alle drei das gemeinsame Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationssystemen zu gewährleisten, und sie überschneiden sich in ihren Strategien und Maßnahmen. Der Bericht weist im Kapitel 2.1. Informations- und Cybersicherheit

daraufhin, versäumt jedoch auf die Gefahr einzugehen, dass bei einer Fokussierung auf die Cybersicherheit, die spezifischen Bedrohungen der Informationssicherheit außerhalb des Cyberraums aus dem Sichtfeld geraten. So sind im Jahr 2023 neun kommunale IT-Sicherheitsvorfälle in der Meldekategorie *„Störung Soft- oder Hardware"* bekannt geworden, die 21 Kommunalverwaltungen betroffen haben. Es ist daher wichtig und richtig, Informationssicherheit als ganzheitlichen Begriff vorrangig zu verwenden.

## Cybersicherheit in der kommunalen Verwaltung

Im Kapitel 3.7 des Berichts wird in einer Art Bestandsaufnahme spezifisch auf die *„Cybersicherheit in der kommunalen Verwaltung"* eingegangen. Neben einer Kurzdarstellung des Projektes *„Sicherheit für Kommunen in Schleswig-Holstein (SiKoSH)"* finden sich noch einige wenige Angaben zu *„Information und Sensibilisierung"* sowie *„Fachtagungen und Vernetzung"*. Dabei wird die zentrale Bedeutung von SiKoSH deutlich, denn ohne die Angebote und Leistungen aus dieser Initiative gäbe es seitens des Landes wenig für die Kommunen zur Verbesserung und Aufrechterhaltung der Informationssicherheit. Dies zeigt auch ein Blick in den *„Cybersicherheitskompass für Kommunen"*[1], in dem die Stiftung Neue Verantwortung e. V. Leistungen von Bund und Ländern zur Förderung der Informationssicherheit und Resilienz von Kommunen dokumentiert hat. Für Kommunen in Schleswig-Holstein werden z. B. keine Leistungen des CERT-Nord angeboten, auf die sie präventiv und im Schadensfall verbindlich sowie direkt zugreifen können.

## „Ausblick" und Empfehlungen

Im Ausblick des Berichts (Kapitel 4) wird die Unterstützung der Kommunen im Handlungsfeld *„Ausbau des Informations- und Cybersicherheitsmanagements der Landesregierung"* aufgeführt. Zu den einzelnen Punkten gebe ich nachfolgende Bewertungen und Empfehlungen:

CERT-Nord

Die geplante Einbindung der Kommunen in das CERT-Nord ist sinnvoll und notwendig. Diese sollte sich nicht auf Warn- und Informationsdienste beschränken, sondern auch die verbindliche Möglichkeit der Inanspruchnahme von Leistungen des Security Operations Centers (SOC) und des mobilen Einsatzteams (MIRT, Mobile Incident Response Team) umfassen. Die Erfahrungen schwerer IT-Sicherheitsvorfälle haben gezeigt, dass vor allem bei Kommunalverwaltungen das Wissen, die Erfahrung und die Ressourcen fehlen, um in den ersten 72 Stunden wesentliche Schritte zur Krisenbewältigung einzuleiten. Das Anfertigen von kommunalen Lagebildern zur Informations- und Cybersicherheit sollte ebenfalls zum Aufgabenspektrum des Landes-CERT gehören.

SiKoSH

Die Verstetigung des Projektes SiKoSH ist absolut geboten. SiKoSH wird überregional unter kommunalen Informations- und IT-Sicherheitsbeauftragten für eine fundierte und effiziente Vorgehensweise geschätzt und anerkannt. So wie Informationssicherheit nicht als Projekt, sondern als Prozess anzusehen ist, sollte SiKoSH dauerhaft etabliert, ausgebaut und weiterentwickelt werden.

Roadshow Kommunen

Das BSI-Angebot *„Roadshow Kommunen"* ist eine virtuelle Veranstaltungsreihe, bei der die Teilnehmenden für die aktuelle Bedrohungslage sensibilisiert werden und konkrete Handlungsempfehlungen erhalten, mit denen sie die Cyber-Resilienz in ihren Kommunen erhöhen können. Das Format hat sich in anderen Bundesländern bereits bewährt, insbesondere, wenn damit die Verwaltungsspitze der Kommunen angesprochen werden. Darauf sollte man in der Umsetzung achten, denn Informationssicherheit ist CheflInnen- und Chefsache.

[1] https://cybersicherheitskompass.de/schleswig-holstein

Förderprogramm *„Kommunale Resilienz“*

Ein Förderprogramm *„Kommunale Resilienz“* kann eine folgerichtige Maßnahme sein, um Städte, Gemeinden und Landkreise gezielt dabei zu unterstützen, ihre Fähigkeit zum Schutz gegen, zur Anpassung an und zur schnellen Erholung von Cyberbedrohungen und anderen Informationssicherheitsrisiken zu verbessern. Bei der Ausgestaltung eines solchen Förderprogramms sollten unbedingt Praktizierende aus den Kommunalverwaltungen einbezogen werden, um effiziente Angebote zu identifizieren. Solch ein Programm könnte folgende Elemente umfassen: Bewusstseinsbildung und Schulungen, technische Unterstützung und Beratung, Zuschüsse für Sicherheitssoftware und -hardware, Entwicklung und Implementierung von Notfallplänen, Förderung der Zusammenarbeit, Auditierungen und Zertifizierungen und rechtliche und regulatorische Unterstützung. Mögliche Synergien mit der Verstetigung von SiKoSH sollten dabei angestrebt werden.

Informationssicherheitsgesetz

Gesetzliche Regelungen zur Informationssicherheit sind auch für Kommunen notwendig, um einheitliche Sicherheitsstandards zu garantieren, die Rechte der Bürger zu schützen und mit technologischen Entwicklungen Schritt zu halten. Sie definieren klare Verantwortlichkeiten und fördern die Rechenschaftspflicht, stärken das Vertrauen in digitale Dienste und stellen sicher, dass Kommunen auf Sicherheitsvorfälle vorbereitet sind. Der Beschluss 2023/39 des IT-Planungsrates mit der Bitte an die Länder, die NIS-2-Richtlinie der EU in der nationalen Umsetzung nicht auf die Kommunen zu erstrecken, basiert auf einer Stellungnahme der AG InfoSic[2]. Es gibt darin eine alternative Empfehlung, die im Beschluss jedoch nicht erwähnt wird: Statt den Anwendungsbereich der NIS-2-Richtlinie auf Kommunen zu auszudehnen, sollten Regelungen für Kommunen außerhalb der NIS-2-Richtlinienumsetzung im jeweiligen Landesrecht geschaffen werden. Das nach Kapitel 4.2.4 des Berichts vorgesehene Informationssicherheitsgesetz für Schleswig-Holstein sollte daher auch Regelungen für die Kommunalebene enthalten.

In meiner Stellungnahme zum Gesetzentwurf *„Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)“* vom Mai vergangenen Jahres habe ich sechs Punkte zur Aufnahme vorgeschlagen, die für das Land Hessen und die Kommunen gemeinsam dazu beitragen, die Informationssicherheit zu verbessern. Diese lassen sich uneingeschränkt auch für ein vorgesehenes Informationssicherheitsgesetz in Schleswig-Holstein übertragen:

1. Pflicht für das Land Schleswig-Holstein, ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitzustellen.
2. Meldepflicht für Kommunen von IT-Sicherheitsvorfällen über das vom Land Schleswig-Holstein bereitgestellte System.
3. Pflicht für das Land Schleswig-Holstein, die Kommunen über die Erkenntnisse zu informieren, die aus Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit gewonnen werden.
4. Pflicht für das Land Schleswig-Holstein zur Unterstützung der Kommunen bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit auf deren Ersuchen.
5. Pflicht für Kommunen zur Erstellung einer „Leitlinie zur Informationssicherheit“, in der der Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit dokumentiert werden.

[2] https://fragdenstaat.de/anfrage/sachstandsbericht-der-ag-informationssicherheit

6. Pflicht für Kommunen eine/n zentralen Ansprechpartner/in (Informationssicherheitsbeauftragte/n) zu benennen.

Prägender Leitgedanke des Sechs-Punktevorschlags sind realistisch erreichbare Mindestanforderungen, die auch außerhalb einer etwaigen Konnexität ihre Wirkungskraft entfalten können. Meine Empfehlungen in Form dieses Sechs-Punktevorschlags wurden nicht im laufenden Gesetzgebungsverfahren in das HITSiG aufgenommen, stehen aber im „Aktionsplan Kommunale Cybersicherheit" des Hessen3C als Empfehlung für ein HITSiG 2.0. Die Begründungen und Aspekte der einzelnen Punkte können meiner Stellungnahme zum HITSiG entnommen werden, die ich als Anlage hier anfüge.

Neben länderspezifischen Regelungen zur Informationssicherheit sollte sich die Landesregierung Schleswig-Holsteins zudem für einen länderübergreifenden einheitlichen Mindeststandard zur Informationssicherheit von Kommunen einsetzen. Denkbar wäre dies im und über den IT-Planungsrat und die Länderarbeitsgruppe Cybersicherheit (LAG Cybersicherheit) der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK).

Kassel, den 21. März 2024
Jens Lange

Anlage: Stellungnahme zum Gesetzentwurf HITSiG

**Kassel documenta Stadt**
**Magistrat**
**Personal- und Organisationsamt**
**Informationstechnologie**

Jens Lange
jens.lange@kassel.de
it@kassel.de
Telefon 0561 787 2318
Fax 0561 787 882318
IBAN DE16 5205 0353 0000 0110 99
BIC HELADEF1KAS

Rathaus
Obere Königsstraße 8
34117 Kassel
Zimmer E1.217
Montag – Donnerstag
9 – 15 Uhr
Freitag
9 – 12.30 Uhr
und nach Vereinbarung

Behördennummer 115
Rechtshinweise
zur elektronischen
Kommunikation
im Impressum unter
www.kassel.de

34112 Kassel documenta Stadt

Hessischer Landtag
Der Vorsitzende des Innenausschusses
Herr Christian Heinz
Schlossplatz 1-3
65183 Wiesbaden

Kassel documenta Stadt

Öffentliche Anhörung im Innenausschuss des Hessischen Landtags
Stellungnahme zum Gesetzentwurf HITSiG

5. Mai 2023


Sehr geehrter Herr Heinz,
sehr geehrte Mitglieder des Innenausschusses des Hessischen Landtags,

ich möchte mich zunächst herzlich für Ihre Anfrage bedanken, eine Stellungnahme zum Gesetzentwurf „Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz - HITSiG) - Drucks. 20/10752 –“ abzugeben. Es ist mir eine große Ehre, dass Sie meinem Fachwissen und meiner Meinung in dieser Angelegenheit vertrauen. Ich schätze Ihre Bereitschaft, verschiedene Perspektiven bei der Erstellung und Verabschiedung wichtiger Gesetze zu berücksichtigen.

Nach eingehender Prüfung des vorliegenden Gesetzentwurfs möchte ich nachfolgend meine Stellungnahme abgeben. Zusammenfassend begrüße ich die Bemühungen der Landesregierung des Landes Hessen, die rechtlichen Grundlagen zur Steigerung der Sicherheit in der Informationstechnik in Hessen anzugehen. Ich hoffe, dass meine Stellungnahme dazu beiträgt, die Diskussion zu bereichern und die Entscheidungsfindung zu unterstützen. Ich stehe gerne für weitere Fragen oder Diskussionen zur Verfügung, um den Gesetzentwurf bestmöglich zu optimieren. Bitte zögern Sie nicht, mich zu kontaktieren, wenn Sie weitere Informationen oder Klarstellungen benötigen. Ich bin jederzeit bereit, meine Expertise und Kenntnisse mit Ihnen zu teilen, um den Gesetzgebungsprozess bestmöglich zu unterstützen. Ich wünsche Ihnen viel Erfolg bei der weiteren Bearbeitung und Verabschiedung des Gesetzentwurfs.

Freundliche Grüße
Im Auftrag

Jens Lange
Informationssicherheitsbeauftragter

## Anlass

Der Innenausschuss des Hessischen Landtags hat mich durch ein Schreiben vom 3. April 2023 darüber informiert, dass ich sowohl schriftlich als auch mündlich zu dem Gesetzentwurf „Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) – Drucks. 20/10752 –“ der Landesregierung angehört werde. Aus diesem Anlass habe ich die nachfolgende schriftliche Stellungnahme verfasst.

## Vorbemerkung

In meiner Funktion als Informationssicherheitsbeauftragter der Stadtverwaltung Kassel und als Mitglied diverser Arbeitsgruppen der kommunalen Spitzenverbände (z. B. AG kommunale Basis-Absicherung, AG BCM Länder/Kommunen, AG Handreichung Informationssicherheitsleitlinie), werde ich meine Betrachtung des Gesetzentwurfs auf die kommunalen Aspekte aus dieser Sichtweise fokussieren.

## Zusammenfassung der wichtigsten Punkte

Die Schaffung einer rechtlichen Grundlage zur Steigerung der Informationssicherheit in Hessen ist begrüßenswert und notwendig. Die Einrichtung einer Zentralstelle und einer oder eines Beauftragten für Informationssicherheit mit Regelungen zu den Aufgaben und Befugnissen ist sinnvoll und angemessen. Nach sorgfältiger Prüfung des Gesetzentwurfs möchte ich im Folgenden die zentralen Punkte aufzeigen, die meiner Meinung nach im Gesetzentwurf fehlen oder nicht ausreichend berücksichtigt wurden:

1. Pflicht für das Land Hessen, ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitzustellen.
2. Meldepflicht für Kommunen von IT-Sicherheitsvorfällen über das vom Land Hessen bereitgestellte System.
3. Pflicht für das Land Hessen, die Kommunen über die Erkenntnisse zu informieren, die aus Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit gewonnen werden.
4. Pflicht für das Land Hessen, zur Unterstützung der Kommunen bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit auf deren Ersuchen.
5. Pflicht für Kommunen zur Erstellung einer „Leitlinie zur Informationssicherheit“, in der der Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit dokumentiert werden.
6. Pflicht für Kommunen eine/n zentralen Ansprechpartner/in (Informationssicherheitsbeauftragte/n) zu benennen.

Die vorgeschlagenen Pflichten für das Land Hessen und die Kommunen tragen gemeinsam dazu bei, die Informationssicherheit zu verbessern. Während das Land durch die Maßnahmen eine gestärkte Zusammenarbeit zwischen den verschiedenen Verwaltungsebenen erreicht, ermöglichen die Pflichten für die Kommunen einen systematischen und strukturierten Ansatz zur Gewährleistung eines angemessenen Schutzniveaus für ihre IT-Systeme und -Dienste.

## Begründung und Aspekte im Einzelnen



**Meldung von IT-Sicherheitsvorfällen**
(Punkt 1 und 2 der Zusammenfassung)

Die Pflicht für das Land Hessen, ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitzustellen (Punkt 1) und die Meldepflicht für Kommunen (Punkt 2) sind zusammenhängend zu betrachten. Deutschlandweit sind 2023 bereits 12 IT-Sicherheitsvorfälle von Kommunalverwaltungen öffentlich bekannt geworden (davon drei in Hessen)[1]. Im Jahr 2022 waren es 18 und im Jahr 2021 sogar 32 Vorfälle. Ein tatsächliches kommunales Lagebild zur Informationssicherheit ist jedoch nicht bekannt. Das Land Hessen sollte aus diesem und den folgenden Gründen ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitstellen und die Kommunen dazu verpflichten, IT-Sicherheitsvorfälle über dieses System an das Land zu melden:

1. Zentralisierte Erfassung: Durch ein zentrales Meldesystem können IT-Sicherheitsvorfälle effizienter erfasst und analysiert werden. Dies ermöglicht einen besseren Überblick über die Häufigkeit, Art und Schwere der Vorfälle in der gesamten Region.
2. Schnellere Reaktionszeiten: Durch das zentrale Meldesystem kann das Land Hessen rascher auf Sicherheitsvorfälle reagieren und angemessene Maßnahmen ergreifen. Dies kann dazu beitragen, Schäden zu minimieren und die Auswirkungen auf betroffene Kommunen zu reduzieren.
3. Erfahrungsaustausch und Best Practices: Ein zentrales Meldesystem ermöglicht es, Informationen und Erfahrungen zwischen den Kommunen und dem Land Hessen auszutauschen. Dadurch können Best Practices und Lösungsansätze gemeinsam entwickelt und angewendet werden, um die IT-Sicherheit in der gesamten Region zu stärken.
4. Ressourceneffizienz: Ein gemeinsames Meldesystem reduziert den Verwaltungsaufwand und die Kosten für die Kommunen, da sie keine eigenen Systeme entwickeln und betreiben müssen. Gleichzeitig profitieren sie von der Expertise des Landes Hessen in Bezug auf IT-Sicherheit.
5. Gesetzliche Vorgaben und Compliance: Durch die Verpflichtung zur Meldung von IT-Sicherheitsvorfällen können gesetzliche Vorgaben eingehalten und die Compliance in Bezug auf IT-Sicherheit gewährleistet werden. Dies ist insbesondere wichtig, um den Schutz sensibler Daten und die Funktionsfähigkeit kritischer Infrastrukturen sicherzustellen.

**Informationspflicht des Landes Hessen**
(Punkt 3 der Zusammenfassung)

Das Land Hessen sollte aus folgenden Überlegungen die Pflicht haben, die Kommunen über die Erkenntnisse zu informieren, die aus der Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit gewonnen werden:

[1] Siehe https://kommunaler-notbetrieb.de

1. Proaktive Risikominimierung: Durch das Teilen von Erkenntnissen können die Kommunen proaktiv Maßnahmen ergreifen, um Risiken zu minimieren und ihre IT-Sicherheit zu verbessern, bevor potenzielle Sicherheitsvorfälle eintreten.
2. Effektive Ressourcennutzung: Die Weitergabe von Informationen ermöglicht es den Kommunen, ihre Ressourcen effektiver einzusetzen, indem sie auf bereits gewonnene Erkenntnisse und Erfahrungen zurückgreifen können, anstatt diese selbst erarbeiten zu müssen.
3. Gemeinsame Strategieentwicklung: Die Kommunikation zwischen dem Bundesland und den Kommunen fördert die Entwicklung gemeinsamer Strategien und Vorgehensweisen zur Verbesserung der Informationssicherheit. Dies stärkt die Zusammenarbeit und führt zu einem kohärenten Ansatz in der gesamten Region.
4. Sensibilisierung und Schulung: Die Weitergabe von Erkenntnissen trägt dazu bei, das Bewusstsein für Informationssicherheit in den Kommunen zu erhöhen und deren Mitarbeiter entsprechend zu schulen. Dies ist eine wichtige Voraussetzung für die Umsetzung wirksamer Sicherheitsmaßnahmen.
5. Transparenz und Vertrauen: Die Offenlegung von Erkenntnissen über Risiken und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit schafft Transparenz und fördert das Vertrauen zwischen dem Bundesland und den Kommunen. Dies ist für eine erfolgreiche Zusammenarbeit und den Schutz kritischer Infrastrukturen von zentraler Bedeutung.

**Unterstützung der Kommunen bei Gefahren für die Informationssicherheit**
(Punkt 4 der Zusammenfassung)

Das Land Hessen sollte unter Berücksichtigung der nachfolgenden Faktoren die Pflicht haben, die Kommunen bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit auf deren Ersuchen zu unterstützen:

1. Expertise und Ressourcen: Ein Bundesland verfügt in der Regel über umfangreichere Expertise und Ressourcen im Bereich der Informationssicherheit als die einzelnen Kommunen. Durch die Unterstützung des Bundeslandes können die Kommunen von diesem Wissen und den verfügbaren Ressourcen profitieren, um ihre Sicherheit effektiv zu erhöhen.
2. Konsistente Sicherheitsstandards: Die Unterstützung durch das Bundesland trägt dazu bei, dass einheitliche und hohe Sicherheitsstandards in der gesamten Region etabliert und eingehalten werden. Dies ist insbesondere wichtig, um kritische Infrastrukturen und sensible Daten zu schützen.
3. Effiziente Reaktion auf Sicherheitsvorfälle: Im Falle eines IT-Sicherheitsvorfalls kann die Hilfe des Bundeslandes dazu beitragen, dass die Kommunen schneller und effektiver auf den Vorfall reagieren können. Dies kann dazu führen, dass Schäden minimiert und die Auswirkungen auf betroffene Systeme und Daten reduziert werden.
4. Kostenersparnis: Die Unterstützung durch das Bundesland kann den Kommunen helfen, Kosten zu sparen, indem sie auf die Expertise und Ressourcen des Bundeslandes zurückgreifen, anstatt eigene Fachkräfte einzustellen oder externe Dienstleister zu beauftragen.

5. Stärkung der Zusammenarbeit: Die Unterstützung des Bundeslandes bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit fördert die Zusammenarbeit zwischen den verschiedenen Verwaltungsebenen und stärkt das Vertrauen zwischen den Kommunen und dem Bundesland.

**Pflicht für Kommunen zur Erstellung einer „Leitlinie zur Informationssicherheit“**
(Punkt 5 der Zusammenfassung)

Die Kommunen des Landes Hessen sollten aufgrund der nachstehenden Aspekte die Pflicht zur Erstellung einer „Leitlinie zur Informationssicherheit“ haben, in der der Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit dokumentiert werden:

1. Strategische Orientierung: Die Leitlinie zur Informationssicherheit gibt den Kommunen eine klare und strukturierte Vorgabe für die Ausrichtung ihrer IT-Sicherheitsstrategie. Sie dient als Grundlage für die Planung, Umsetzung und Überwachung von Sicherheitsmaßnahmen.
2. Verbindlichkeit: Die Dokumentation der verbindlichen Prinzipien und des anzustrebenden Sicherheitsniveaus schafft Verbindlichkeit und Verantwortlichkeit innerhalb der Kommunalverwaltung. Dadurch wird sichergestellt, dass alle Beteiligten sich an den Vorgaben orientieren und ihren Aufgaben im Bereich der Informationssicherheit nachkommen.
3. Kontinuität und Nachvollziehbarkeit: Eine Leitlinie zur Informationssicherheit trägt zur Kontinuität und Nachvollziehbarkeit der Sicherheitsmaßnahmen bei. Sie ermöglicht es, den Fortschritt der Sicherheitsinitiativen zu verfolgen und gegebenenfalls Anpassungen vorzunehmen, um das angestrebte Sicherheitsniveau zu erreichen oder zu erhalten.
4. Sensibilisierung und Schulung: Die Leitlinie zur Informationssicherheit unterstützt die Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter in den Kommunen. Sie informiert über die Relevanz der Informationssicherheit, die geltenden Prinzipien und das angestrebte Schutzniveau, sodass alle Beteiligten ein gemeinsames Verständnis entwickeln können.
5. Rechtliche und regulatorische Anforderungen: Die Erstellung einer Leitlinie zur Informationssicherheit hilft den Kommunen, gesetzliche und regulatorische Anforderungen im Bereich der IT-Sicherheit zu erfüllen. Sie dient als Nachweis für die Einhaltung von Vorschriften und kann im Falle von Sicherheitsvorfällen oder Audits als Referenz herangezogen werden.

In einer solchen Pflicht für die Kommunen zur Erstellung einer „Leitlinie zur Informationssicherheit“ sollten in Anbetracht der nachfolgenden Punkte zunächst keine Mindeststandards gefordert werden:

1. Flexibilität und Anpassungsfähigkeit: Indem keine Mindeststandards vorgeschrieben werden, erhalten die Kommunen die Flexibilität, ihre Leitlinien an ihre spezifischen Bedürfnisse und Ressourcen anzupassen. Dies ermöglicht es ihnen, die Informationssicherheit auf eine Weise zu gestalten, die ihren individuellen Gegebenheiten und Herausforderungen gerecht wird.

2. Autonomie der Kommunen: Die Kommunen verfügen über eigene Zuständigkeiten und Verantwortungsbereiche. Indem keine Mindeststandards auf Landesebene vorgegeben werden, wird die Autonomie der Kommunen gewahrt und ihre Entscheidungsfreiheit bei der Ausgestaltung ihrer Informationssicherheitsstrategie respektiert.
3. Anreiz zur Selbstverantwortung: Ohne vorgegebene Mindeststandards werden die Kommunen dazu angehalten, selbst aktiv zu werden und eigene Vorgehensweisen für ihre Informationssicherheit zu entwickeln. Dies fördert die Selbstverantwortung der Kommunen und motiviert sie, ihre IT-Sicherheit kontinuierlich zu verbessern.
4. Berücksichtigung von Best Practices und Branchenstandards: Die Kommunen haben die Möglichkeit, ihre Leitlinien zur Informationssicherheit an bestehenden Best Practices und Standards (z. B. IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung) auszurichten, ohne dass ihnen von Landesebene spezifische Vorgaben gemacht werden. Dies ermöglicht eine flexible und effektive Anwendung von bewährten Sicherheitsmaßnahmen.

**Pflicht für Kommunen zur Benennung einer/s Ansprechpartner/in**
(Punkt 6 der Zusammenfassung)

Die Kommunen des Landes Hessen sollten basierend auf den folgenden Überlegungen die Pflicht zur Benennung einer/s zentralen Ansprechpartner/in (Informationssicherheitsbeauftragte/n) haben:

1. Klare Zuständigkeiten: Die Benennung eines zentralen Ansprechpartners schafft klare Zuständigkeiten und Verantwortlichkeiten in Bezug auf Informationssicherheit. Dies erleichtert die Steuerung und Koordination von Sicherheitsmaßnahmen und gewährleistet, dass Entscheidungen und Aktivitäten im Bereich der IT-Sicherheit effizient umgesetzt werden.
2. Kompetenzbündelung: Die Benennung eines Informationssicherheitsbeauftragten fördert die Bündelung von Kompetenzen und Expertise in der Kommunalverwaltung. Der/die Informationssicherheitsbeauftragte ist die zentrale Anlaufstelle für Fragen rund um die Informationssicherheit und kann so gezielte und fachkundige Beratung und Unterstützung für die verschiedenen Abteilungen und Mitarbeiter/innen anbieten.
3. Kommunikation und Zusammenarbeit: Ein/e zentrale/r Ansprechpartner/in dient als Schnittstelle zwischen den verschiedenen Verwaltungseinheiten, dem Bundesland und ggf. externen Partnern. Dadurch wird die Kommunikation und Zusammenarbeit in Fragen der Informationssicherheit verbessert, und es entsteht ein gemeinsames Verständnis für die Bedeutung und Umsetzung von Sicherheitsmaßnahmen.
4. Kontinuierliche Verbesserung: Der/die Informationssicherheitsbeauftragte überwacht und bewertet regelmäßig die Wirksamkeit der eingesetzten Sicherheitsmaßnahmen und identifiziert Verbesserungspotenziale. Dies gewährleistet eine kontinuierliche Anpassung und Optimierung der Informationssicherheit in der Kommunalverwaltung.

5. Schulung und Sensibilisierung: Der/die Informationssicherheitsbeauftragte kann verantwortlich für die Schulung und Sensibilisierung der Mitarbeiter/innen hinsichtlich der Informationssicherheit sein. Dies trägt dazu bei, das Sicherheitsbewusstsein zu erhöhen und die Einhaltung von Sicherheitsrichtlinien und -verfahren in der gesamten Organisation zu fördern.