Landesrechnungshof Mecklenburg-Vorpommern

Landesrechnungshof Mecklenburg-Vorpommern, Wismarsche Str. 159, 19053 Schwerin

lt. Verteiler

per E-Mail

Bearbeiter: Steffen Wirks
Telefon: +49 (0) 385 74 12 -113
Fax: +49 (0) 385 74 12 -100
E-Mail: swirks@lrh-mv.de
Ihr Zeichen:
GZ: 12-0.09149-32#1 - 28134/2015

Schwerin, 11. Januar 2016

Rundschreiben Nr. 2/2016 des Landesrechnungshofes Mecklenburg-Vorpommern

Informationssicherheitsmanagement

Allgemeines

Der Landesrechnungshof Mecklenburg-Vorpommern informiert in unregelmäßigen Abständen über Themen von über den Einzelfall hinausgehender Bedeutung durch Rundschreiben. Adressat der Rundschreiben sind alle Stellen der öffentlichen Verwaltung in Mecklenburg-Vorpommern, die vom Landesrechnungshof geprüft werden können. Der Versand erfolgt ausschließlich elektronisch, die Rundschreiben werden auch auf der Homepage des Landesrechnungshofes zur Verfügung gestellt.

Der Landesrechnungshof wird die in seinen Rundschreiben mitgeteilten Feststellungen und Wertungen seiner künftigen Prüfungstätigkeit zugrunde legen und als bei den geprüften Stellen als bekannt voraussetzen. Er bittet deshalb die Empfänger, in geeigneter Weise sicherzustellen, dass die Rundschreiben allen Beschäftigten bekannt gemacht werden.

1 Positionierung der Rechnungshöfe des Bundes und der Länder zum Informationssicherheitsmanagement

Die Rechnungshöfe des Bundes und der Länder haben ein Grundsatzpapier zum Informationssicherheitsmanagement (ISM) erarbeitet. Dieses Papier ist auf der Homepage des Landesrechnungshofes[1] im Bereich Veröffentlichungen unter dem Punkt Gemeinsame

[1] www.lrh-mv.de

Dokumente der Rechnungshöfe abrufbar. Bestandteil des Papiers ist ein Fragenkatalog als Mindeststandard für die Prüfung eines ISM.

Die Rechnungshöfe empfehlen in dem Papier die Einrichtung eines zentralen ISM. Verantwortlichkeiten in der IT sollen nicht mehr organisationsbezogen, sondern Dienste bezogen festgelegt werden. Unerlässlich für ein wirkungsvolles ISM ist das Vorhandensein von qualifiziertem Personal. Die Einrichtung eines Computer Emergency Response Team[2] (CERT) in den Ländern sehen die Rechnungshöfe als wichtigen Baustein für das operative ISM. Die Rechnungshöfe formulieren einen Katalog an Erwartungen an die Verwaltungen, um angemessene Informationssicherheit herzustellen.

Der dem Papier beigefügte Fragenkatalog soll zukünftig als ein Prüfungsmaßstab des Landesrechnungshofes vorrangig in der Landesverwaltung bzw. in angepasster Form auch bei Prüfungen in Kommunalverwaltungen herangezogen werden. Er kann von den Verwaltungen auch für eine Selbstüberprüfung genutzt werden. Die Struktur des Fragenkatalogs beruht auf fünf Säulen: Informationssicherheitsmanagement, Absicherung der Netzinfrastruktur, einheitliche Sicherheitsstandards für ebenenübergreifende Verfahren, gemeinsame Abwehr von IT-Angriffen sowie Standardisierung und Produktsicherheit. Die fünf Säulen sind jeweils unterteilt in Fragen für die übergeordnete zentrale Ebene und die dezentrale Ebene der einzelnen Einrichtung. Zusätzlich enthält der Katalog eine sechste Säule mit Detailfragen zur Informationssicherheit zur Vertiefung und Ergänzung der Fragen in den fünf Säulen.

Zum Thema ISM existieren eine Reihe von Regelungen, Dokumenten und Standards, die teilweise verbindlich sind, teilweise empfehlenden oder ergänzenden Charakter haben. Das Rundschreiben soll einen Überblick geben und darlegen, welche dieser Regelungen für die Landesverwaltung und die Kommunen im Land verbindlich anzuwenden sind bzw. zur Anwendung empfohlen werden.

2 Überblick

Um ein einheitliches Mindestsicherheitsniveau für Bund und Länder bei ebenenübergreifenden IT-Verfahren sowie der gemeinsamen Kommunikation und dem Datenaustausch zu erreichen, hat der IT-Planungsrat eine Leitlinie zur Informationssicherheit erlassen.

Für die Landesverwaltung in Mecklenburg-Vorpommern gilt die Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung Mecklenburg-Vorpommern (IS-

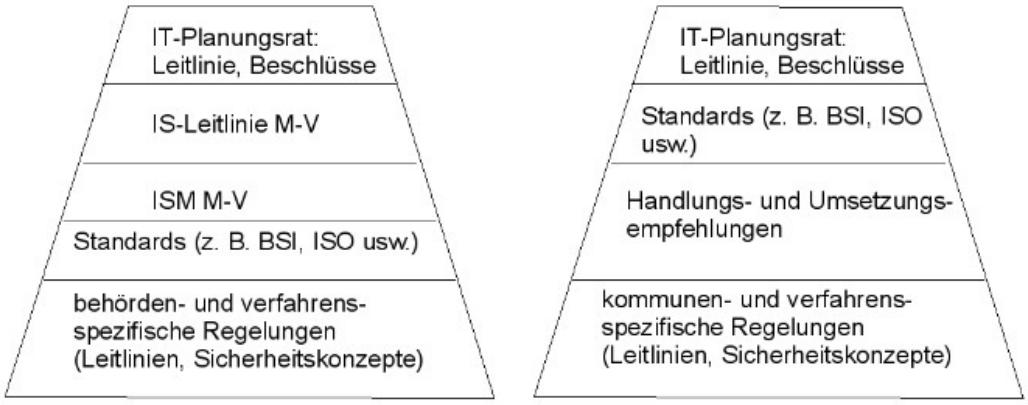
[2] Computer-Notfall-Team.

Leitlinie M-V) sowie das Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern (ISM M-V).

Zum ISM existieren eine Reihe von Standards (BSI, ISO/IEC 2700x, COBIT 5 InfoSec, ITIL), die teilweise verpflichtend anzuwenden sind, teilweise zur Anwendung empfohlen werden. Darüber hinaus können sie ergänzend für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) herangezogen werden.

Für Kommunen existiert eine Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen. Zudem wird für kleine bis mittelgroße Kommunen die ISIS12-Vorgehensweise[3] empfohlen.

Auf unterster Ebene sind jeweils spezifische auf die Einrichtung (Kommune, Behörde) und auf die IT-Verfahren bezogene Regelungen zur Informationssicherheit zu treffen.



ISM in der Landesverwaltung — ISM in Kommunen

3 Darstellung der Regelungen

3.1 IT-Planungsrat

3.1.1 Leitlinie des IT-Planungsrats für die Informationssicherheit in der öffentlichen Verwaltung

Die Leitlinie legt für die Behörden und Einrichtungen der Verwaltungen von Bund und Ländern ein einheitliches Mindestsicherheitsniveau orientiert am Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[4] fest. Die Vorgaben der Leitlinie sind von Bund und Ländern in ihren Zuständigkeitsbereichen eigenständig umzusetzen. In Mecklenburg-Vorpommern ist dies durch die Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V)[5] erfolgt. Der IT-Planungsrat empfiehlt den Kommunen die Anwendung der Leitlinie.

[3] Vgl. 5.2.

[4] Vgl. 4.1.

Die Leitlinie stützt sich auf dieselben fünf Säulen, in die auch der Fragenkatalog der Rechnungshöfe gegliedert ist (vgl. Abschnitt 1).

Informationssicherheitsmanagement

Die Behörden und Einrichtungen sollen ein Informationssicherheitsmanagementsystem (ISMS) nach einheitlichen verwaltungsübergreifenden Mindestanforderungen orientiert am Grundschutz des BSI aufbauen. Als Basis wird die Anwendung der ISO/IEC 27001[6] empfohlen. Die Leitlinie definiert die Mindestanforderungen. Hierzu zählen insbesondere:

- Festlegung und Dokumentation der Verantwortlichkeiten,
- Erlass einer Leitlinie für Informationssicherheit,
- Erstellung und Umsetzung von Sicherheitskonzepten,
- Etablierung von Prozessen zur Kontrolle der Umsetzung, Wirksamkeit und Beachtung von Informationssicherheitsmaßnahmen sowie
- Information, Weiterbildung und Sensibilisierung aller Beschäftigten und anforderungsgerechte Fortbildung der IT-Sicherheitsbeauftragten.

Absicherung der Netzinfrastruktur

Für das Verbindungsnetz zwischen Bund und Ländern schreibt die Richtlinie für die Anschlussbedingungen u.a. fest, dass ein ISMS eingerichtet wird. Für direkt angeschlossene Netze sind die BSI Standards 100-1, 100-2, 100-3 und 100-4[7] umzusetzen.

Sicherheitsstandards für ebenenübergreifende Verfahren

Bei Planung und Anpassung von Verfahren, die Bund-Länder-übergreifend oder von mehreren Bundesländern genutzt werden (ebenenübergreifende Verfahren)[8], ist der IT-Grundschutz des BSI anzuwenden. Die ebenenübergreifenden IT-Verfahren, insbesondere die kritischen[9], sind zu erfassen und zu beschreiben.

Die Umsetzung der Vorgaben der Leitlinie ist über Bund und Länder hinaus durch den IT-Verfahrensverantwortlichen im notwendigen Umfang auf die jeweiligen Verfahrensbeteiligten auszudehnen. Für Kommunen als Beteiligte an ebenenübergreifenden Verfahren sind die Vorgaben zum Mindestsicherheitsniveau für den Betrieb des Verfahrens verbindlich

---

5 https://cms.cn.mv-regierung.de/cms/Lotse_prod/Lotse/Landesverwaltung/_SonstigeSeiten/Zentrales_IT-Management/Zentrales_IT-Management.jsp; vgl. 3.2.1

6 Vgl. 4.2.

7 Vgl. 4.1.

8 Z. B. das Nationale Waffenregister.

9 Kritische IT-Verfahren sind für die Arbeitsfähigkeit der Verwaltung von grundlegender Bedeutung. Bezüglich Verfügbarkeit, Vertraulichkeit und Integrität besteht ein besonderer Schutzbedarf.

anzuwenden. Da die ebenenübergreifenden Verfahren und die ebenenübergreifende Kommunikation in die jeweilige IT-Architektur der kommunalen Gebietskörperschaft eingebunden sind, sollte das Sicherheitsniveau aller Komponenten (Hardware, Dienste, Netzwerk) den am BSI-Grundschutz orientierten Mindestanforderungen der Leitlinie entsprechen[10].

Gemeinsame Abwehr von IT-Angriffen

Es soll ein VerwaltungsCERT-Verbund (VCV) von Bund und Ländern aufgebaut werden. Hierzu sollen in den Ländern CERTs aufgebaut, übergreifende Prozesse, Meldeverfahren und Meldewege festgelegt und die gegenseitige Unterstützung und Hilfeleistung bei IT-Sicherheitsvorfällen geregelt werden.

Standardisierung und Produktsicherheit

Es sollen gemeinsame Basiskomponente angeboten werden. Der Bedarf soll ermittelt werden. Gemeinsame Sicherheitsanforderungen für sichere Produkte, Systeme und Verfahren sollen festgelegt werden.

3.1.2 Beschlüsse und Empfehlungen des IT-Planungsrats (IT-PLR)

Der IT-Planungsrat als zentrales Steuerungs- und Entscheidungsgremium von Bund und Ländern in Fragen der IT und des E-Governments entscheidet durch Beschluss oder Empfehlung. Legt der IT-Planungsrat Standards durch Beschluss fest, entfalten diese Bindungswirkung für Bund und Länder.

Der IT-Planungsrat tagt dreimal im Jahr und veröffentlicht seine Entscheidungen unter http://www.it-planungsrat.de/DE/Entscheidungen/Entscheidungen_node.html.

Beschlossene Standards sind in der Landesverwaltung umzusetzen. Empfehlungen des IT-Planungsrats sollen berücksichtigt werden.

3.2 ISM in der Landesverwaltung

3.2.1 Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V)

Die Leitlinie setzt die Vorgaben der Leitlinie des IT-Planungsrats um. Sie gilt für die Staatskanzlei und die Ressorts der Landesregierung. Die Richtlinie regelt dieselben fünf Bereiche wie die Leitlinie des IT-Planungsrats (vgl. Abschnitt 3.1.1).

[10] Dies kann erreicht werden durch die Umsetzung der BSI-Standards 100-1, 100-2, mindestens aber durch die Umsetzung des ISO/IEC-Standards 27001 oder bei kleinen und mittelgroßen Kommunen durch die Umsetzung der ISIS12-Vorgehensweise.

Informationssicherheitsmanagement

Als Mindestsicherheitsniveau wird die jeweils aktuelle Fassung der BSI-Standards[11] festgeschrieben. Diese sind durch die Staatskanzlei und die Ressorts verbindlich anzuwenden.

Die Richtlinie regelt vorrangig die Einrichtung eines ressortübergreifenden ISMS. Sie legt fest, dass der BSI-Standard 100-1 *Managementsysteme für Informationssicherheit* anzuwenden ist. Damit wird die Verantwortlichkeit der Leitungsebene der Staatskanzlei, der Ministerien und deren nachgeordneter Einrichtungen und Behörden für die Informationssicherheit festgeschrieben. Der Standard beschreibt zudem den Informationssicherheitsprozess.

Die Richtlinie bezieht sich auf die Vorgaben der IS-Leitlinie des IT-Planungsrats, so dass die dort formulierten Mindestanforderungen an ein ISMS gelten.

Absicherung der Netz- und Kommunikationsstruktur

Für den Anschluss der Behörden an das Corporate Network LAVINE (CN LAVINE) müssen die Behörden über ein Sicherheitskonzept auf Basis der IT-Grundschutzkataloge des BSI verfügen. Die Sicherheitsmaßnahmen nach dem IT-Sicherheits- und Notfallkonzept des CN LAVINE sind umzusetzen. Die Wirksamkeit der Sicherheitsmaßnahmen ist regelmäßig zu kontrollieren, zu dokumentieren und weiterzuentwickeln.

Einheitliche Sicherheitsstandards für übergreifende IT-Verfahren

Die übergreifenden IT-Verfahren, insbesondere die kritischen, sind zu erfassen und zu beschreiben. Bei Planung, Betrieb und Pflege dieser Verfahren sind die IT-Grundschutz-Standards des BSI anzuwenden. IT-Sicherheitskonzepte sind zu erstellen. Die darin enthaltenen Maßnahmen sind durch alle am Verfahren beteiligte Stellen umzusetzen.

Gemeinsame Abwehr von IT-Angriffen

Die Richtlinie benennt die wesentlichen Aufgaben des CERT M-V.

Standardisierung und Basisinfrastruktur

Die Richtlinie schreibt fest, dass die im IT-Strukturrahmen des Landes enthaltenen Regelungen zur Nutzung von Standards und zentralen Diensten einzuhalten sind.

---

[11] vgl. 4.1

3.2.2 Konzept zum Aufbau und Betrieb eines Informationsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern (ISM M-V[12])

Das Konzept beschreibt die Informationssicherheitsorganisation des Landes, Aufbau, Befugnisse und Dienstleistungen des CERT, Regelungen zur Behandlung von Sicherheitsvorfällen einschließlich Melde- und Berichtspflichten der Behörden, die Durchführung von Informationssicherheitsrevisionen, die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen sowie Zeit- und Finanzierungsplanung zur Umsetzung des Konzepts.

Schwerpunktmäßig enthält das Konzept übergreifende Regelungen, vereinzelt aber auch Festlegungen zum ISM auf Ebene der jeweiligen Einrichtung.

Die Behörden der Landesverwaltung sind verpflichtet, mindestens alle drei Jahre Informationssicherheitsrevisionen durchzuführen. Die Vorgehensweise soll sich am Leitfaden des BSI (Informationssicherheitsrevision – Ein Leitfaden für die IS-Revisionen auf Basis von IT-Grundschutz[13]) orientieren. Die IT-Sicherheitsbeauftragten einer Behörde haben sicherzustellen, dass Sensibilisierungs- und Schulungsmaßnahmen entsprechend dem Maßnahmekatalog M 3.5 der IT-Grundschutzkataloge durchgeführt werden. Die IT-Sicherheitsbeauftragten der Ressorts haben zu prüfen, ob die erforderlichen Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit in den zum Geschäftsbereich gehörenden Behörden auch tatsächlich durchgeführt werden.

Die behördeninternen Abläufe zur Behandlung von Sicherheitsvorfällen sind entsprechend des Bausteins B 1.8 der IT-Grundschutzkataloge zu regeln. Dementsprechend haben die Behörden die dort empfohlenen Maßnahmen umzusetzen.

4 Standards

4.1 IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

IT-Grundschutzstandards des BSI sind:

- BSI-Standard 100-1 Managementsysteme für Informationssicherheit,
- BSI-Standard 100-2 Vorgehensweise nach IT-Grundschutz sowie die IT-Grundschutzkataloge,
- BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz und
- BSI-Standard 100-4 Notfallmanagement.

---

12 ebd.

13 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf?

Für die Staatskanzlei und die Ressorts der Landesregierung und ihrer Geschäftsbereiche schreibt die IS-Leitlinie M-V als Mindestsicherheitsniveau den IT-Grundschutz des BSI fest.

Bei ebenenübergreifenden Verfahren ist der Grundschutz des BSI verpflichtend anzuwenden.

Die Anforderungen an die Informationssicherheit in EU-Zahlstellen für die Gemeinsame Agrarpolitik nach den Vorgaben der Verordnung (EG) 907/2014[14] müssen durch die Umsetzung des BSI Grundschutzes erfüllt werden, sofern nicht einer der beiden anderen vorgegeben Standards umgesetzt wird[15].

Im Übrigen empfiehlt der Landesrechnungshof den Rechtspersonen des öffentlichen Rechts in Trägerschaft des Landes oder kommunaler Gebietskörperschaften, den Landkreisen, kreisfreien Städten und großen kreisangehörigen Städten, die IT-Grundschutzstandards des BSI anzuwenden[16].

4.2 ISO/IEC-Standards zur Informationssicherheit (2700x-Reihe)

Der Standard ISO/IEC 27000 erläutert grundlegende Prinzipien, Konzepte, Begriffe und Definitionen für ISMS. Im Standard ISO/IEC 27001 werden allgemeine Empfehlungen zu Einführung, Betrieb und Verbesserung von ISMS gegeben. Der BSI Standard 100-1 ist kompatibel zum ISO/IEC 27001. Der ISO/IEC-Standard 27002 ist das Rahmenwerk für den Aufbau eines ISMS. Er beschreibt die erforderlichen Sicherheitsmaßnahmen. Die BSI-Standards berücksichtigen diesen Standard. Rahmenempfehlungen zum Risikomanagement für Informationssicherheit enthält der ISO/IEC-Standard 27005. Der Standard ISO/IEC 27006 enthält die Anforderungen an die Akkreditierung von Zertifizierungsstellen für ISMS. Die weiteren Standards der Normenreihe ISO/IEC 2700x behandeln verschiedene Aspekte des Sicherheitsmanagements und beziehen sich auf Anforderungen der ISO/IEC 27001.

Werden die BSI-Standards umgesetzt, sind im Wesentlichen auch die ISO/IEC-Standards 27001 und 27002 eingehalten. Behörden und Kommunen, die gerade erst beginnen, ein verbindliches Rahmenwerk zu entwickeln, sollten zunächst den ISO/IEC-Standard 27001 umsetzen. Dies entspricht auch der Empfehlung des IT-Planungsrats in der Leitlinie zur

[14] Delegierte Verordnung (EU) Nr. 907/2014 der Kommission vom 11. März 2014 zur Ergänzung der Verordnung (EU) Nr. 1306/2013 des Europäischen Parlaments und des Rates im Hinblick auf die Zahlstellen und andere Einrichtungen, die finanzielle Verwaltung, den Rechnungsabschluss, Sicherheiten und die Verwendung des Euro, Anhang I 3. B) i.

[15] Anstelle des BSI-Grundschutzes können auch angewandt werden COBIT oder der Standard ISO/IEC 27002.

[16] Für kleinere und mittelgroße Kommunen siehe nachfolgend ISIS12-Vorgehensweise.

Informationssicherheit. Im Übrigen können die ISO-Standards der Reihe 2700x ergänzend herangezogen werden.

4.3 COBIT 5 InfoSec

COBIT 5 InfoSec baut auf das COBIT 5 Rahmenwerk für IT-Management auf, ist aber auf Informationssicherheit fokussiert. Das Papier berücksichtigt mehrere internationale Standards (z. B. die Standards der ISO-Reihe 2700x). Es trifft Aussagen zur IT-Organisation sowie zu Diensten, Infrastrukturen und Applikationen. Es enthält ein für die Belange des ISMS zugeschnittenes COBIT-5-Prozessmodell.

Der ganzheitliche Ansatz von COBIT 5 und COBIT 5 for Information Security kann ergänzend für den Aufbau eines ITMS im Rahmen des IT-Managements herangezogen werden.

4.4 IT Infrastructure Library (ITIL)

ITIL ist ein Standard für Gestaltung, Implementierung und Management wesentlicher Steuerungsprozesse in der IT.

Eigene Aussagen zur IT-Sicherheit werden in ITIL nicht getroffen. Das Informationssicherheitsmanagement ist eingebettet in das IT-Servicemanagement. Daraus ergibt sich eine prozessbezogene Sichtweise auf das IT-Sicherheitsmanagement. Bei der Implementierung der IT-Serviceprozesse können die Bausteine des IT-Grundschutzes integriert werden.

ITIL kann bei der Definition von Prozessen im Rahmen des IT-Managements ergänzend herangezogen werden.

5 Handlungs- und Umsetzungsempfehlungen für Kommunen

5.1 Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen[17]

Eine vom Deutschen Städtetag, Deutschen Landkreistag, Deutschen Städte- und Gemeindebund und der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V. eingesetzte Arbeitsgruppe hat eine Handreichung zur Ausgestaltung der Informationssicherheitsrichtlinie in Kommunalverwaltungen erarbeitet.

[17] http://www.staedtetag.de/imperia/md/content/dst/internet/fachinformationen/2013/handreichung_ausgestaltung_infromationssicherheitsleitlinie_nov_2014_.pdf

Der Leitfaden richtet sich in erster Linie an die Leitungsebene der Kommunalverwaltungen. Er beschreibt in einem Vier-Phasen-Modell die Einführung eines ISMS. Der Leitfaden enthält Musterformulierungen für eine Informationssicherheitsleitlinie.

Der IT-Planungsrat hält die Handreichung insbesondere in der Orientierungs- und Einstiegsphase der Entwicklung und Gestaltung von Informationssicherheitsleitlinien sowie für Aufbau und Betrieb eines kommunalen ISMS für geeignet und empfiehlt den Kommunalverwaltungen deren Anwendung (Entscheidung 2015/05).
Der Landesrechnungshof empfiehlt die Vorgehensweise nach dem Leitfaden.

5.2 Informations-Sicherheits-Management-System in 12 Schritten (ISIS12)

Die Einführung eines Informationssicherheitsmanagements nach ISO/IEC 27001 oder dem BSI-Grundschutz ist aufwändig. Für kleine und mittelständische Unternehmen wurde die ISIS12-Vorgehensweise entwickelt. Im Unterschied zum hochgradig detaillierten BSI-Grundschutz weist ISIS12 einen mittleren Detaillierungsgrad auf, ist aber praktikabler umsetzbar, als die eher abstrakten Standards der ISO/IEC 2700x-Reihe. Während der BSI-Grundschutz ca. 1.100 Maßnahmen und 4.500 Seiten umfasst, konzentriert sich ISIS12 auf ca. 400 Maßnahmen und beschränkt die Dokumentation auf ca. 170 Seiten.

Das ISIS12-Handbuch beschreibt den Einführungsprozess eines ISMS in 12 sequentiell zu durchlaufenden Schritten. Der Katalog enthält eine ausgewählte Untermenge der IT-Grundschutz-Kataloge des BSI mit dazugehörigen Maßnahmen.

Der IT-Planungsrat stellt fest, dass mit ISIS12 für kleine und mittelgroße Kommunen ein pragmatisches und skalierbares Vorgehensmodell zur Einführung eines ISMS zur Verfügung steht, das die entsprechenden Mindestanforderungen des IT-Planungsrats abdeckt (Entscheidung 2015/05).

Der Landesrechnungshof empfiehlt Gemeinden und Amtsverwaltungen, die ISIS12-Vorgehensweise umzusetzen.

6 Fazit

Staatskanzlei, Ministerien, nachgeordnete Behörden und Einrichtungen der Landesverwaltung müssen die IT-Grundschutzstandards des BSI anzuwenden. In der Einführungsphase sind vorrangig die Mindestanforderungen aus der Leitlinie des IT-Planungsrats für Informationssicherheit in der öffentlichen Verwaltung und der ISO/IEC-Standards 27001 umzusetzen.

Rechtspersonen des öffentlichen Rechts in Trägerschaft des Landes wird empfohlen, die IT-Grundschutzstandards des BSI oder mindestens die ISO/IEC-Standards 27001, 27002 und 27005 anzuwenden.

Landkreise, kreisfreie Städte und die großen kreisangehörigen Städte sowie Rechtspersonen des öffentlichen Rechts in kommunaler Trägerschaft sollen die IT-Grundschutzstandards, Ämter und Gemeinden die ISIS12-Vorgehensweise umsetzen. Kommunen als Beteiligte an ebenenübergreifenden Verfahren müssen die Mindeststandards der Leitlinie des IT-Planungsrats für Informationssicherheit in der öffentlichen Verwaltung einhalten.

7 Prüfungsmaßstäbe des Landesrechnungshofes

Der Landesrechnungshof Mecklenburg-Vorpommern wird, soweit unter Berücksichtigung der o. g. Empfehlungen jeweils einschlägig, bei Prüfungen von Informationssicherheitsmanagementsystemen folgende Maßstäbe heranziehen:

- Grundsatzpapier der Rechnungshöfe zum Informationssicherheitsmanagement,
- Fragenkatalog der Rechnungshöfe zum Informationssicherheitsmanagement,
- ISO/IEC-Standard 27001,
- BSI-Standards 100-1, 100-2, 100-3 und 100-4,
- ISIS12-Handbuch und -Katalog,
- Leitlinie des IT-Planungsrats für die Informationssicherheit in der öffentlichen Verwaltung,
- IS-Leitlinie M-V (für Prüfungen bei Staatskanzlei und Ressorts),
- ISM M-V (für Prüfungen bei Staatskanzlei und Ressorts),
- Beschlüsse und Empfehlungen des IT-Planungsrats.

Ergänzend und mit empfehlenden Charakter wird der Landesrechnungshof die Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, weitere ISO/IEC-Standards zur Informationssicherheit der Reihe 2700x, COBIT 5 InfoSec und ITIL heranziehen.

gez. Dr. Schweisfurth gez. Arenskrieger
gez. Dr. Hempel gez. Scheeren