Landesrechnungshof
Schleswig-Holstein

Bemerkungen 2017

mit Bericht zur
Landeshaushaltsrechnung 2015

und

Stellungnahme 2016

zum Abbau des strukturellen
Finanzierungsdefizits bis 2020

Kiel, 6. April 2017

Bemerkungen 2017

des Landesrechnungshofs Schleswig-Holstein

mit Bericht zur
Landeshaushaltsrechnung 2015

und

Stellungnahme 2016 zur Planung der Landesregierung vom 06.09.2016 zum Abbau des strukturellen Finanzierungsdefizits bis 2020

Kiel, 6. April 2017

Landesrechnungshof Schleswig-Holstein
Berliner Platz 2, 24103 Kiel
Pressestelle: Tel.: 0431 988-8905
Fax: 0431 988-8686
Internet: www.lrh.schleswig-holstein.de

13. Gemeinsam zu mehr Informationssicherheit

Angriffe auf Informations- und Kommunikationstechnik stellen das Land Schleswig-Holstein vor immer größere Herausforderungen. Das Informationssicherheitsmanagement ist zu einer zentralen Aufgabe geworden.

Eine Bestandsaufnahme in 42 Landesbehörden zeigt, dass die Landesverwaltung hier noch Nachholbedarf hat. Eine grundlegende Überarbeitung der IT-Sicherheitsleitlinie von 2010 ist überfällig. Defizite gibt es bei der Sicherheitskonzeption. Einige Behörden haben noch nicht einmal die organisatorischen Voraussetzungen für ein Informationssicherheitsmanagement geschaffen.

Die Zeit wird knapp: Bis 2018 muss Schleswig-Holstein die Vorgaben des IT-Planungsrats von 2013 umsetzen. Dazu gehören z. B. die Benennung von Beauftragten für die Informationssicherheit sowie die Ausrichtung der Landesverwaltung an anerkannten Sicherheitsstandards.

Informationssicherheit ist Führungsaufgabe einer jeden Behörde. Die Landesregierung sollte das Know-how für Informationssicherheit in einem Kompetenzzentrum bündeln. Nur so können die Landesbehörden bei der Bewältigung dieser Daueraufgabe effektiv und effizient unterstützt werden.

13.1 Risiken für die IT-Infrastruktur wachsen

Modernes Verwaltungshandeln ist ohne den Einsatz von Informationstechnik nicht mehr denkbar. Die Angriffsfläche der Landesverwaltung im IT-Umfeld ist stark angewachsen, u. a. durch eine stärkere Vernetzung, das Angebot von Services über das Internet und die Einbindung von mobilen Endgeräten. Die Bedrohung, dass Daten der Bürgerinnen und Bürger sowie der Unternehmen abhandenkommen, ist gestiegen. Daten sind zu einer Handelsware geworden, auf die mit kriminellen Mitteln wie z. B. Hackerangriffen zugegriffen wird. Informationssicherheit ist damit zu einem kritischen Faktor für das Vertrauen in die Funktionsfähigkeit des Staates geworden.

13.2 Informationssicherheitsmanagement - Länder sind bis 2018 gefordert

Der IT-Planungsrat als das zentrale Gremium für die föderale Zusammenarbeit von Bund, Ländern und Kommunen im Bereich der Informationstechnik hat die Bedeutung der Informationssicherheit für eine erfolgreiche

IT-Modernisierung schon 2011 erkannt. 2013 wurden in einer Leitlinie für Informationssicherheit die Eckpunkte für ein gemeinsames Vorgehen von Bund und Ländern definiert:

- Informationssicherheitsmanagement,
- Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung,
- einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren,
- gemeinsame Abwehr von IT-Angriffen sowie
- Standardisierung und Produktsicherheit.

In einem Umsetzungsplan wurde konkretisiert, welche Schritte bis April 2018 erfolgen müssen. Die Vorgaben der Leitlinie und des Umsetzungsplans sind für alle Behörden der Bundes- und Landesverwaltung verbindlich. Den Kommunen wird die Anwendung der Leitlinie empfohlen.

Der IT-Planungsrat orientiert sich bei seinen Forderungen an etablierten Sicherheitsstandards wie z. B. dem IT-Grundschutzstandard des Bundesamts für Sicherheit in der Informationstechnik (BSI). Während zunächst die Definition von Mindeststandards für die IT-Sicherheit im Vordergrund stand, sind die Länder derzeit insbesondere in folgenden Punkten gefordert:

- Sie müssen mit dem Aufbau eines Computer Emergency Response Teams (CERT) für die Landesverwaltung die Voraussetzungen für die gemeinsame Abwehr von IT-Angriffen schaffen.
- Die Länder müssen einen IT-Sicherheitsbeauftragten für das Land und IT-Sicherheitsbeauftragte für wesentliche Behörden[1] benennen.
- IT-Sicherheitsleitlinien müssen verabschiedet und
- Informationssicherheitsmanagementsysteme eingeführt werden.

Diesen Anforderungen muss die Landesregierung bis April 2018 gerecht werden.

13.3 Informationssicherheit - auch ein Thema der Rechnungshöfe

Die Rechnungshöfe des Bundes und der Länder befassen sich seit einigen Jahren mit Fragestellungen zur Sicherheit der IT in der öffentlichen Verwaltung. Sie haben schon 2011 in ihren IuK-Mindestanforderungen die Einrichtung eines Informationssicherheitsmanagements gefordert. 2015 wurden die Erfahrungen der Rechnungshöfe in einem Grundsatzpapier zum Informationssicherheitsmanagement zusammengefasst.

---

[1] Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung - Umsetzungsplan - Seite 3 (10. IT-Planungsrat Beschluss 2013/01).

Die IuK-Mindestanforderungen 2016[1] weisen über die Anforderungen des IT-Planungsrats hinaus insbesondere auf folgende Punkte hin:

- Die Verantwortung für die IT-Sicherheit liegt bei der Leitung der jeweiligen Einrichtung.
- Die Wirksamkeit und die Umsetzung des Informationssicherheitsmanagements sind kontinuierlich zu überwachen und zu verbessern.
- Besonderes Augenmerk ist auch auf die Information und Sensibilisierung aller Beschäftigten zu legen.
- Für die Landesverwaltung ist ein zentrales Informationssicherheitsmanagement einzurichten und eine ressortübergreifende Aufgabenerledigung anzustreben.
- Die Wirksamkeit von Sicherheitsmaßnahmen und -prozessen sollte durch angemessene Audit-Verfahren oder Revisionen nachgewiesen werden.

13.4 Bestandsaufnahme 2016 - es ist noch viel zu tun

Der LRH hat 2016 eine Bestandsaufnahme dazu durchgeführt, welche Maßnahmen die Staatskanzlei und die Ressorts bislang zur Einführung eines Informationssicherheitsmanagements ergriffen haben. 42 Landesbehörden haben zum Stichtag 01.10.2016 u. a. dazu Auskunft gegeben, ob sie

- einen IT-Sicherheitsbeauftragten benannt,
- eine IT-Sicherheitsleitlinie verabschiedet,
- Sicherheitskonzepte erstellt und
- ein Informationssicherheitsmanagement aufgebaut haben.

Die Bestandsaufnahme macht deutlich, dass noch viel zu tun ist.

Im Oktober 2016 hatten weniger als die Hälfte der befragten Landesbehörden einen IT-Sicherheitsbeauftragten benannt. Das Finanzministerium hat lediglich im zugeordneten Amt für Informationstechnik IT-Sicherheitsbeauftragte bestellt, für das Ministerium ist die Funktion unbesetzt.

Die für das Zentrale IT-Management zuständige Staatskanzlei hat sowohl auf einen Landes-IT-Sicherheitsbeauftragten als auch auf einen IT-Sicherheitsbeauftragten für ihren Geschäftsbereich verzichtet. Organisatorische Voraussetzungen wurden nur insoweit getroffen, als das Zentrale IT-Management für das Informationssicherheitsmanagement des Landes zuständig ist. Dazu gehört neben der Konzeption und Planung von Sicherheitsprozessen auch die Kontrolle, ob Sicherheitsmaßnahmen umgesetzt werden. Der CIO des Landes koordiniert das Sicherheitsmanagement.

---

1 http://www.landesrechnungshof-sh.de/file/iuk-mindestanforderungen_2016.pdf.

Damit ist das Informationssicherheitsmanagement in der Staatskanzlei personell aber noch nicht so aufgestellt, dass es seinen Aufgaben in der Praxis auch nachkommen kann.

Die **Staatskanzlei** merkt hierzu an, dass der CIO und das Zentrale IT-Management ressortübergreifend Zuständigkeiten insbesondere im Bereich der Standard-IT (Standard-IT-Arbeitsplatz, Standard-IT-Infrastruktur, Standard-IT-Funktionalitäten) wahrnehmen würden. Das Zentrale IT-Management habe dahin gehend besondere ressortübergreifende Kompetenzen und Verantwortlichkeiten im Bereich der IT-Sicherheit in der Landesverwaltung. Die hiermit in Zusammenhang stehenden Aufgaben und Kompetenzen würden - analog zu anderen Bundesländern - durch einen/eine Informationssicherheitsmanager/-in für das Land Schleswig-Holstein wahrgenommen. Der/die Informationssicherheitsmanager/-in sei zuständig für die Grundsatzangelegenheiten des Informationssicherheitsmanagements und für das Informationssicherheitsmanagement der vom Zentralen IT-Management verantworteten Standard-IT/IT-Basisinfrastruktur. Er/Sie würde das ressortübergreifende integrierte Sicherheitsmanagementsystem leiten und koordinieren und die Landesverwaltung in Fragen der Informationssicherheit fachlich gegenüber anderen Bundesländern und gegenüber dem Bund, insbesondere in der Arbeitsgruppe Informationssicherheit des IT-Planungsrates, vertreten.

13.5 Sicherheitsaufgaben müssen wahrgenommen werden

Der LRH hat schon in seinen Bemerkungen 2010 in Bezug auf das SAP-Verfahren des Landes festgestellt, dass *„IT-Sicherheit … nicht zum Nulltarif zu haben ist“.*[1] Die Sicherheit eines IT-Verfahrens kann nur gewährleistet werden, wenn permanent ein Abgleich zwischen der Konzeptlage und der Verfahrenswirklichkeit stattfindet.

Dies gilt umso mehr, wenn es um das Informationssicherheitsmanagement für die gesamte IT-Infrastruktur des Landes geht. Von einer kontinuierlichen Aufgabenwahrnehmung ist die Landesverwaltung hier noch weit entfernt.

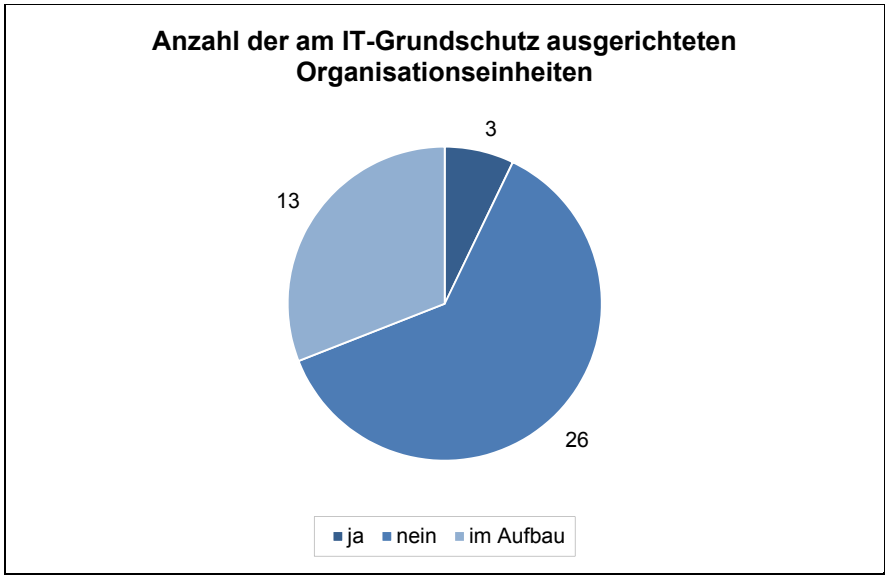
Zwar hat die Landesregierung schon 2010 eine „IT-Sicherheitsleitlinie für die IT-Basisinfrastruktur der Schleswig-Holsteinischen Landesverwaltung“ erlassen. Aber eine kontinuierliche Überarbeitung der Leitlinie im Abstand von 2 Jahren hat nicht stattgefunden. Eine 2014 begonnene Fortschreibung der Sicherheitsleitlinie wurde bis Ende 2016 nicht zum Abschluss gebracht.

---

1 Vgl. Bemerkungen 2010 des LRH, Nr. 18.2.3.

Die IT-Sicherheitsleitlinie von 2010 muss dringend überarbeitet werden. Sie muss neben der IT-Basisinfrastruktur z. B. auch Mindeststandards für Fachanwendungen umfassen.

Obwohl die Landesregierung bereits 2010 beschlossen hat, sich an etablierten Sicherheitsstandards wie dem IT-Grundschutzstandard des BSI zu orientieren, haben die Behörden dieses Ziel bisher nicht erreicht.



Stand: 01.10.2016

Lediglich 3 von 42 befragten Behörden gaben an, ein Informationssicherheitsmanagement gemäß BSI-Grundschutz zu betreiben. Damit ist die Landesverwaltung von der Vorgabe des IT-Planungsrats, bis April 2018 die IT-Sicherheitskonzeption am IT-Grundschutz des BSI auszurichten, noch ein gutes Stück entfernt.

13.6 Keine Informationssicherheit ohne Beteiligung der Mitarbeiterinnen und Mitarbeiter

Obwohl viele Gefahrenquellen für IT-Anwendungen der Landesbehörden außerhalb des Landesnetzes liegen, resultiert ein großer Anteil der Bedrohung der Informationssicherheit aus dem Inneren der Organisationseinheiten: Neben technischen Sicherheitsvorkehrungen in der IT-Infrastruktur ist es deshalb ebenso wichtig, ein gemeinsames Bewusstsein für IT-Sicherheit zu erzielen.

Alle Mitarbeiterinnen und Mitarbeiter müssen erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg eines Informationssicherheitsmanagements sind. Sie müssen bereit sein, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen. Hierfür müssen eine

Sicherheitskultur und ein Sicherheitsbewusstsein aufgebaut und gepflegt werden. Insbesondere müssen die Mitarbeiterinnen und Mitarbeiter darüber informiert werden, wie sie in sicherheitskritischen Situationen reagieren sollen. Hierzu sind Sensibilisierungs- und Schulungsmaßnahmen erforderlich. Mitarbeiterinnen und Mitarbeiter müssen die notwendigen Kenntnisse und Kompetenzen für ein sicherheitsbewusstes Verhalten erwerben.

Ohne Einbindung und Akzeptanz der Mitarbeiterinnen und Mitarbeiter ist die Etablierung und Wirkung eines Informationssicherheitsmanagements zum Scheitern verurteilt.

Informationssicherheit ist ebenso wie Datenschutz Führungsaufgabe. Die Führungskräfte sind in besonderer Weise für die Wahrnehmung dieser Aufgabe zu schulen und zu sensibilisieren. Dies darf sich nicht allein auf die Mitwirkung bei der Erstellung einer bereichsspezifischen Informationssicherheitsleitlinie beschränken.

Sensibilisierungs- und Schulungsmaßnahmen sind eine Daueraufgabe. Schulungen für Informationssicherheitsverantwortliche und Anwenderinnen und Anwender sollten zentral geplant und koordiniert werden. Der LRH empfiehlt, bereits vorhandene Kampagnen und Angebote von Bund, Ländern und Kommunen zu nutzen und mögliche Kooperationen mit Lernplattformen zur Informationssicherheit zu prüfen. Die Aktivitäten sollten in einem Kompetenzzentrum gebündelt werden.

13.7 Kompetenzen für Datenschutz und Informationssicherheit bündeln

Die rechtlichen und gesellschaftlichen Anforderungen, ein hohes Maß an Informationssicherheit zu erreichen, treffen in der Landesverwaltung auf eine bestehende Mangelsituation:

- Haushaltsmittel werden nur beschränkt zur Verfügung gestellt.
- Personalressourcen sind begrenzt.
- Know-how steht nicht in ausreichender Menge und Fachtiefe zur Verfügung.
- Vorhandenes IT-Personal wird für den IT-Betrieb und für die Steuerung von IT-Projekten benötigt.
- Aufgaben wie z. B. die Revision der Informationssicherheit werden nicht wahrgenommen.

Gleichzeitig müssen die Landesbehörden die Forderung der Datenschutzgrundverordnung[1] bis zum Mai 2018 umsetzen und behördliche Datenschutzbeauftragte bestellen. Dies verstärkt den Ressourcenkonflikt.

Das Vorhalten von Spezialwissen für den Datenschutz und die Informationssicherheit in jedem einzelnen Ressort ist unwirtschaftlich. Der LRH hat deshalb bereits in seinen Bemerkungen 2012 empfohlen, den Sachverstand für einzelne IT-Aufgaben in Kompetenzzentren zu bündeln.[2] Die Aufgabenbereiche Datenschutz und Informationssicherheit bieten sich dafür an. Aufgaben, die zentral wahrgenommen werden können, sollten in ein Kompetenzzentrum verlagert werden.

Das Kompetenzzentrum könnte folgende Aufgaben übernehmen:

- Grundsatzaufgaben eines behördlichen Datenschutzbeauftragten,
- Tätigkeiten des Informationssicherheitsbeauftragten für die Ressorts, die alleine keine wirtschaftliche Aufgabenwahrnehmung sicherstellen können,
- Erstellung der zentralen Dokumentationen wie Leitlinie, Sicherheitskonzepte etc.,
- Sicherstellen einer Informationssicherheitsrevision,
- Planung und Steuerung von Sensibilisierungsmaßnahmen,
- Planung und Steuerung der Schulungen für Sicherheitsbeauftragte, Führungskräfte, Anwenderinnen und Anwender,
- Unterstützung der Ressorts bei der Erarbeitung bereichsspezifischer Leitlinien, Maßnahmen und Dokumentationen,
- Erstellung und Bereitstellung von Musterdienstanweisungen und Richtlinien,
- Sicherstellung einer regelmäßigen Evaluierung.

Das Kompetenzzentrum muss zügig eingerichtet und mit den erforderlichen personellen Ressourcen ausgestattet werden. Es muss zeitnah seine Tätigkeit aufnehmen.

13.8 Die Planungen zur Neuorganisation beginnen

Die **Staatskanzlei** teilt hierzu mit, dass das Zentrale IT-Management neben der Aktualisierung der IT-Sicherheitsleitlinie in 2016 auch mit der Erarbeitung eines Konzepts zum Aufbau eines Kompetenzzentrums für Datenschutz und Informationssicherheit begonnen habe. Wesentliche Punkte des Konzepts würden mit den Ausführungen des LRH zu den von

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG; Amtsbl. Europäische Union, L119/1 vom 04.05.2016.

2 Vgl. Bemerkungen 2012 des LRH, Nr. 22.5.

einem Kompetenzzentrum wahrzunehmenden Aufgaben übereinstimmen. Der aktuelle Stand des Konzepts sei am 16.02.2017 in der „Konferenz der Leiterinnen und Leiter der Allgemeinen Abteilung der Staatskanzlei und der Ministerien“ vorgestellt worden. Im Ergebnis solle das Konzept im Hinblick auf eine Neuorganisation der Themenkomplexe „Datenschutz“ und „Informationssicherheit“ unter Berücksichtigung von Handlungsalternativen weiterentwickelt und dem Kabinett zur Beschlussfassung vorgelegt werden.