Informationssicherheit der Landkreisverwaltungen

9

An das Thema Informationssicherheit ist die überwiegende Anzahl der Landkreisverwaltungen unsystematisch herangegangen. Es gibt noch große Lücken.

Die Landkreisverwaltungen sind auf Notfälle nicht ausreichend vorbereitet.

1 Prüfungsgegenstand

1 Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität sowie Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind.[1]

2 Modernes Verwaltungshandeln ist ohne Einsatz von IT (IT-Infrastrukturen und IT-Verfahren) nicht mehr denkbar. Die Verlässlichkeit des IT-Einsatzes gilt es zu schützen. Mit der Prüfung sollte deshalb untersucht werden, ob die Landkreisverwaltungen an das Thema Informationssicherheit systematisch herangehen und wie sie es ausgestalten. Dabei interessierte insbesondere, welche Maßnahmen die Landkreise getroffen haben, um die Informationssicherheit in ihrer Verwaltung zu gewährleisten. Der Prüfungszeitraum umfasst die Jahre 2011 bis 2015 und schließt alle 10 Landkreisverwaltungen ein.

3 Maßstab bei der Bewertung des SRH sind die Empfehlungen zum IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI).[2]

2 Prüfungsergebnisse

2.1 Standards

4 Für die Gewährleistung einer angemessenen Informationssicherheit ist eine systematische und konzeptionelle Herangehensweise an den Informationssicherheitsprozess notwendig. Dafür stehen verschiedene Standards wie die IT-Grundschutzstandards des BSI, die ISO 2700x[3], die ISIS12[4] oder die VdS-Richtlinien 3473[5] zur Verfügung.

5 Eine Rechtsgrundlage zur Gewährleistung von Informationssicherheit, wie die VwV Informationssicherheit in der sächsischen Staatsverwaltung, gibt es im Kommunalbereich nicht. Damit sind die Landkreisverwaltungen nicht verpflichtet, sich auf einen Standard zur Informationssicherheit festzulegen.

6 3 Landkreisverwaltungen haben den IT-Grundschutz des BSI als maßgeblichen Standard für ihr Informationssicherheitsmanagement festgelegt. Bei den anderen 7 Landkreisverwaltungen fehlt diese Festlegung, wobei 5 Landkreisverwaltungen sich zumindest am IT-Grundschutz des BSI orientieren.

Keine verbindliche Vorgehensweise

[1] VwV Informationssicherheit, Nr. 2.1.1.
[2] Diese hat das BSI zwischenzeitlich weiterentwickelt und die 1. Edition des IT-Grundschutzkompendiums 2018 herausgebracht. Die 2. Edition mit weiteren Bausteinen soll im Februar 2019 veröffentlicht werden. Entsprechende Migrationshilfen stellt das BSI bereit.
[3] International Organization for Standardization.
[4] Informations-Sicherheitsmanagement-System in 12 Schritten.
[5] Herausgeber: VdS Schadenverhütung GmbH

7 **Fehlt die Festlegung auf einen Standard, fehlt zugleich die verbindliche Vorgehensweise, wie ein angemessenes Sicherheitsniveau für die Informationssicherheit zu erzielen und aufrechtzuerhalten ist.**

2.2 Leitlinie

8 Die Informationssicherheitsleitlinie ist das zentrale Strategiepapier für die Informationssicherheit einer Institution. Sie dokumentiert die Sicherheitsziele und die Strategie ihrer Umsetzung.

Mängel in Leitlinien

9 Alle 10 Landkreisverwaltungen hatten eine Leitlinie erlassen. Viele Leitlinien enthielten aber Mängel.

10 So war z. B. in 4 Landkreisverwaltungen die Gesamtverantwortung des Landrates für Informationssicherheit nicht klar geregelt. In anderen Leitlinien fehlte die eindeutige Festlegung ihres Geltungsbereichs, sodass nicht feststand, ob die Leitlinie auch für die rechtlich unselbstständigen nachgeordneten Einrichtungen oder Eigenbetriebe der Landkreisverwaltung gelten soll oder ob diese eigene Regelungen zur Informationssicherheit erlassen müssen.

11 **Die Leitlinie, als die gemeinsame Wertebasis einer Institution, sollte klar und eindeutig definiert sein.**

2.3 Informationssicherheitskonzept

12 Das Informationssicherheitskonzept beschreibt, wie die in der Informationssicherheitsleitlinie gesetzten Sicherheitsziele einer Institution zu erreichen sind. Es umfasst die Strukturanalyse, die Schutzbedarfsfeststellung sowie die Auswahl, Konsolidierung, Anpassung und Realisierung geeigneter Maßnahmen.

2.3.1 Strukturanalyse

13 Grundlage eines Informationssicherheitskonzeptes ist die genaue Kenntnis der Informationen, Prozesse und unterstützenden technischen Systeme. Diese sind lückenlos zu erheben und im Rahmen einer Strukturanalyse zu betrachten. Für nicht analysierte Informationen, Prozesse und unterstützende technische Systeme können keine angemessenen Sicherheitsmaßnahmen ergriffen werden.

14 Alle Landkreisverwaltungen hatten mit der Strukturanalyse begonnen. Zumeist wurde sie nur für die Verfahren *Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums* und *Nationales Waffenregister* durchgeführt. Die weiteren betriebenen IT-Verfahren blieben großteils außer Betracht, die Strukturanalyse war somit unvollständig.

Unvollständiges Lagebild erschwert verlässliche Entscheidungen

15 **Damit fehlt hier den Verantwortlichen ein vollständiges Lagebild, sodass Sicherheitsmaßnahmen weder verlässlich geplant noch umgesetzt werden können.**

2.3.2 Schutzbedarfsfeststellung

16 Nach Vorlage der Strukturanalyse gilt es festzustellen, welcher Schutz ausreichend und angemessen ist. Die Schutzbedarfsfeststellung sollte sich an den zu erwartenden Auswirkungen, die bei der Verletzung eines der Schutzziele Vertraulichkeit, Verfügbarkeit oder Integrität eintreten können, orientieren.

Schutzbedarf unvollständig erhoben

17 Nur 2 der 10 Landkreisverwaltungen hatten den Schutzbedarf vollständig erhoben. Oft war der Prozess auch noch nach Jahren unvollständig. So fehlten z. B. bei einer Landkreisverwaltung nach 6 Jahren noch immer zahlreiche Rückmeldungen der Fachbereiche. Eine andere Landkreisverwaltung hatte die Schutzbedarfsfeststellung ihrer Fachbereiche zwar erhalten, schätzte diese aber als nicht geeignet für eine Konzepterstel-

lung ein. Auch hier war der Schutzbedarf nach 7 Jahren nicht festgestellt.

18 Obwohl der Schutzbedarf in 8 Landkreisverwaltungen nicht hinreichend festgestellt war, wurden Sicherheitsmaßnahmen umgesetzt. So haben z. B. 2 Landkreisverwaltungen neue Serverräume eingerichtet. Ohne Schutzbedarfsfeststellung fehlt jedoch der Maßstab zur Beurteilung, ob die bereits umgesetzten und die geplanten Sicherheitsmaßnahmen angemessen und damit wirtschaftlich sind.

19 **Der Schutzbedarf steuert die Sicherheitsanstrengungen zielgerichtet.**

20 Die Landkreisverwaltungen haben in weiten Teilen vergleichbare Aufgaben zu erfüllen und setzen dabei häufig gleiche oder vergleichbare IT-Verfahren ein.

21 Dennoch wiesen die Schutzbedarfsfeststellungen - soweit sie vorlagen - teilweise erhebliche Unterschiede auf. So haben Landkreisverwaltungen z. B. die Integrität des IT-Verfahrens *Nationales Waffenregister* in die niedrigste und andere Landkreisverwaltungen in die höchste Schutzbedarfskategorie eingestuft.

22 **Dies kann teuer werden, denn ein höherer Schutzbedarf als notwendig erfordert weitergehende Maßnahmen mit entsprechendem Aufwand und Folgeaufwand.**

2.3.3 Maßnahmen

23 Der SRH hat u. a. die von den Landkreisverwaltungen ergriffenen Maßnahmen zum Passwortgebrauch, zur Datensicherung und zum Schutz ihrer zentralen IT (Serverräume) geprüft.

Passwortregelungen unzureichend

24 Nur in 5 Landkreisverwaltungen waren die Regelungen zum Passwortgebrauch BSI-konform. In 4 Landkreisverwaltungen hatten diese z. T. erhebliche Mängel. So waren Passwörter nicht ausreichend komplex, der Passwortwechsel wurde nicht erzwungen, sodass dasselbe Passwort bis zu einem Jahr genutzt werden konnte oder der Zugang zum IT-System wurde auch nach einer beliebigen Anzahl falscher Passworteingaben nicht gesperrt. Eine Landkreisverwaltung hatte keine Regelungen zum Passwortgebrauch erlassen.

25 **Ist der Zugang zum IT-System oder einer Anwendung nicht eng vorgegeben, besteht ein erhebliches Risiko, z. B. durch reines „Ausprobieren" oder mit entsprechenden Werkzeugen einen Treffer zu landen und damit unberechtigt Zugriff auf Informationen und Anwendungen erhalten zu können.**

26 9 der 10 Landkreisverwaltungen hatten ein Datensicherungskonzept erarbeitet. Davon waren jedoch nur 2 Konzepte BSI-konform, wobei sich die Erarbeitung eines der beiden Konzepte über 8 Jahre hinzog. In den anderen 7 Konzepten fehlten häufig Verantwortlichkeiten und Befugnisse. Einige Datensicherungskonzepte waren sehr allgemein und nicht auf die eigene Landkreisverwaltung zugeschnitten. Eine Landkreisverwaltung hatte kein Datensicherungskonzept erarbeitet.

27 **Eine angemessene und funktionstüchtige Datensicherung ist elementare Vorsorge auf den Notfall. Es empfiehlt sich, dafür ein Datensicherungskonzept entsprechend BSI zu erarbeiten.**

28 In Servern elektronisch gespeicherte Daten und Software der Verwaltung sind Teil der ordnungsgemäßen Informationsverwaltung. Server sind in diesem Sinne die Lagerräume für die Rohstoffe (Daten) und Produktionsmittel (Software) der Landkreisverwaltungen. Ohne intakte und sichere Server können die Landkreisverwaltungen ihre Aufgaben nicht mehr erfüllen.[6] Ein Serverraum ist deshalb ein sicherheitsrelevanter Bereich, an den spezielle Anforderungen gestellt werden.

Mängel bei Serverräumen

29 Der SRH hat 15 Serverräume in 5 Landkreisverwaltungen vor Ort geprüft. Es gab keinen Serverraum ohne Mangel, in 7 Serverräumen waren die Mängel erheblich.

30 Mehrfach waren Eingangstüren zu den Serverräumen einfache Bürotüren, keine Sicherheits- oder Brandschutztüren und nicht alarmgesichert. Auch die Wände boten teilweise nur wenig Schutz. Sie waren in Trockenbauweise erstellt.

31 Häufig fehlte ein Konzept für die Zutrittskontrolle zu den Serverräumen. Zutrittsberechtigungen wurden teilweise sehr weit ausgelegt. So hatte in einer Landkreisverwaltung neben den Administratoren die gesamte Leitungsebene der Landkreisverwaltung die Schließberechtigung für alle Serverräume.

32 Gefährdungen durch Wasser bestanden in mehreren Serverräumen. Oft waren angeschlossene Heizkörper ein Risiko. In einem Serverraum verlief unmittelbar über den Servern ein wasserführendes Rohr. Die darunter montierte Rinne hätte austretendes Wasser zwar zur Wand abgeleitet, dort wäre das Wasser aber im freien Fall aus einer Höhe von rd. 2,5 m auf den Boden gefallen und hätte sich im abflusslosen Serverraum gestaut.

33 In einer anderen Landkreisverwaltung war ein Feuchtefühler vorhanden, der aber keinen Alarm auslöste.

34 **Allein die Dokumentation eines sicherheitsrelevanten Ereignisses reicht jedoch nicht aus. Dies wäre vergleichbar mit einem Rauchmelder, der nur den Zeitpunkt der Branderkennung dokumentiert, aber keinen Alarm auslöst.**

35 Zum Teil wurden Serverräume auch als Lager- und Abstellraum für IT und Verpackungsmaterial genutzt. Hier war eine nicht unerhebliche Brandlast vorhanden. Im direkten Umfeld mehrerer Serverräume waren auch Pulver-Feuerlöscher vorhanden. Diese sollten hier allerdings nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind.

36 Die Landkreisverwaltungen haben in vielen Fällen noch während der Prüfung die Hinweise des SRH zu den Serverräumen aufgegriffen und Maßnahmen umgesetzt oder deren Umsetzung zugesagt.

Systematischere Herangehensweise erforderlich

37 **Dies reicht jedoch nicht aus. Bei einer systematischeren Herangehensweise an den Prozess Informationssicherheit wäre eine Vielzahl der vorgefundenen Mängel vermeidbar gewesen.**

2.4 Notfallmanagement

38 Ziel des Notfallmanagements ist es, die Robustheit der IT-Systeme und -Prozesse zu erhöhen, um bei Störungen oder im Schadensfall, deren Auswirkung auf die Verwaltungsprozesse zu minimieren.

[6] Vgl. Niedersächsischer Landesrechnungshof, Jahresbericht 2015, V.4. Informationssicherheit in Serverräumen.

39 Die systematische Herangehensweise sollte sich im Notfallmanagement fortsetzen. Dafür empfiehlt es sich, ein Notfallkonzept zu erarbeiten. Lediglich 4 Landkreisverwaltungen haben sich bereits intensiver mit der Konzeption eines IT-Notfallmanagements auseinandergesetzt und konnten entsprechende Dokumente vorlegen. Weitere 4 Landkreisverwaltungen haben zumindest elementare Bausteine umgesetzt und damit Grundlagen für ein Notfallkonzept geschaffen. In 2 Landkreisverwaltungen fehlte eine entsprechende Konzeption.

40 In einem weiteren Schritt werden alle für die Notfallbewältigung benötigten Strukturen, Informationen sowie Maßnahmen nach Eintritt eines Notfalls und zur Wiederaufnahme des Geschäfts in einem Notfallhandbuch zusammengefasst.

Notfallhandbücher fehlen

41 5 Landkreisverwaltungen haben kein Notfallhandbuch oder Handlungsanweisungen im Sinne eines IT-Notfallmanagements. Weitere 3 Landkreisverwaltungen konnten ein nur unvollständiges Notfallhandbuch vorweisen, so fehlten Kontaktdaten/Verantwortliche oder Handlungsanweisungen für kritische Prozesse und Verfahren. Lediglich 2 Landkreisverwaltungen haben Notfallhandbücher übersandt, die gemessen am Inhalt, eine angemessene Reaktion im Notfall ermöglichen.

42 **Die Landkreisverwaltungen sind auf Notfälle nicht ausreichend vorbereitet.**

43 Die Wirksamkeit vorgesehener Maßnahmen des Notfallmanagements ist mithilfe von Tests und Notfallübungen zu überprüfen. Ziel dieser Tests und Übungen ist, Inkonsistenzen in Notfallplänen oder Mängel bei der Planung und Umsetzung von Notfallmaßnahmen aufzudecken sowie die Abläufe für den Notfall zu trainieren.[7] Die Tests und Notfallübungen sollten auf einem Konzept basieren.

44 3 Landkreisverwaltungen hatten weder Tests noch Notfallübungen im Sinne eines IT-Notfallmanagements vorgesehen. In 6 weiteren Landkreisverwaltungen gab es Regelungen, die entsprechende Übungen zumindest vorsahen. Nur eine von 10 Landkreisverwaltungen hat eine ausführliche Planung für Tests und Notfallübungen ausgearbeitet.

Keine Notfallübungen

45 Ereignisunabhängige Tests und Übungen von Notfallmaßnahmen konnte jedoch keine Landkreisverwaltung nachweisen.

46 **Die Landkreisverwaltungen sollten IT-Notfallübungen und Tests künftig systematisch planen, vorbereiten, durchführen, auswerten und dokumentieren.**

3 Folgerungen

47 Den Landkreisverwaltungen wird die verbindliche Anwendung der IT-Grundschutzstandards des BSI empfohlen. Diese Standards haben sich bewährt und sind in vielen Bereichen der öffentlichen Verwaltung, z. B. in der sächsischen Staatsverwaltung oder in der Bundesverwaltung, maßgeblich.

48 Die Landkreisverwaltungen sollten die Strukturanalyse durchführen und den Schutzbedarf umfassend feststellen. Erst dann haben die Verantwortlichen ein vollständiges Lagebild, aus dem angemessene Schutzmaßnahmen abgeleitet werden können.

[7] Vgl. BSI, IT-Grundschutz-Kataloge: 13. Ergänzungslieferung, Stand 2013, S 4.991.

49 Der SRH empfiehlt dringend - auch im Hinblick auf die vorgefundenen Mängel -, sich des Themas IT-Notfallmanagement mehr als bisher anzunehmen.

4 Stellungnahmen

50 Die Landkreisverwaltungen trugen keine Einwände oder Bedenken zu den dargestellten Prüfungsergebnissen vor.

51 Das SMI teilte mit, der Jahresberichtsbeitrag zeige in seiner detaillierten Betrachtung und Analyse einen Status quo auf, der sich mit der Einschätzung des Beauftragten für Informationssicherheit des Landes zur Lage der Informationssicherheit in der kommunalen Selbstverwaltung decke. Der schlussfolgernden Empfehlung an die Landkreisverwaltungen, die IT-Grundschutzstandards des BSI anzuwenden, schließe sich der Beauftragte für Informationssicherheit des Landes an. Derzeit erarbeite er ein Sächsisches Informationssicherheitsgesetz. Es soll den IT-Grundschutz des BSI für die Staatsverwaltung verbindlich und für die Kommunen im Sinne einer „Soll"-Vorschrift vorschreiben. Mit Verabschiedung des Gesetzes würden viele der beschriebenen Mängel, wie die teilweise noch fehlende Gesamtverantwortung der Behördenleitung für die Informationssicherheit in ihrem Bereich, durch die Verwaltungen abgestellt werden.

5 Schlussbemerkung

52 Der SRH begrüßt die Erarbeitung eines Sächsischen Informationssicherheitsgesetzes, mit dem der IT-Grundschutz des BSI auch für die Kommunen im Sinne einer „Soll"-Vorschrift festgelegt wird.