Landesrechnungshof Sachsen-Anhalt

Bericht

über

die Prüfung der Sicherheit der IT

in den Kommunen Sachsen-Anhalts

Aktenzeichen 42-04311/Querschnitt IT

Dessau-Roßlau, 29. Juni 2023

Inhaltsverzeichnis Seite

Vorschriften und Abkürzungsverzeichnis

Rechtsgrundlagen

AO	Abgabenordnung in der Fassung der Bekanntmachung vom 01.10.2002 (BGBl. I S. 3866, ber. 2003 S. 61) zuletzt geändert durch Gesetz vom 16.12.2022 (BGBl. I S. 2294)
BeamtStG	Beamtenstatusgesetz in der bis 6. Dezember 2018 bzw. 6. Juli 2021 geltenden Fassung
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982)
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Artikel 1 der Verordnung vom 23. Februar 2023 (BGBl. I Nr. 53)
DSGVO	Datenschutzgrundverordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27. April 2016 in der Fassung vom 25. Mai 2018
GG	Grundgesetz
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) – BMF-Schreiben vom 28.11.2019 – IV A 4 – S 0316/19/10003 :001
KomKBVO	Verordnung über die Kassen- und Buchführung der Kommunen im Land Sachsen-Anhalt nach den Grundsätzen der doppelten Buchführung (Kommunalkassen- und Buchführungsverordnung - KomKBVO) vom 25. März 2021
KVG LSA	Kommunalverfassungsgesetz des Landes Sachsen-Anhalt vom 17. Juni 2014 zuletzt geändert durch Gesetz vom 19. März 2021 (GVBl. LSA S. 100)

Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
DA	Dienstanweisung
GVBl.	Gesetz und Verordnungsblatt
HVB	Hauptverwaltungsbeamte/r
ISB	Informationssicherheitsbeauftragte/r
ISM	Informationssicherheitsmanagement
IT	Informationstechnik
LK	Landkreis
LSA	Land Sachsen-Anhalt
RPA	Rechnungsprüfungsamt
Tz.	Textziffer
VzÄ	Vollzeitäquivalente

I. Zusammenfassung der wesentlichen Prüfungsfeststellungen

Der Landesrechnungshof stellte bei seiner überörtlichen Querschnittsprüfung der Sicherheit der IT in 27 Kommunen im Land Mängel und Versäumnisse fest. Diese lassen sich wie folgt zusammenfassen:

Keine der geprüften 28 Kommunen war hinsichtlich der Sicherheit der IT zertifiziert oder testiert. In 20 von 28 Kommunen (71 %) fehlte als wesentliche Grundlage für IT-Sicherheit eine Leitlinie und in 19 von 28 Kommunen (68 %) ein Notfallhandbuch. Ein IT-Sicherheitskonzept war sogar in 26 von 28 Kommunen (93 %) nicht vorhanden.

Einen Informationssicherheitsbeauftragten (ISB) als maßgebliche Stelle für die operative Erfüllung der Aufgabe „Informationssicherheit" hatten nur 11 von 28 Kommunen (39 %) benannt. Dabei betrug der prozentuale Stellenanteil des ISB bezogen auf eine VzÄ zwischen 5 % und 100 %.

Obwohl alle geprüften Kommunen flächendeckend Schutzprogramme vor Schadprogrammen einsetzten, verfügten nur 9 von 28 (32 %) über ein schriftliches Konzept für den Schutz des IT-Systems vor Schadprogrammen.

Von den geprüften Kommunen verfügte eine Kommune nach ihren eigenen Angaben über keine Sicherheitsmechanismen.

Von den geprüften Kommunen verfügten nur 13 von 28 (46 %) über ein niedergeschriebenes Konzept zur Datensicherung (Minimaldatensicherungskonzept). Eine Kommune führte überhaupt keine Datensicherungen durch.

Eine Kommune hatte ihre Serverräume nicht gegen unberechtigten Zutritt gesichert.

Nur 15 von 28 Kommunen (54 %) boten für ihre IT-Mitarbeiter und 14 von 28 (50 %) für die anderen Mitarbeiter spezielle Fortbildungen zum Thema IT-Sicherheit an. In 27 von 28 Kommunen (96 %) bestand keine Verpflichtung der IT-Mitarbeiter zur mindestens jährlichen Fortbildung im Bereich der IT-Sicherheit. Darüber hinaus fanden in 8 von 28 Kommunen (29 %) keine Belehrungen zum Thema IT-Sicherheit statt.

II. Vorbemerkungen

Die überörtlichen Kommunalprüfungen sowie die Prüfungen der Eröffnungsbilanzen haben regelmäßig Mängel der Organisation der IT bei notwendigen Regelungen und Verantwortlichkeiten in den Kommunen aufgezeigt. Diese Feststellungen wurden durch die Vorfälle der jüngeren Vergangenheit, wie Angriffe auf die IT in Kommunen (u. a. im LK Anhalt-Bitterfeld im Juli 2021) bestätigt. Zu den Risiken einer Cyberattacke gehören neben den direkten Kosten in der Institution selbst (z. B. Kosten für Produktivitätsausfall, Personalkosten, Kosten für die Fehlersuche, Kosten für die Fehlerbereinigung) auch etwaige Schadensersatzansprüche (z. B. durch die Verletzung von Persönlichkeitsrechten auf der Grundlage der DSGVO).

Die IT durchdringt alle Bereiche der Kommune. Sie trägt zu fast jeder kommunalen Leistungserstellung unmittelbar oder mittelbar bei. Die Folgen eines Fehlers oder Ausfalls von Funktionen aufgrund einer Beeinträchtigung oder Manipulation der IT können gravierende Auswirkungen haben. Des Weiteren sind Investitionen in die IT Infrastruktur gewichtige Haushaltsgrößen. Diese Investitionen sind durch die Implementierung von Sicherheitsvorkehrungen ausreichend zu schützen.

Zwar gibt es für die konkrete Ausgestaltung von IT-Systemen in Kommunen keine rechtlichen Vorgaben. Der Hauptverwaltungsbeamte[1] (HVB) ist jedoch gemäß § 66 Abs. 1 KVG LSA für die sachgemäße Erledigung der Aufgaben und für den ordnungsgemäßen Gang der Verwaltung verantwortlich und regelt ihre innere Organisation. Er haftet folglich, wenn in Folge mangelnder Regelungen nicht geeigneten Personals bzw. fehlender Kontrollen Fehler oder Ausfälle von Funktionen der IT eintreten und daraus Schäden für Dritte resultieren. So haben z. B. Personen nach Art. 82 DSGVO Anspruch auf Schadensersatz, wenn aufgrund eines nicht den technischen Anforderungen entsprechenden Systems (IT-System/Datensicherheitssystem[2]) z. B. Daten von Personen rechtswidrig öffentlich gemacht werden.
Die Haftung für schuldhaftes Verhalten (Handeln oder Nichthandeln) kann finanzielle (Schadensersatz), disziplinarische[3], ordnungsrechtliche oder sogar strafrechtliche[4] Folgen nach sich ziehen.

Des Weiteren besteht eine Vielzahl von Vorschriften, die vorgeben, welche Anforderungen ein IT-System erfüllen muss. Dabei ist zu berücksichtigen, dass es häufig keine trennscharfe Abgrenzung, z. B. von Rechtsbereichen, gibt. So gibt es Schnittmengen zwischen

---

1 Landrat, Oberbürgermeister, Bürgermeister.
2 Dieses betrifft digitale und analoge Daten.
3 Oberverwaltungsgericht des Landes Sachsen-Anhalt, Urteil vom 6. Juli 2022 - 10 L 1/21 - juris.
4 Abgrenzung §§ 371, 378 Abs. 3 AO, siehe Bundesfinanzministerium, Anwendungserlass zu § 153 AO vom 23.05.2016, Az. IV A 3 - S 0324/15/10001, IV A 4 - S 0324/14/10001 (DOK 2016/0470583)

Datenschutz(recht) (u. a. DSGVO), Datensicherheit und Informationssicherheit. Das Steuerrecht regelt für den Steuerpflichtigen verbindlich, dass er beim Einsatz elektronischer Verfahren die GoBD[5] zu beachten hat. Auch §§ 25 bis 28 KomKBVO machen verbindliche Vorgaben für Software und IT-Systeme einschließlich einzelner Sicherheitsstandards.

Was bedeutet das für die IT-Sicherheit in Kommunen?

Gemäß Artikel 20 Abs. 3 GG ist die öffentliche Verwaltung an Recht und Gesetz gebunden. Die Ordnungsmäßigkeit einer Verwaltung wird daher zunächst an der Rechtmäßigkeit des Verwaltungshandelns gemessen. Um die verfassungsrechtlichen Vorgaben einheitlich und flächendeckend umsetzen zu können, muss jede öffentliche Verwaltung über ein gesetzeskonformes Regelwerk verfügen, das

- regelmäßig aktualisiert wird,
- verbindlich in der Anwendung für alle Bediensteten ist und
- alle Geschäftsvorfälle und Entscheidungen für Dritte nachvollziehbar, systematisch und einheitlich dokumentieren lässt.

Die Gesamtheit aller systematisch gestalteten sowie aufeinander abgestimmten organisatorischen Maßnahmen und Kontrollen wird auch als Internes Kontrollsystem bezeichnet.

Für die systematische IT-Sicherheit in der jeweiligen Verwaltung stellt die Anwendung der BSI-Standards und des IT-Grundschutz-Kompendiums, die den allgemeinen Stand der Technik abbilden, einen grundlegenden Baustein dar. Dabei ist zu berücksichtigen, dass die durch das BSI gesetzten Standards von Betreibern (Behörden, Unternehmen, Einrichtungen) Kritischer Infrastrukturen (KRITIS) zwingend beachtet werden müssen[6] und sich daher als System etabliert haben. Auf die BSI-Standards stützen sich auch die Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik.[7]

Eine Empfehlung zur Anwendung des BSI-Grundschutzes hatte der Deutsche Landkreistag in Zusammenarbeit mit dem BSI bereits mit Datum vom 17.12.2021 in einem Leitfaden zusammengefasst. Für die Kommunalverwaltung wird darin mindestens eine Standard-Absicherung empfohlen.

Der Deutsche Landkreistag hat dies durch einen Beschluss vom 17.12.2021 bekräftigt und sich für eine verbindliche Festlegung des IT-Grundschutzes des BSI in allen Kreisverwaltungen ausgesprochen. Um die Standard-Absicherung zu erreichen, kann der Einstieg über die

---

5 BMF-Schreiben vom 28.11.2019 - IV A 4 - S 0316/19/10003 :001.

6 § 8a BSI-Gesetz i. V. m. BSI-KritisV.

7 Rechnungshöfe des Bundes und der Länder, Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik - Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen - (IT-Mindestanforderungen 2020).

Basis-Absicherung, beispielsweise mittels des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung", erleichtert werden.

III. Prüfungsgegenstand und Prüfungsverlauf

Der Landesrechnungshof prüfte im Rahmen der überörtlichen Kommunalprüfung die organisatorischen Vorkehrungen in den Verwaltungen unter dem Blickwinkel, ob Mindeststandards der IT-Sicherheit gemäß BSI gewährleistet wurden.

Prüfungsgegenstand ist das aufeinander aufbauende System von Regelungen und Rollen bei der Aufgabenwahrnehmung der Kommunen im Hinblick auf die Sicherheit der IT-Systeme. Zur Erhebung der Daten wurde ein strukturierter Online-Fragebogen zu Aspekten der IT Sicherheit nach dem BSI (BSI-Standards als anerkannte Regeln der Technik) an alle Kommunen in der Prüfungszuständigkeit des Landesrechnungshofes (11 Landkreise und 17 Städte) versandt.

Die Prüfung umfasste 13 Bereiche:

- Zertifizierung und Testierung,
- Informationssicherheitsmanagement (ISM),
- Notfallmanagement,
- Sicherheit von IT-Systemen,
- Internet-Anbindung,
- Wartung von IT-Systemen,
- Umgang mit Updates,
- Sicherheitsmechanismen,
- Datensicherung,
- Infrastruktursicherheit,
- Cloud,
- Personal,
- IT-Prüfung,
- Praxisfragen.

Zusätzlich forderte der Landesrechnungshof grundlegende Dokumente (Leitlinie, Sicherheitskonzept, Notfallhandbuch) ab, die er auf Plausibilität prüfte.

Der vorliegende Prüfungsbericht wertet die erhobenen Daten aus. Die Auswertungen basieren auf eigenen Angaben der Kommunen und auf eigenen Bewertungen der vorgelegten Unterlagen durch den Landesrechnungshof.

IV. Prüfungsergebnisse

Keine der in die Prüfungszuständigkeit des Landesrechnungshofes fallenden Kommunen war für ihr Informationssicherheitsmanagement zertifiziert oder testiert. Mit einem Zertifikat oder Testat wäre dokumentiert, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsanforderungen gemäß IT-Grundschutz realisiert wurden. Andererseits hatten alle Kommunen nach ihren Angaben ihre IT-Systeme durch eine Firewall geschützt.

1. Leitlinie

1.1 Grundvoraussetzungen

Die Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution (Behörde). In ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Laut BSI soll die Institutionsleitung, hier der HVB, im Rahmen ihrer Gesamtverantwortung eine übergeordnete Leitlinie zur Informationssicherheit verabschieden und regelmäßig aktualisieren. Die Institutionsleitung muss die Leitlinie zur Informationssicherheit allen Mitarbeitern und sonstigen Mitgliedern der Institution bekannt geben. Sowohl die regelmäßige Aktualisierung als auch die Bekanntgabe der Leitlinie sollten im Vordergrund stehen.

Der Landesrechnungshof hatte das Vorhandensein einer Leitlinie, die Festlegung von Sicherheitszielen in der Leitlinie, die Bekanntgabe sowie die jährliche Aktualisierung bei den Kommunen abgefragt. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zu diesen Fragen zusammen:

Tabelle 1 - Leitlinie

	Leitlinie	Festlegung Sicherheits-ziele in Leitlinie	Jährliche Aktualisie-rung	Bekannt-gabe
Kommune 1	●			
Kommune 2	○	○	○	○
Kommune 3	●			
Kommune 4	○	○	○	○
Kommune 5	●			
Kommune 6	●			
Kommune 7	●			
Kommune 8	●			
Kommune 9	●			
Kommune 10	●			
Kommune 11	○	○	●	○
Kommune 12	●			
Kommune 13	●			
Kommune 14	○	○	●	○
Kommune 15	●			
Kommune 16*	○	●	●	●
Kommune 17	●			
Kommune 18	●			
Kommune 19	●			
Kommune 20	○	○	●	○
Kommune 21	○	○	○	○
Kommune 22	●			
Kommune 23	○	○	○	○
Kommune 24	●			
Kommune 25	●			
Kommune 26	●			
Kommune 27	●			
Kommune 28	●			
Summe	8 (29 %)	7	4	7

* lag nur im Entwurf vor

In 20 von 28 Kommunen (71 %) lag dieses zentrale Dokument der IT-Sicherheit nicht vor.[8] Von den acht vorliegenden Leitlinien beinhalteten sieben die Informationssicherheitsziele. Vier Leitlinien wurden regelmäßig mindestens jährlich aktualisiert. Bei den übrigen vier Kommunen erfolgte die letzte Aktualisierung ihrer Leitlinie 2016, 2017 bzw. 2018. Sieben der acht Leitlinien

[8] Nach Abforderung und Überprüfung der Unterlagen konnte in einem Fall das Vorhandensein einer Leitlinie nicht bestätigt und somit nicht berücksichtigt werden. In einem Fall war nur der Entwurf vorgelegt worden und wurde durch den Landesrechnungshof somit einer inhaltlichen Bewertung unterzogen.

wurden allen Mitarbeitern und sonstigen Mitgliedern der Behörde (z. B. Kreistags- oder Stadtratsmitgliedern) u. a. in Form von Rundmails bzw. Veröffentlichungen im Intranet bekannt gegeben.

Der Landesrechnungshof sieht es als bedenklich an, dass bei ca. 71 % der geprüften Kommunen das grundlegende Dokument nicht vorliegt. Auch eine Leitlinie, die beispielsweise im Jahr 2016 das letzte Mal aktualisiert wurde, kann dem Grunde nach nicht den aktuellen Gegebenheiten entsprechen und ist anpassungsbedürftig.
Er hält es für dringend notwendig, dass alle Kommunen flächendeckend eine Leitlinie unter Berücksichtigung der o. g. Regelungen erlassen. Darüber hinaus sind die vorhandenen Leitlinien regelmäßig zu aktualisieren und darauf zu prüfen, ob alle erforderlichen Regelungen getroffen wurden (u. a. Benennung der Informationssicherheitsziele).

1.2 Weiterführende Voraussetzungen

Die Leitlinie soll für die betroffenen Mitarbeiter verständlich sein. Es soll in einem angemessenen Umfang beschrieben werden, welche Sicherheitsziele angestrebt und in welchem organisatorischen Rahmen diese umgesetzt werden sollen. Der Geltungsbereich der Leitlinie soll konkretisiert und die Verantwortung der Leitung betont werden. Die Organisationsstruktur für Informationssicherheit und die Aufgaben der verschiedenen Sicherheitsverantwortlichen sollen vorgestellt werden. Insbesondere soll auf die Möglichkeit von Sicherheitsschulungen und Sensibilisierungsmaßnahmen hingewiesen werden.

Die dem Landesrechnungshof vorgelegten Unterlagen wurden auf Umfang, Verständlichkeit, Geltungsbereich, Verantwortung, Organisationsstruktur der IT sowie Sensibilisierung der Mitarbeiter geprüft. Die folgende Tabelle fasst die abgefragten Kriterien zusammen.

Tabelle 2 - Prüfung und Bewertung der vorliegenden Leitlinien nach festgelegten Kriterien

	Umfang	Verständlichkeit	Geltungsbereich			Konkrete Verantwortung	Organisationsstruktur der IT	Schulung/ Sensibilisierung	**Gesamtbewertung durch den LRH[9]**
			Mitarbeiter	Eigenbetriebe	Polit. Gremien				
Kommune 2	○	○	○	○	●	●	○	●	○
Kommune 4	○	○	○	○	●	●	○	○	○
Kommune 11	○	○	○	○	●	○	○	○	○
Kommune 14	○	○	○	○	●	○	●	○	○
Kommune 16*	○	○	○	○	●	○	○	○	○
Kommune 20	○	○	○	○	●	○	○	○	○
Kommune 21	●	○	○	○	●	○	○	○	○
Kommune 23	○	○	○	○	●	○	●	○	○

* lag nur im Entwurf vor

Nahezu alle vorliegenden Leitlinien beschrieben auf wenigen Seiten verständlich die Sicherheitsziele ihrer Behörden. In der Kommune 21 waren die Festlegungen der Leitlinie Bestandteil einer mit 256 Seiten sehr umfangreichen Verwaltungsvorschrift. Diese Einbindung beeinträchtigt Lesbarkeit und Verständlichkeit und somit die Anwendung.

Der Geltungsbereich war regelmäßig auf die Mitarbeiter der Verwaltung bestimmt, aber nur zum Teil auf „angeschlossene" Eigenbetriebe/Einrichtungen der Verwaltung oder Dritte. In allen Fällen fehlte die Einbeziehung der Mitglieder der politischen Gremien. In allen vorliegenden Leitlinien wurde die Verantwortung für die Behördenleitung deutlich. In 75 % der geprüften Leitlinien wurde vom Prinzip des informierten Mitarbeiters ausgegangen und auf kontinuierliche Schulungs- und Sensibilisierungsmaßnahmen hingewiesen.

Der Landesrechnungshof bewertet die vorgelegten Leitlinien grundsätzlich als gut. Sie stellen eine Basis dar, enthalten allerdings noch Regelungslücken, die schnellstmöglich geschlossen werden sollten.

Er hält es für notwendig, dass die Kommunen in ihren Leitlinien die Verantwortung der Behördenleitung sowie die Organisationsstruktur für die Informationssicherheit klar aufzeigen. Der Geltungsbereich sollte auf alle Teilbereiche der Gebietskörperschaft,

---

[9] Bei der Gesamtbewertung handelt es sich um eine individuelle Einschätzung des LRH bezüglich des Umfanges, der Verständlichkeit, des Geltungsbereiches, der Verantwortung, der Organisationsstruktur der IT sowie der Sensibilisierung der vorgelegten Leitlinien. Die grüne Bewertung konnte erteilt werden, wenn alle Kriterien bis auf den Geltungsbereich in politischen Gremien erfüllt wurden. Beim Fehlen weiterer höchstens 4 Voraussetzungen konnte die Leitlinie vom LRH mit gelb bewertet werden. Bei mehr als 4 fehlenden Kriterien wurde die Richtlinie durch den LRH mit rot bewertet.

insbesondere auch auf die politischen Gremien, ausgeweitet werden. Der Landesrechnungshof empfiehlt der Kommune 21, ihre Leitlinie aus der 256-seitigen Verwaltungsvorschrift herauszulösen; auch um ihrer Stellung als Grundsatzdokument umfassend Rechnung zu tragen.

2. Sicherheitskonzept

2.1 Grundvoraussetzungen

Zur Umsetzung einer entsprechenden Sicherheitsstrategie, zur Erreichung gesetzter Sicherheitsziele sowie für die Erstellung konkreter Sicherheitsmaßnahmen muss eine Kommune ein angemessenes Sicherheitskonzept erstellen. Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution (Behörde) zu erreichen. Im Sicherheitskonzept müssen aus den Sicherheitszielen der Behörde, dem identifizierten Schutzbedarf und der Risikobewertung konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet werden. Die im Sicherheitskonzept vorgesehenen Maßnahmen müssen zeitnah in die Praxis umgesetzt werden. Dies muss geplant und die Umsetzung muss kontrolliert werden.

Der Landesrechnungshof hatte das Vorhandensein eines Sicherheitskonzeptes bei den Kommunen abgefragt. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen:

Tabelle 3 - Sicherheitskonzept

	Vorliegen eines Sicherheitskonzeptes
Kommune 1	●
Kommune 2	●
Kommune 3	●
Kommune 4	●
Kommune 5	●
Kommune 6	●
Kommune 7	●
Kommune 8	●
Kommune 9	●
Kommune 10	●
Kommune 11	●
Kommune 12	●
Kommune 13	●
Kommune 14	●
Kommune 15	●
Kommune 16	●
Kommune 17	●
Kommune 18	●
Kommune 19	●
Kommune 20	●
Kommune 21	○
Kommune 22	●
Kommune 23	○
Kommune 24	●
Kommune 25	●
Kommune 26	●
Kommune 27	●
Kommune 28	●
Summe	2 (7 %)

26 der 28 geprüften Kommunen hatten kein IT-Sicherheitskonzept. Lediglich bei zwei der geprüften Kommunen lag das zentrale Dokument im Sicherheitsprozess einer Behörde vor.

Der Landesrechnungshof bewertet es kritisch, dass 93 % der geprüften Kommunen nicht über ein IT-Sicherheitskonzept verfügten.

Er hält es für notwendig, dass alle Kommunen ein angemessenes Sicherheitskonzept erstellen. Dies dient der systematischen Umsetzung der Sicherheitsstrategie zur Erreichung der Sicherheitsziele.

2.2 Weiterführende Voraussetzungen

Im Rahmen des Sicherheitskonzeptes muss die geplante Vorgehensweise zur Umsetzung der Sicherheitsstrategie eindeutig beschrieben werden, damit die Sicherheitsziele unter wirtschaftlichem Einsatz der Ressourcen erreicht werden. Der Geltungsbereich soll klar festgelegt und erkennbar sein.

Das Sicherheitskonzept beschreibt, wie und mit welchen Maßnahmen die Ziele und Strategien der Leitlinie umgesetzt werden sollen. Es soll dabei immer einen festgelegten Geltungsbereich haben. Vorzugsweise soll die gesamte Institution betrachtet werden.

Der Landesrechnungshof hat die vorgelegten Sicherheitskonzepte auf das Vorhandensein eines Maßnahmenkataloges, die jährliche Aktualisierung, die Durchführung einer Risikobewertung, die Umsetzung der vorgesehenen Maßnahmen, die Festlegung verbindlicher Fristen, die Identifizierung des Schutzbedarfes, die Beschreibung der Umsetzung sowie des Geltungsbereiches geprüft und bewertet. Die folgende Tabelle fasst die abgefragten Kriterien zusammen.

Tabelle 4 - Prüfung und Bewertung der vorliegenden Sicherheitskonzepte nach festgelegten Kriterien

	Maßnahmenkatalog	Aktualisierung des Konzeptes einmal p.a.	Durchführung einer Risikobewertung	Umsetzung der vorgesehenen Maßnahmen (Kontrolle)	Festlegung verbindlicher Fristen zu Umsetzung	Identifizierung des Schutzbedarfes	Beschreibung der Umsetzung	Geltungsbereich			Gesamtbewertung durch den LRH[10]
								Mitarbeiter	Eigenbetriebe	Polit. Gremien	
Kommune 21	○	○	○	○	○	●	○	○	○	●	○
Kommune 23	○	○	○	○	●	○	○	○	○	●	○

Die geprüften Sicherheitskonzepte, eines lag nur in der Entwurfsfassung vor, enthielten nur zum Teil Maßnahmen zur Umsetzung der Sicherheitsstrategie. Der Geltungsbereich war

[10] Bei der Gesamtbewertung handelt es sich um eine Einschätzung des LRH. Da bei beiden Sicherheitskonzepten nach Auffassung des LRH jeweils eine wesentliche Festlegung zur Umsetzung der Sicherheitsstrategie fehlte, konnten diese nur mit gelb bewertet werden.

regelmäßig auf die Mitarbeiter der Verwaltung und auf Eigenbetriebe bestimmt. In beiden Fällen fehlte die Einbeziehung der Mitglieder der politischen Gremien oder sonstiger damit verbundener Personen (z. B. Mitarbeiter der Fraktionen).

Beide Kommunen aktualisieren regelmäßig mindestens jährlich das Sicherheitskonzept und haben eine Risikobewertung durchgeführt. Die vorgesehenen Maßnahmen aus dem Sicherheitskonzept wurden umgesetzt. Eine Kommune legte verbindliche Fristen für die Umsetzung fest und kontrollierte bzw. dokumentierte die Umsetzung. Eine Kommune hat in ihrem Sicherheitskonzept den Schutzbedarf identifiziert.

Der Landesrechnungshof bewertet die vorgelegten Sicherheitskonzepte grundsätzlich als geeignet, eine entsprechende Sicherheitsstrategie umzusetzen und damit gesetzte Sicherheitsziele zu erreichen. Allerdings fehlten in den Sicherheitskonzepten wesentliche Festlegungen zu Fristen und zur Identifizierung des Schutzbedarfes.
Der Landesrechnungshof hält es für notwendig, die Sicherheitskonzepte mit klaren Festlegungen zu ergänzen.

3. Dienstanweisungen, Informationsrichtlinien oder andere verbindliche Regelungen, Sicherheitsmechanismen

Die Aufgaben, Rollen, Verantwortungen und Kompetenzen im Sicherheitsmanagement müssen nachvollziehbar definiert und zugewiesen sein. Für alle wichtigen Funktionen in der IT-Organisation für Informationssicherheit muss es wirksame Vertretungsregelungen geben. Kommunikationswege müssen geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es muss für alle Aufgaben und Rollen festgelegt sein, wer wen informiert und wer bei welchen Aktionen in welchem Umfang informiert werden muss. Darüber hinaus ist der Zugang zu schützenswerten Ressourcen einer Institution auf berechtigte Benutzer und berechtigte IT-Komponenten einzuschränken. Benutzer und IT-Komponenten müssen zweifelsfrei identifiziert und authentisiert werden. Die Institution muss den Gebrauch dieser Sicherheitsmechanismen verbindlich regeln. In Behörden können für die genannten Regelungen auch Dienstanweisungen (DA) oder andere verbindliche Regelungen Anwendung finden.

Für eine gut funktionierende Sicherheit der IT sind eindeutige, transparente und detaillierte Regelungen von essentiellem Wert. Um richtig handeln zu können, müssen alle Mitarbeiter über die Rahmenbedingungen der IT-Nutzung und Sicherheitsmaßnahmen aufgeklärt werden. Weiterführende Regularien über die IT-Sicherheit sind hierbei ausschlaggebend. Die Erstellung von weitergehenden Regelungen zum Thema IT-Sicherheit ist auf verschiedene Art und Weise möglich.

Der Landesrechnungshof hatte das Vorhandensein von weitergehenden Regelungen (DA, Informationsrichtlinien oder andere verbindliche Regelungen) zum Thema IT-Sicherheit sowie das Vorhandensein von Zuständigkeiten und Verantwortlichkeiten abgefragt. Dabei handelte es sich beispielsweise um Regelungen zur Internetnutzung, zum Datenschutz, zur elektronischen Post oder zum Homeoffice. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen.

Tabelle 5 - DA, Informationsrichtlinien oder andere verbindliche Regelungen

	DA	Regelungen zur Internetnutzung	Regelungen zum Datenschutz	Regelungen zur elektronischen Post	Regelungen zum Homeoffice	Bekanntgabe
Kommune 1	●					
Kommune 2	○	○	○	○	○	○
Kommune 3	●					
Kommune 4	○	○	○	○	●	○
Kommune 5	○	○	○	○	○	●
Kommune 6	○	○	○	○	○	○
Kommune 7	○	○	●	○	○	○
Kommune 8	○	○	○	○	○	○
Kommune 9	○	○	○	●	○	○
Kommune 10	○	○	○	○	○	○
Kommune 11	○	○	○	○	○	○
Kommune 12	○	○	○	○	○	○
Kommune 13	○	○	○	○	○	○
Kommune 14	○	○	○	○	○	○
Kommune 15	○	●	○	○	○	○
Kommune 16	○	○	○	●	○	○
Kommune 17	○	●	●	○	○	○
Kommune 18	○	○	○	○	○	○
Kommune 19	○	○	○	●	○	○
Kommune 20	○	○	○	○	○	○
Kommune 21	○	○	○	○	○	○
Kommune 22	○	○	○	○	○	○
Kommune 23	○	○	○	○	○	○
Kommune 24	○	○	○	○	○	○
Kommune 25	○	●	○	○	○	○
Kommune 26	○	○	○	○	○	○
Kommune 27	○	○	○	○	○	○
Kommune 28	○	●	●	●	○	○
Summe	26 (93 %)	22	23	22	25	25

Nur 2 von 28 Kommunen hatten keine weitergehenden Regelungen zur IT-Sicherheit.

Der Landesrechnungshof regt an, dass in allen Kommunen weitergehende Regelungen zum Thema IT-Sicherheit erlassen werden.

Der Landesrechnungshof hatte darüber hinaus abgefragt, ob die Kommunen über Sicherheitsmechanismen, wie Passwortschutz oder Verschlüsselungsverfahren, verfügen und ob es eine verbindliche Festlegung der Sicherung der Arbeitsplatzrechner gibt.
Die Anwendung von Sicherheitsmechanismen liegt nach Auffassung des Landesrechnungshofes nicht im Ermessen der Kommune. Nach der Auflistung der elementaren Gefährdungen des BSI bestehen hierbei insbesondere die Gefahren des unbefugten Eindringens in IT-Systeme und des Verstoßes gegen Gesetze oder Regelungen.

Alle geprüften Kommunen verfügten über Sicherheitsmechanismen. In 5 Kommunen (Kommune 1, 5, 12, 15 und 17) wurde nicht verbindlich festgelegt, dass die Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert werden müssen.

Der Landesrechnungshof bewertet die vorgefundene Situation positiv. Gleichzeitig möchte er darauf hinweisen, dass die weiteren Regelungen die Leitlinie und das Sicherheitskonzept nicht ersetzen.
Der Landesrechnungshof hält es für notwendig, dass in allen Kommunen verbindlich festgelegt werden sollte, dass die Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert werden müssen.

4. Informationssicherheitsbeauftragter

Ein Informationssicherheitsbeauftragter (ISB) ist für die operative Erfüllung der Aufgabe „Informationssicherheit" zuständig. Die Institutionsleitung (HVB) muss einen ISB benennen. Der ISB muss die Informationssicherheit in der Behörde fördern und den Sicherheitsprozess mitsteuern und koordinieren. Der HVB muss dem ISB die Möglichkeit einräumen, bei Bedarf direkt an ihn selbst zu berichten. Der ISB muss bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme frühzeitig beteiligt werden. Der ISB muss allen Mitarbeitern der Behörde bekannt sein.
In jeder Institution muss es Ansprechpartner für Sicherheitsfragen geben, die sowohl scheinbar einfache als auch komplexe oder technische Fragen beantworten können.

Der Landesrechnungshof hatte das Vorhandensein eines Informationssicherheitsbeauftragten sowie dessen Stellenanteil bei den Kommunen abgefragt. Des Weiteren wurde abgefragt, ob

dieser bei größeren Projekten frühzeitig beteiligt wird und ob dieser den Mitarbeitern bekanntgegeben worden ist. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen:

Tabelle 6 - Informationssicherheitsbeauftragter

	ISB	Stellenanteil in %	Direktberichterstattung an den HVB	Frühzeitige Beteiligung	Bekanntgabe an MA
Kommune 1	●				
Kommune 2	○	65	○	○	○
Kommune 3	●				
Kommune 4	●				
Kommune 5	●				
Kommune 6	●				
Kommune 7	○	50	○	○	○
Kommune 8	●				
Kommune 9	●				
Kommune 10	○	5	●	○	●
Kommune 11	○	100	○	○	○
Kommune 12	●				
Kommune 13	○	10	○	○	○
Kommune 14	○	5	○	○	○
Kommune 15	●				
Kommune 16	●				
Kommune 17	○	100	●	●	●
Kommune 18	●				
Kommune 19	○	5	●	○	○
Kommune 20	○	5	○	○	○
Kommune 21	○	6	○	○	○
Kommune 22	●				
Kommune 23	○	38	○	○	○
Kommune 24	●				
Kommune 25	●				
Kommune 26	●				
Kommune 27	●				
Kommune 28	●				
Summe	11 (39 %)		8	10	9

Nur 11 der geprüften 28 Kommunen (39 %) hatten einen ISB benannt. Dabei betrug der prozentuale Stellenanteil des ISB, bezogen auf eine VzÄ, zwischen 5 % und 100 %. Nur acht konnten direkt an den HVB berichten. In zehn Kommunen wurde der ISB bei allen größeren

Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme frühzeitig beteiligt. Der ISB wurde nur bei neun Kommunen allen Mitarbeitern bekanntgegeben.

Der Landesrechnungshof bewertet es als bedenklich, dass 61 % der geprüften Kommunen keinen Informationssicherheitsbeauftragten hatten. Nicht nachvollziehbar ist weiterhin, dass die prozentualen Stellenanteile des ISB zwischen 5 und 100 % stark variieren.
Er erwartet von allen Kommunen die Benennung eines ISB, der direkt an den HVB berichten kann. Aufgrund der elementaren Bedeutung der Informationssicherheit für eine Behörde und ihre Geschäftsprozesse hält es der Landesrechnungshof für notwendig, dass die Kommunen unter Berücksichtigung der Hinweise des Landesrechnungshofes den prozentualen Stellenanteil eines vorhandenen ISB überprüfen.

5. Notfallhandbuch

5.1 Grundvoraussetzungen

Für die Aufrechterhaltung der Handlungsfähigkeit der Kommune, die Gewährleistung der Informationssicherheit und die schnellstmögliche Durchführung von relevanten Sofortmaßnahmen bei einer Notfallsituation (Hackerangriff) muss ein entsprechendes Notfallkonzept bzw. Notfallhandbuch mit den wichtigsten Informationen/Handlungsanweisungen erstellt werden.
In Notfällen müssen Behörden weiter auf Informationen zugreifen können, um einen Geschäftsprozess, ein IT-System oder eine Fachaufgabe wiederherstellen zu können. In Notfällen dient das Notfallhandbuch auch dazu weitergehenden Schaden von der Kommune abzuwenden.

Es sollte ein Notfallhandbuch erstellt werden, in dem die wichtigsten Informationen zu Rollen (Verantwortlichkeiten), Sofortmaßnahmen, Alarmierung und Eskalation sowie Kommunikations-, grundsätzlichen Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen enthalten sind. Zuständigkeiten und Befugnisse sollten zugewiesen, kommuniziert und im Notfallhandbuch festgehalten werden. Das Notfallhandbuch sollte allen Mitarbeitern bekanntgegeben werden und muss insbesondere im Notfall zugänglich, d. h. tatsächlich anwendungsbereit, sein. Alle wesentlichen Sofortmaßnahmen und Notfallpläne sollten in angemessener Weise regelmäßig und anlassbezogen getestet und geübt werden.

Der Landesrechnungshof hatte das Vorhandensein eines Notfallhandbuches mit den wichtigsten Informationen sowie die Zugänglichkeit und die Bekanntgabe sowie die Testung der Notfallpläne bei den Kommunen abgefragt.
Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen:

Tabelle 7 - Notfallhandbuch

	Notfallhandbuch	Rollen	Sofortmaßnahmen	Inform. zu Alarmierung	Inform. zu Geschäftsfortführungsplänen	Wiederherst.-/Wiederanlaufpläne	Zugänglichkeit im Notfall	Bekanntgabe	Testung der Notfallpläne
Kommune 1	●								
Kommune 2	●								
Kommune 3	●								
Kommune 4	●								
Kommune 5	○	○	○	○	○	●	○	●	●
Kommune 6	○	●	○	●	●	○	○	●	●
Kommune 7	○	○	○	●	●	●	●	●	●
Kommune 8	●								
Kommune 9	○	○	○	○	●	○	●	●	●
Kommune 10	○	○	○	○	○	○	○	●	○
Kommune 11	●								
Kommune 12	●								
Kommune 13	○	○	○	○	●	●	○	○	●
Kommune 14	○	○	○	○	●	○	●	●	●
Kommune 15	●								
Kommune 16	●								
Kommune 17	●								
Kommune 18	●								
Kommune 19	●								
Kommune 20	●								
Kommune 21	●								
Kommune 22	●								
Kommune 23	○	○	○	○	○	○	○	●	●
Kommune 24	●								
Kommune 25	●								
Kommune 26	○	○	○	○	●	○	○	●	○
Kommune 27	●								
Kommune 28	●								
Summe	9 (32 %)	8	9	7	3	6	6	1	2

Nur 9 von 28 Kommunen (32 %) hatten ein Notfallhandbuch.

Die Bekanntgabe erfolgte nur in einem Fall. Nur sechs Kommunen gaben an, dass das Notfallhandbuch auch im Notfall zugänglich ist. In zwei Kommunen wurde in den vergangenen

Jahren (davon zwei im Jahr 2022 und einer im Jahr 2018) ein Notfall erprobt. In zwei Kommunen wurde dafür ein Stromausfall simuliert und in einer ein Totalausfall.

Der Landesrechnungshof hält für äußerst bedenklich, dass 19 Kommunen (68%) keine Regelungen für einen Notfall geschaffen haben.
Er hält es für dringend notwendig, dass alle Kommunen ein gut zugängliches Notfallhandbuch vorhalten, um auch in Notfällen die Informationssicherheit aufrechterhalten und die Aufgaben der Kommune wahrnehmen zu können. Der Landesrechnungshof empfiehlt den Kommunen, die vorhandenen Notfallhandbücher entsprechend dem BSI-Standard zu überarbeiten und die noch fehlenden Regelungen zu ergänzen.
Alle Mitarbeiter sind darüber auch zu unterrichten. Der Landesrechnungshof regt an, dass die vorhandenen Notfallpläne in regelmäßigen Abständen auf ihre Praktikabilität getestet werden.

5.2 Weiterführende Voraussetzungen

Das Notfallhandbuch umfasst alle Dokumente, die eine angemessene Reaktion auf Krisen und Notfälle unterstützen sollen. Im Hinblick auf die Fortführung der Geschäftsprozesse sind insbesondere die Geschäftsfortführungspläne und Wiederanlaufpläne wichtig.[11]

Geschäftsfortführungspläne beschreiben die Handlungsschritte für die Wiederherstellung der Geschäftsprozesse nach Krisen und Notfällen, beispielsweise die Schritte zur Inbetriebnahme eines Ausweichrechenzentrums. Wiederanlaufpläne beschreiben die Handlungsschritte für die Wiederherstellung oder den Wiederanlauf wichtiger Ressourcen, die Priorität, mit der diese Schritte erfolgen müssen sowie die zugehörigen Verantwortlichkeiten. Bei Eintritt eines Notfalls ist es unabdingbar festzulegen, wie die betroffenen Prozesse fortgesetzt bzw. wieder anzulaufen haben. Voraussetzungen dafür sind die Kenntnis der Infrastruktur, von möglichen Schadpotentialen und das Festlegen der notwendigen Reaktion.

Der Landesrechnungshof hat unter diesen Gesichtspunkten die Notfallhandbücher geprüft. Von vier Kommunen wurde kein Notfallhandbuch vorgelegt, obwohl bei der Abfrage angegeben wurde, dass ein Notfallhandbuch vorhanden sei. Die Vorlage des Notfallhandbuches war Bestandteil des Prüfungskomplexes.

---

[11] Im Anhang des BSI-Standards 100-4 befinden sich Mustergliederungen für ein Notfallhandbuch und Geschäftsfortführungspläne.

Tabelle 8 - Prüfung der vorliegenden Notfallhandbücher nach festgelegten Kriterien

	Darstellung der bestehenden Infrastruktur	Klassifizierung möglicher Schadpotentiale	Reaktions-/Abschaltpläne	Alarmierungspläne	Geschäftsfortführungs-/Wiederanlaufpläne	**Gesamtbewertung durch den LRH[12]**
Kommune 5	🟢	🟢	🟢	🟢	🔴	🟢
Kommune 6*						
Kommune 7*						
Kommune 9	🟢	🟢	🔴	🟢	🔴	🟡
Kommune 10	🟢	🔴	🔴	🟢	🔴	🟡
Kommune 13*						🔴
Kommune 14	🔴	🟢	🔴	🟢	🔴	🟡
Kommune 23*						
Kommune 26	🔴	🔴	🟢	🟢	🔴	🟡

* wurden dem LRH nicht übergeben

Der Landesrechnungshof stellte bei der Durchsicht der vorgelegten Notfallhandbücher bei drei abgefragten Kriterien widersprüchliche Feststellungen, z. B. zu Alarmierungsplänen oder Wiederanlaufplänen fest.

Der Landesrechnungshof hält für bedenklich, dass die vorgelegten Notfallhandbüchern teilweise die notwendigen Voraussetzungen nicht erfüllten, um im Fall eines Notfalles beispielsweise die Fortführung des Dienstbetriebes sicher zu stellen.
Er empfiehlt, in die Notfallhandbücher die Klassifizierung möglicher Schadpotentiale, die Reaktions-/Abschaltpläne, die Alarmierungspläne sowie Geschäftsfortführungs- und Wiederanlaufpläne aufzunehmen.

---

[12] Bei der Gesamtbewertung handelt es sich um eine Einschätzung des LRH bezüglich des Umfanges, der Verständlichkeit und des Inhalts der Notfallhandbücher (Darstellung der bestehenden Infrastruktur, Klassifizierung möglicher Schadpotentiale, Reaktions-/Abschaltpläne, Geschäftsfortführungs-/Wiederanlaufpläne). Die grüne Bewertung konnte erteilt werden, wenn alle Kriterien bis auf eines erfüllt wurden. Beim Fehlen weiterer höchstens drei Voraussetzungen konnte das Notfallhandbuch vom LRH mit gelb bewertet werden. Bei mehr als vier fehlenden Kriterien bzw. bei fehlendem Notfallhandbuch wurde dieses durch den LRH mit rot bewertet.

6. Identitäts- und Berechtigungsmanagement

Ziel eines Identitäts- und Berechtigungsmanagements ist, dass Benutzer oder auch IT-Komponenten ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen und für die sie autorisiert sind. Mit Zugriff wird die Nutzung von Informationen oder Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen zu nutzen oder Transaktionen auszuführen.

Abhängig von ihren Rollen und Aufgaben erhalten Personen entsprechende Zutritts-, Zugangs- und Zugriffsberechtigungen. Auf diese Weise soll einerseits der Zugang zu Informationen gesteuert und kontrolliert werden. Andererseits soll es den Personen ermöglicht werden, bestimmte Aufgaben zu erledigen. Beispielsweise benötigen Personen oder Gruppen bestimmte Berechtigungen, um Anwendungen ausführen oder Informationen bearbeiten zu können.
Benutzerkennungen und Berechtigungen dürfen nur aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden. Bei personellen Veränderungen müssen die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt werden. Es muss festgelegt und dokumentiert werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden.

Ein fehlendes oder unvollständiges Identitäts- und Berechtigungsmanagement birgt u. a. die Gefahr des Diebstahles von Daten, Geräten, Datenträgern und Dokumenten sowie der Manipulation von Informationen.

Die Berechtigungsverwaltung sollte gewährleisten, dass Berechtigungen nach dem Minimalprinzip vergeben und regelmäßig überprüft werden. Administrative Tätigkeiten sollten so organisiert werden, dass dafür zwei Personen erforderlich sind. Die Aufgaben zwischen den einzelnen Administratoren sollten so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Administrationslücken entstehen. Die Vorgaben sollten insbesondere eigenmächtige Änderungen der Administratoren ausschließen, soweit diese über die ihnen explizit übertragenen Aufgaben hinausgehen und nicht notwendig sind, um einen Sicherheitsvorfall oder Störfall abzuwenden. Es sollten unterschiedliche Administrationsrollen für Teilaufgaben eingerichtet werden.

Administrative Berechtigungen erlauben es, umfassend auf vertrauliche Informationen wie Dokumente, Kommunikationsinhalte oder Datenbanken zuzugreifen. Administratoren können diese weitreichenden Berechtigungen nicht nur dazu benutzen, die ihnen übertragenen Aufgaben zu erfüllen, sondern auch für eigene Zwecke oder im Sinne von Dritten.

Die Schaffung sogenannter Super-User[13] birgt die Gefahr der Spionage, der Manipulation von Hard- oder Software und von Informationen. Darüber hinaus besteht die Gefahr der unberechtigten Nutzung oder Administration von Geräten und Systemen und des Missbrauches von Berechtigungen sowie der Nötigung, Erpressung oder Korruption.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob Zugriffberechtigungen vergeben wurden und ob es schriftliche Regelungen der Zugriffserforderlichkeit gibt. Außerdem wurden die Dokumentation der Zugriffsrechte und Regelungen zum Entzug von Zugriffsrechten sowie der Ausschluss von Super-Usern abgefragt. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen:

Tabelle 9 - Zugriffsberechtigungen

	Zugriffsberechtigungen vergeben	Schriftliche Regelung der Zugriffserforderlichkeit	Dokumentation der Zugriffsrechte	Regelungen für Entzug von Zugriffsrechten	Super-User ausgeschlossen
Kommune 1	○	●	●	○	○
Kommune 2	○	○	○	○	●
Kommune 3	○	●	○	○	○
Kommune 4	○	●	○	○	●
Kommune 5	○	●	○	○	○
Kommune 6	○	○	○	○	○
Kommune 7	○	●	○	○	○
Kommune 8	○	●	○	○	○
Kommune 9	○	●	●	○	●
Kommune 10	○	○	○	○	○
Kommune 11	○	●	○	○	●
Kommune 12	○	●	○	○	●
Kommune 13	○	●	●	●	○
Kommune 14	○	○	○	○	●
Kommune 15	○	○	○	○	●
Kommune 16	○	●	○	○	○
Kommune 17	●	●	●	●	●
Kommune 18	○	●	○	●	●
Kommune 19	○	●	○	○	●
Kommune 20	○	○	●	○	●
Kommune 21	○	●	○	○	○
Kommune 22	○	○	○	○	○

13 Superuser sind in der Lage , uneingeschränkte, potenziell nachtellige, systemweite Änderungen vorzunehmen.

	Zugriffsberechtigungen vergeben	Schriftliche Regelung der Zugriffserforderlichkeit	Dokumentation der Zugriffsrechte	Regelungen für Entzug von Zugriffsrechten	Super-User ausgeschlossen
Kommune 23	○	○	○	○	●
Kommune 24	○	○	○	○	○
Kommune 25	○	○	○	○	○
Kommune 26	○	●	○	○	●
Kommune 27	○	●	○	○	●
Kommune 28	○	○	○	○	○
Summe	27 (96 %)	11	23	25	14

In 27 Kommunen wurden Zugriffsberechtigungen vergeben. Von diesen 27 Kommunen hatten elf schriftlich geregelt, welche Berechtigungen im Einzelfall für die Erledigung der jeweiligen Aufgabe erforderlich sind.

In 23 Kommunen erfolgte eine Dokumentation der vergebenen Zugriffsrechte. Es gab in 25 Kommunen eine Regelung über den Entzug der Zugriffsberechtigung für Nutzer eines Verfahrens, die die Organisation verlassen oder aus anderen Gründen keine Zugangsberechtigungen mehr benötigen.

Die Hälfte der geprüften Kommunen, die Zugriffsberechtigungen vergeben hatten, verfügte über Administratoren, die alle Berechtigungen besaßen, bzw. Administratoren mit unbeschränkten Nutzungsrechten (Super-User), die sowohl administrative als auch sachbearbeitende Zugriffe in allen Bereichen des IT-Verfahrens ermöglichten.

Der Landesrechnungshof bewertet es positiv, dass 27 Kommunen über ein Identitäts- und Berechtigungsmanagement verfügen. Als besonders kritisch bewertet der Landesrechnungshof allerdings die mit 13 sehr hohe Anzahl an Super-Usern.

Der Landesrechnungshof hält es für erforderlich, dass jede Kommune über ein gut funktionierendes Identitäts- und Berechtigungsmanagement verfügt, welches sicherstellt, dass Berechtigungen nur aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden.

Der Landesrechnungshof empfiehlt eine kritische Überprüfung der vergebenen Administratorenrechte, um sogenannte Super-User zu vermeiden.

7. Schutz vor Schadprogrammen

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung des Benutzers schädliche Funktionen auf einem IT-System ausführen. Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen ausgeführt werden. Es muss ein Konzept erstellt werden, das beschreibt, welche IT-Systeme vor Schadprogrammen geschützt werden müssen.

Das Schutzkonzept soll die Anforderungen beschreiben, die zu erfüllen und umzusetzen sind, um eine Behörde effektiv gegen Schadprogramme zu schützen. Der Landesrechnungshof sieht die Erstellung eines Konzeptes für den Schutz vor Schadprogrammen als Pflicht der Kommune an, da das IT-Grundschutz-Kompendium des BSI dies eindeutig regelt. Nach der Auflistung der elementaren Gefährdungen besteht hierbei insbesondere die Gefahr des Missbrauches personenbezogener Daten.

Benutzer müssen regelmäßig über die Bedrohung durch Schadprogramme aufgeklärt werden. Sie müssen die grundlegenden Verhaltensregeln einhalten, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien, E-Mails, Webseiten usw. aus nicht vertrauenswürdigen Quellen sollten nicht geöffnet werden. Benutzern müssen entsprechende Ansprechpartner für den Fall eines Verdachtes auf eine Infektion mit einem Schadprogramm bekannt sein. Benutzer müssen sich an die ihnen benannten Ansprechpartner wenden, wenn der Verdacht auf eine Infektion mit einem Schadprogramm besteht.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob Schutzprogramme eingesetzt werden und ob es zum Schutz vor Schadprogrammen ein Konzept gibt. Darüber hinaus wurde die Aufklärung der Benutzer vor Schadprogrammen und die Benennung von Ansprechpartnern abgefragt. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen:

Tabelle 10 - Schutzprogramme

	Einsatz von Schutzprogram-men	Konzept für Schutz vor Schadprogram-men	Aufklärung der Benutzer vor Schadprogram-men	Benennung Ansprechpartner
Kommune 1	○	●	●	●
Kommune 2	○	○	○	○
Kommune 3	○	○	○	○
Kommune 4	○	●	○	○
Kommune 5	○	●	●	○
Kommune 6	○	○	●	○
Kommune 7	○	●	○	○
Kommune 8	○	○	○	○
Kommune 9	○	○	○	○
Kommune 10	○	○	○	○
Kommune 11	○	●	○	○
Kommune 12	○	●	○	○
Kommune 13	○	●	●	○
Kommune 14	○	○	●	○
Kommune 15	○	●	●	○
Kommune 16	○	●	○	○
Kommune 17	○	●	●	●
Kommune 18	○	●	●	●
Kommune 19	○	●	○	○
Kommune 20	○	●	○	○
Kommune 21	○	○	○	○
Kommune 22	○	●	○	○
Kommune 23	○	○	○	○
Kommune 24	○	●	●	○
Kommune 25	○	●	○	○
Kommune 26	○	●	○	○
Kommune 27	○	●	●	○
Kommune 28	○	●	●	○
Summe	28 (100 %)	9	17	25

Alle 28 Kommunen setzten in der gesamten Verwaltung flächendeckend Schutzprogramme vor Schadprogrammen ein. Von den geprüften 28 Kommunen verfügten aber nur neun über ein schriftliches Konzept für den Schutz des IT-Systems vor Schadprogrammen.

In 17 der 28 Kommunen erfolgte eine regelmäßige dokumentierte Aufklärung der Benutzer über die mögliche Bedrohung durch Schadprogramme. In 25 der 28 Kommunen wurden die Ansprechpartner für den Fall eines Verdachts auf eine Infektion mit Schadprogrammen bekanntgegeben.

Der Landessrechnungshof bewertet es positiv, dass alle Kommunen Schutzprogramme einsetzen. Er hält es allerdings für kritisch, dass nur in neun Kommunen ein schriftliches Konzept vorhanden ist.
Der Landesrechnungshof hält es für dringend notwendig, dass alle Kommunen entsprechend dem BSI-Grundschutz ein schriftliches Schutzkonzept vor Schadprogrammen erstellen, das beschreibt, welche IT-Systeme vor Schadprogrammen geschützt werden müssen.
Er hält es darüber hinaus für erforderlich, die Benutzer über Bedrohungen durch Schadprogramme aufzuklären und dies zu dokumentieren.

8. Deaktivierung und Deinstallation

Nach der Installation sollte überprüft werden, welche Komponenten der Firmware sowie des Betriebssystems und welche Anwendungen und weiteren Tools auf den Clients installiert und aktiviert sind. Nicht benötigte Module, Programme, Dienste, Aufgaben und Firmwarefunktionen (wie Fernwartung) sollten deaktiviert oder ganz deinstalliert werden. Nicht benötigte Benutzerkennungen sollten deaktiviert oder gelöscht werden.

Durch das Vorhandensein nicht mehr benötigter Programme oder Funktionen sowie Benutzerkennungen besteht die Gefahr der Offenlegung schützenswerter Informationen, des unbefugten Eindringens in IT-Systeme, der unberechtigten Nutzung oder Administration von Geräten und Systemen und des Datenverlustes.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob nicht benötigte Programme und Funktionen deinstalliert bzw. deaktiviert werden. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen:

Tabelle 11 - Deaktivierung und Deinstallation von Programmen und Funktionen

	Deinstallation/Deaktivierung nicht benötigter Programme	Deinstallation/ Deaktivierung nicht benötigter Funktionen
Kommune 1	○	○
Kommune 2	○	○
Kommune 3	●	○
Kommune 4	●	●
Kommune 5	○	○
Kommune 6	○	●
Kommune 7	○	○
Kommune 8	○	●
Kommune 9	○	○
Kommune 10	○	○
Kommune 11	●	●
Kommune 12	○	○
Kommune 13	●	●
Kommune 14	○	○
Kommune 15	○	○
Kommune 16	○	●
Kommune 17	●	●
Kommune 18	○	○
Kommune 19	○	○
Kommune 20	●	●
Kommune 21	●	●
Kommune 22	○	○
Kommune 23	○	○
Kommune 24	○	○
Kommune 25	○	○
Kommune 26	○	○
Kommune 27	○	●
Kommune 28	○	●
Summe	21 (75 %)	17 (61 %)

In 21 der geprüften Kommunen wurden nicht benötigte Programme konsequent deinstalliert bzw. deaktiviert. Nicht benötigte Funktionen wurden nur in 17 Kommunen konsequent deinstalliert bzw. deaktiviert.

Der Landesrechnungshof sieht es als kritisch an, wenn nicht in allen Kommunen nicht benötigte Programm und Funktionen deinstalliert bzw. deaktiviert werden, da dies zu einem Datenverlust führen kann.

Der Landesrechnungshof erwartet, dass die Kommunen nicht benötigte Programme und Funktionen konsequent deinstallieren bzw. deaktivieren.

9. Wartung von IT-Systemen - Umgang mit Updates

Es ist eine große Herausforderung, die in einer Institution (Behörde) eingesetzten Komponenten der IT korrekt und zeitnah zu aktualisieren. Ein fehlendes oder vernachlässigtes Änderungsmanagement führt daher schnell zu möglichen Angriffspunkten. Aufgabe des Patch- und Änderungsmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten. Für alle Organisationsbereiche müssen Zuständige für das Änderungsmanagement festgelegt werden.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob Updates zeitnah durchgeführt und dokumentiert werden. Im Weiteren wurde das Vorhandensein eines Änderungsmanagements abgefragt. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen:

Tabelle 12 - Updates und Änderungsmanagement

	Zeitnahe Aktualisierung (Updates)	Dokumentation der Updates	Änderungsmanagement
Kommune 1	○	●	●
Kommune 2	○	○	○
Kommune 3	○	○	○
Kommune 4	○	○	○
Kommune 5	○	○	○
Kommune 6	○	○	○
Kommune 7	○	○	○
Kommune 8	○	○	○
Kommune 9	○	●	○
Kommune 10	○	○	○
Kommune 11	○	○	○
Kommune 12	○	○	●
Kommune 13	○	●	●
Kommune 14	○	○	○
Kommune 15	○	○	○
Kommune 16	○	●	○
Kommune 17	○	●	●
Kommune 18	○	●	●
Kommune 19	○	●	●
Kommune 20	○	●	○
Kommune 21	○	○	○
Kommune 22	○	○	○
Kommune 23	○	●	○
Kommune 24	○	○	○
Kommune 25	○	●	○
Kommune 26	○	○	●
Kommune 27	○	●	○
Kommune 28	○	○	○
Summe	28 (100 %)	17 (61 %)	21 (75 %)

Alle 28 Kommunen kontrollierten regelmäßig, ob es Updates zu angewendeten Programmen der Kommune gab und spielten diese auch regelmäßig ein. Das Einspielen der Updates wurde in 17 Kommunen dokumentiert. Bei 21 der 28 geprüften Kommunen wurde geregelt, wer für die regelmäßige Information über relevante Updates verantwortlich ist.

Der Landesrechnungshof bewertet es positiv, dass alle geprüften Kommunen regelmäßig das Vorhandensein von Updates kontrollieren und diese einspielen. Als kritisch sieht er allerdings an, dass nur in 21 Kommunen ein Änderungsmanagement vorhanden ist.
Der Landesrechnungshof regt an, dass alle Kommunen festlegen, wer für die regelmäßige Information über relevante Updates verantwortlich ist.

10. Datensicherung - Backup

Wenn Daten verloren gehen und sie nicht vorher gesichert wurden, kann das existenzbedrohende Folgen für die Institution (Behörde) haben.
Durch regelmäßige Datensicherungen lassen sich Auswirkungen von Datenverlusten jedoch minimieren. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der Betrieb der Informationstechnik kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.
Die Kommune muss für jedes IT-System ein Verfahren festlegen, das definiert, welche Daten des IT-Systems wie gesichert werden.
Der IT-Betrieb muss ein Minimaldatensicherungskonzept auf Basis der festgelegten Verfahrensweise für die Datensicherung erstellen. Dieses muss festlegen, welche Anforderungen für die Datensicherung mindestens von der Kommune einzuhalten sind. Das Minimaldatensicherungskonzept muss mindestens eine kurze Beschreibung dazu enthalten,

- welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,
- wie die Datensicherungen erstellt und wiederhergestellt werden können,
- welche Parameter, z. B. Wiederanlaufzeiten, zu wählen sind sowie
- welche Hard- und Software eingesetzt wird.

Wird für Datensicherungsmaßnahmen kein angemessenes Minimaldatensicherungskonzept erstellt und befolgt, besteht die Gefahr, dass gesicherte Daten bei Bedarf nicht wiederhergestellt werden.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob sie über ein Minimaldatensicherungskonzept, Festlegungen zur Verfahrensweise, Offline-Backups[14] und eine getrennte Lagerung der Backups verfügen. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen.

---

[14] Unter Offline-Backups versteht man die Art der Sicherung von Daten, bei der man diese an einen Speicherort kopiert, auf den der Zugriff möglich ist, ohne dass der Computer mit dem Internet verbunden ist.

Tabelle 13 - Minimaldatensicherungskonzept und Offline-Backups

	Minimaldatensicherungskonzept	Festlegung zur Verfahrensweise	Offline-Backups	Getrennte Lagerung der Backups
Kommune 1	●	●	○	○
Kommune 2	●	○	○	○
Kommune 3	○	○	○	○
Kommune 4	○	○	○	○
Kommune 5	●	○	○	○
Kommune 6	○	○	○	○
Kommune 7	●	○	○	○
Kommune 8	○	○	●	●
Kommune 9	●	○	○	○
Kommune 10	○	○	○	○
Kommune 11	○	○	○	○
Kommune 12	●	●	○	○
Kommune 13	●	●	○	○
Kommune 14	○	○	○	○
Kommune 15	●	●	○	○
Kommune 16	●	○	○	○
Kommune 17	●	●	●	●
Kommune 18	●	●	○	○
Kommune 19	○	○	○	○
Kommune 20	●	○	○	●
Kommune 21	●	○	○	○
Kommune 22	○	●	○	●
Kommune 23	○	●	○	○
Kommune 24	○	○	○	○
Kommune 25	●	●	●	●
Kommune 26	○	○	○	○
Kommune 27	●	●	○	○
Kommune 28	○	○	○	○
Summe	13 (46 %)	18 (64 %)	25 (89 %)	23

Von den 28 geprüften Kommunen verfügten nur 13 über ein niedergeschriebenes Konzept zur Datensicherung (Minimaldatensicherungskonzept). Insgesamt hatten 18 Kommunen niedergeschriebene Festlegungen zur Verfahrensweise für die Datensicherung.

Von den 27 Kommunen, die Backups durchführen, führten 25 auch Offline-Backups durch. Die Lagerung dieser Offline-Backups erfolgte bei 23 Kommunen räumlich getrennt von den Online-Backups bzw. den Originaldatenträgern.

Der Landesrechnungshof sieht es als kritisch an, dass nur 46 % der Kommunen über ein Minimaldatensicherungskonzept verfügen.

Der Landesrechnungshof regt für die bei Bedarf notwendige Wiederherstellung gesicherter Daten an, dass alle Kommunen ein niedergeschriebenes Konzept zur Datensicherung erstellen und Datensicherungen danach durchführen. Die Datenträger von Datensicherungen sollten geeignet aufbewahrt werden, sodass diese vor unbefugtem Zugriff geschützt werden. Sie sollten räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden.

11. Infrastruktursicherheit - Serverräume

Der Zutritt zu IT-sicherheitsrelevanten Räumen, wie z. B. Rechenzentren, Serverräumen, muss kontrolliert werden. Zutrittsrechte müssen gemäß dem Grundschutzkompendium des BSI gesondert vergeben werden. Für im Rechenzentrum tätige Personen muss sichergestellt werden, dass diese keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten.
Alle Türen des Rechenzentrums müssen stets verschlossen gehalten werden.

Fehlen Zutrittskontrollen oder sind diese unzureichend, erhöht sich die Gefahr, dass unberechtigte Personen IT-sicherheitsrelevante Räumen betreten und dort fahrlässig, z. B. aufgrund mangelnder Fachkenntnisse, oder vorsätzlich Schaden anrichten. Angreifer können so z. B. schützenswerte Daten entwenden, Geräte stehlen oder Server manipulieren. Unzureichende Zutrittskontrollen wirken sich somit auf die Verfügbarkeit, Vertraulichkeit und die Integrität von Daten und IT-Komponenten aus.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob sie ihre Serverräume gegen Zutritt gesichert haben und die Berechtigung des Zutritts schriftlich geregelt hatten. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen.

Tabelle 14 - Zutrittssicherung der Serverräume

	Sicherung der Serverräume gegen Zutritt	Schriftliche Regelung
Kommune 1	○	●
Kommune 2	○	○
Kommune 3	○	○
Kommune 4	○	○
Kommune 5	○	○
Kommune 6	○	○
Kommune 7	○	○
Kommune 8	○	○
Kommune 9	○	○
Kommune 10	○	○
Kommune 11	○	●
Kommune 12	○	○
Kommune 13	○	○
Kommune 14	○	○
Kommune 15	○	●
Kommune 16	○	○
Kommune 17	●	
Kommune 18	○	●
Kommune 19	○	●
Kommune 20	○	○
Kommune 21	○	●
Kommune 22	○	●
Kommune 23	○	○
Kommune 24	○	○
Kommune 25	○	●
Kommune 26	○	●
Kommune 27	○	○
Kommune 28	○	●
	27 (96%)	17

In allen fast allen geprüften Kommunen (außer Kommune 17) wurden die Serverräume nach eigenen Angaben gegen unberechtigten Zutritt gesichert. 17 Kommunen hatten die Berechtigung des Zutritts schriftlich geregelt.

Der Landesrechnungshof bewertet es als kritisch, dass eine Kommune nach eigenen Angaben ihre Serverräume nicht gegen unberechtigten Zutritt gesichert hat.

Er erwartet, dass alle Kommunen ihre Serverräume gegen unberechtigten Zugriff sichern und die Zutrittsberechtigung schriftlich regeln.

12. Personal

12.1 Personalausstattung im IT-Bereich

Die IT durchdringt alle Bereiche der Kommune. Sie trägt zu fast jeder kommunalen Leistungserstellung unmittelbar oder mittelbar bei. Die Folgen eines Fehlers oder Ausfalls von Funktionen aufgrund einer Beeinträchtigung oder Manipulation der IT können gravierende Auswirkungen haben. Das Personal im IT-Bereich hat damit einen entscheidenden Anteil am Erfolg oder Misserfolg der Behörde. Sind die verantwortlichen Mitarbeiter nicht ausreichend qualifiziert, sensibilisiert und geschult, könnten sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so könnten Angriffe unerkannt bleiben.

Der Landesrechnungshof hat eine quantitative Abfrage der Personalausstattung im IT-Bereich der Kommunen durchgeführt, dessen Ergebnisse in der folgenden Tabelle dargestellt sind.

Tabelle 15 - Personelle Ausstattung, zu betreuende Systeme und deren Verhältnis

	Personelle Ausstattung	Anzahl der betreuten IT-Systeme	Verhältnis IT-Systeme je VZÄ (gesamt)	Eigenbetreute Systeme	Verhältnis IT-Systeme je VZÄ (eigene)	Fremdbetreute Systeme	Anzahl der Fachprogramme	Verhältnis Fachprogramme je VZÄ
Kommune 1	4	1.000	250	1.000	250	0	30	8
Kommune 2	9	2.976	331	749	83	2.227	204	23
Kommune 3	15	2.700	180	700	47	2.000	70	5
Kommune 4	3	920	307	920	307	0	27	9
Kommune 5	4,6	1.295	282	1.285	279	10	44	10
Kommune 6	4	1.000	250	1.000	250	0	30	8
Kommune 7	7,63	855	112	845	111	10	108	14
Kommune 8	8,75	2.300	263	2.290	262	10	170	19
Kommune 9	3	900	300	730	243	170	40	13
Kommune 10	15	8.000	533	8.000	533	0	100	7
Kommune 11	31,75	3.400	107	3.398	107	2	200	6
Kommune 12	5	835	167	825	165	10	70	14
Kommune 13	4	850	213	600	150	250	21	5
Kommune 14	8,5	2.826	332	2.736	322	90	44	5
Kommune 15	19,5	3.500	179	3.500	179	0	170	9
Kommune 16	12	9.600	800	9.600	800	0	208	17
Kommune 17	5	3.500	0	0	0	3.500	0	0
Kommune 18	4,9	600	122	600	122	0	40	8
Kommune 19	21	2.000	95	1.980	94	20	200	10
Kommune 20	11	2.000	182	2.000	182	0	65	6
Kommune 21	14	4.712	337	0	0	4.712	180	13
Kommune 22	7	600	86	570	81	30	80	11
Kommune 23	20	15.000	750	15.000	750	0	50	3
Kommune 24	5	750	150	500	100	250	52	10
Kommune 25	15	4.500	300	4.500	300	0	140	9
Kommune 26	4	1.020	255	1.020	255	0	44	11
Kommune 27	6,35	2.200	346	2.200	346	0	100	16
Kommune 28	7	700	100	700	100	0	80	11
Durchschnitt			262		229			10

In den 28 Kommunen war der Bereich der IT mit 3 bis 31,75 VzÄ ausgestattet. Die Mitarbeiter der IT betreuten zwischen 600 und 15.000 IT-Systeme wie beispielsweise PC, Notebook, Telefone usw. Viele Kommunen banden bei der Betreuung ihrer IT-Systeme zunehmend externe Dienstleister ein. Zwei Kommunen (Kommune 17 und Kommune 21) ließen alle IT-Systeme durch externe Dienstleister betreuen. Darüber hinaus wurden zwischen 21 bis 204 Fachprogramme durch das IT-Personal betreut. Eine Kommune (Kommune 17) ließ die Fachprogramme extern betreuen.

Der Landesrechnungshof verkennt nicht, dass die Kommunen im Rahmen ihrer Selbstverwaltung die IT-Bereiche eigenverantwortlich organisieren. Auffällig ist die heterogene personelle

Ausstattung der einzelnen Kommunen im Verhältnis zu den (fremd-)betreuten IT-Systemen oder den Fachanwendungen.

Aufgrund der elementaren Bedeutung der Informationssicherheit für eine Behörde und ihrer Geschäftsprozesse empfiehlt der Landesrechnungshof, dass die Kommunen regelmäßig Organisationsuntersuchungen zum Personalschlüssel im IT-Bereich durchführen und die Personalausstattung im IT-Bereich kritisch hinterfragen.

12.2 Vertretungsregelungen im IT-Bereich

Die Mitarbeiter einer Kommune, insbesondere im IT-Bereich, haben die wichtige Aufgabe, Informationssicherheit durchzusetzen. Dafür muss sichergestellt werden, dass es für alle wesentlichen Geschäftsprozesse und Aufgaben praktikable Vertretungsregelungen gibt.
Bei diesen Regelungen muss der Aufgabenumfang der vertretenden Person im Vorfeld klar definiert werden. Es muss sichergestellt werden, dass die vertretende Person über das dafür nötige Wissen verfügt.

In der öffentlichen Verwaltung darf nicht allein auf die Integrität der handelnden Bediensteten vertraut werden. Die IT muss unabhängig von den handelnden Personen durch eine wirksame Aufbau- und Ablauforganisation stetig und reibungslos funktionieren. Generalvertretungen sollten vermieden werden, denn sie können dazu führen, dass bestimmte Aufgaben nicht mehr oder nicht zeitnah wahrgenommen werden können.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob Vertretungen festgelegt wurden und diese dokumentiert sind. Es wurde auch erhoben, ob es Einzelvertretungen gibt und Generalvertretungen ausgeschlossen wurden. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen.

Tabelle 16 - Vertretungsregelungen im IT-Bereich

	Vertretungsregeln festgelegt	Vertretungsregeln dokumentiert	Einzelvertretung	Ausschluss von Generalvertretungen aller IT-Mitarbeiter
Kommune 1	○	●	●	●
Kommune 2	○	○	○	○
Kommune 3	○	○	○	○
Kommune 4	○	●	●	●
Kommune 5	○	○	○	●
Kommune 6	○	○	●	●
Kommune 7	○	○	○	○
Kommune 8	○	○	○	○
Kommune 9	○	●	○	●
Kommune 10	○	○	○	○
Kommune 11	○	○	○	○
Kommune 12	○	○	○	●
Kommune 13	○	○	●	●
Kommune 14	○	○	○	●
Kommune 15	○	○	○	●
Kommune 16	○	●	○	●
Kommune 17	●	●	●	●
Kommune 18	○	○	○	○
Kommune 19	●	●	●	●
Kommune 20	○	○	○	●
Kommune 21	○	○	○	○
Kommune 22	○	○	○	●
Kommune 23	○	○	○	●
Kommune 24	○	●	○	○
Kommune 25	○	○	○	○
Kommune 26	○	○	○	○
Kommune 27	○	○	○	○
Kommune 28	○	○	○	●
Summe	26 (93 %)	21	22	12

In 26 Kommunen waren die Vertretungsregelungen der IT-Mitarbeiter bindend festgelegt. In 21 Kommunen (81 % der 26 Kommunen) waren die Vertretungsregelungen niedergeschrieben. In 22 Kommunen gab es Einzelvertretungen. Nur in 12 der geprüften Kommunen wurde die Generalvertretungen für alle IT-Mitarbeiter untereinander ausgeschlossen.

Der Landesrechnungshof sieht es als kritisch an, dass bei 16 der geprüften Kommunen die Möglichkeit der Generalvertretung im IT-Bereich bestand, da durch die fehlende Zuordnung einer Aufgabe im Vertretungsfall ein Schaden entstehen kann.
Er regt an, dass die Kommunen für alle wesentlichen Geschäftsprozesse und Aufgaben praktikable Vertretungsregelungen erlassen. Von Generalvertretungen im IT-Bereich sollte abgesehen werden.

12.3 Fortbildung/Schulung und Sensibilisierung zur IT-Sicherheit

Mitarbeiter müssen regelmäßig geschult bzw. weitergebildet werden. In allen Bereichen muss sichergestellt werden, dass kein Mitarbeiter mit veraltetem Wissensstand arbeitet. Weiterhin sollte den Mitarbeitern während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.

Es ist wichtig, dass die Mitarbeiter die Sicherheitsziele kennen. Die Sicherheitsmaßnahmen sollen verständlich und jeder einzelne Mitarbeiter in der Lage sein, diese umzusetzen.
Die Voraussetzung dafür ist, dass ein aktives Sicherheitsbewusstsein aufgebaut und innerhalb der Institution gelebt wird. Mitarbeiter müssen für relevante Gefährdungen sensibilisiert sein und deren Auswirkungen auf die Institution kennen. Werden Benutzer und Administratoren nicht gezielt darin geschult und dafür sensibilisiert, Sicherheitsvorfälle zu erkennen und auf diese angemessen zu reagieren, können Sicherheitslücken unentdeckt bleiben und ausgenutzt werden. Falls Sicherheitsvorfälle zu spät oder gar nicht erkannt werden, können wirksame Gegenmaßnahmen nicht rechtzeitig ergriffen werden. Kleine Sicherheitslücken der Institution können zu kritischen Gefährdungen für die Integrität, Vertraulichkeit und Verfügbarkeit heranwachsen.

Der Landesrechnungshof hat bei den Kommunen abgefragt, ob die Mitarbeiter (IT-Mitarbeiter und sonstige Mitarbeiter) zur IT-Sicherheit regelmäßig geschult und belehrt werden. Die folgende Tabelle fasst die Selbstauskünfte der Kommunen zusammen.

Tabelle 17 - Schulung und Belehrung der Mitarbeiter zur IT-Sicherheit

	Regelm. Schulung IT-MA	Regelm. Schulung sonst. MA	Verpflichtende Schulung IT-MA	Belehrung aller Mitarbeiter
Kommune 1	●	○	●	○
Kommune 2	○	○	●	○
Kommune 3	○	○	●	○
Kommune 4	○	○	●	○
Kommune 5	●	●	●	●
Kommune 6	●	●	●	●
Kommune 7	●	○	●	○
Kommune 8	○	●	●	○
Kommune 9	○	●	●	○
Kommune 10	○	○	●	○
Kommune 11	○	○	●	○
Kommune 12	●	○	●	○
Kommune 13	○	○	●	○
Kommune 14	●	●	●	○
Kommune 15	○	●	●	●
Kommune 16	○	●	●	○
Kommune 17	●	●	●	●
Kommune 18	●	●	●	●
Kommune 19	●	●	●	○
Kommune 20	●	●	●	●
Kommune 21	○	○	○	○
Kommune 22	●	○	●	○
Kommune 23	○	●	●	○
Kommune 24	●	○	●	●
Kommune 25	●	●	●	○
Kommune 26	○	○	●	●
Kommune 27	○	○	●	○
Kommune 28	○	○	●	○
Summe	15 (54 %)	14 (50 %)	1 (4 %)	20 (71 %)

15 der 28 geprüften Kommunen boten für ihre IT-Mitarbeiter und 14 für die anderen Mitarbeiter spezielle Fortbildungen zum Thema IT-Sicherheit an. In 27 Kommunen bestand keine Verpflichtung der IT-Mitarbeiter zur mindestens jährlichen Fortbildung im Bereich der IT-Sicherheit. In 20 Kommunen wurden alle Mitarbeiter und Mitarbeiterinnen zur IT-Sicherheit belehrt.

Der Landesrechnungshof sieht es als besonders kritisch an, dass es im sehr risikobehafteten und schnelllebigen Bereich der IT-Sicherheit nur bei ca. der Hälfte der geprüften Kommunen regelmäßig Schulungen der IT-Mitarbeiter und der sonstigen Mitarbeiter gab. Besonders bedenklich ist, dass nur in einer Kommune die Verpflichtung zur jährlichen Fortbildung der IT-Mitarbeiter bestand. Auch die fehlende Belehrung aller Mitarbeiter zur IT-Sicherheit bei 8 Kommune ist als bedenklich einzustufen.

Der Landesrechnungshof hält es für dringend erforderlich, dass alle Mitarbeiter zum Thema IT-Sicherheit regelmäßig belehrt und geschult werden.

13. IT-Prüfung durch das Rechnungsprüfungsamt (RPA)

Die IT durchdringt alle Bereiche der Kommune. Sie trägt zu fast jeder kommunalen Leistungserstellung mittelbar oder unmittelbar bei.

Der IT-Bereich ist sehr risikobehaftet, hat ein hohes Schadenspotential und ist dementsprechend sehr schutzwürdig. Daher ist es nach Auffassung des Landesrechnungshofes empfehlenswert, wenn das RPA die IT-Sicherheit regelmäßig prüft.

Die Vorteile von IT-Prüfungen durch das RPA sind:

- Feststellung von Mängeln,
- rechtzeitige Behebung der Mängel,
- Minimierung von Risiken,
- Vorbeugen von Schäden und
- kurze Kommunikationswege innerhalb der Verwaltung.

Der Landesrechnungshof hatte im Rahmen seiner Online- Erhebungen auch um Übersendung von Prüfberichten der zuständigen RPÄ zum Thema IT-Sicherheit gebeten.
Lediglich ein RPA (Kommune 21) führte bisher eine Prüfung zu diesem Thema durch.

Der Landesrechnungshof empfiehlt den Kommunen, eine regelmäßige Prüfung der IT-Sicherheit durch das zuständige RPA zu veranlassen.

14. Interkommunale Zusammenarbeit

Die interkommunale Zusammenarbeit von Kommunen auf diesem Gebiet kann nach Auffassung des Landesrechnungshofes durch mögliche Spezialisierung zur Erhöhung der IT-Sicherheit beitragen.

Die interkommunale Zusammenarbeit bietet die Möglichkeit, die Aufgaben effektiver und kostengünstiger zu gestalten. Spezialisiertes Fachpersonal kann dabei für mehrere Kommunen eingesetzt werden; dadurch können Personalkosten gesenkt und effiziente Arbeitsstrukturen geschaffen werden. Für die komplexen Aufgaben im Bereich der IT-Sicherheit können Geschäftsprozesse einheitlich gestaltet werden. Risiken können so leichter identifiziert und abgestellt werden. Daher sollten die Kommunen auch bei der IT-Sicherheit prüfen, mit anderen Gebietskörperschaften zusammenzuarbeiten. Die Alternative der interkommunalen Zusammenarbeit sollte zukünftig im Rahmen von Wirtschaftlichkeitsbetrachtungen bei der Gewährleistung der IT-Sicherheit einbezogen werden.

Von den geprüften Kommunen haben 17 angegeben, interkommunal auf dem Gebiet der IT-Sicherheit zusammen zu arbeiten.

Der Landesrechnungshof empfiehlt den Kommunen, die Möglichkeit einer interkommunalen Zusammenarbeit im Bereich der IT-Sicherheit zu prüfen.

V. Schlussfolgerungen

Die Prüfung des Landesrechnungshofes hat vielschichtige Mängel im Bereich der IT-Sicherheit aufgezeigt. Keine der geprüften Kommunen hat sich zertifizieren oder testieren lassen, obwohl dies nach dem BSI-Standard die größtmögliche Sicherheit bietet, dass die Aufbau- und Ablauforganisation im Bereich IT-Sicherheit ordnungsgemäß ist.

Für einen guten Schutz nach dem BSI-Standard braucht es die Fokussierung auf den heutzutage so wichtigen Bereich der IT. HVB müssen ihre Verantwortung dafür erkennen, mögliche Risiken zu beherrschen und damit Schäden, die erhebliche finanzielle Auswirkungen haben können, zu vermeiden.

Es fehlte bisher bei der Mehrzahl der Kommunen an den durch das BSI als notwendig bestimmten Grundsatzpapieren wie Leitlinie, Sicherheitskonzept und Notfallhandbuch. Der Landesrechnungshof erwartet von den Kommunen, dass sie die festgestellten Mängel umgehend beseitigen und die fehlenden Grundsatzdokumente schaffen. Weiterhin empfiehlt er den Kommunen, vorhandene Regelungen in angemessenen Zeiträumen zu überprüfen. Er weist in diesem Zusammenhang darauf hin, dass unvollständige Regelungen, die gleichwohl Grundlage für zielgerichtetes Verwaltungshandeln sein können, in jedem Fall besser sind als keine Regelungen.

Der Landesrechnungshof erwartet von allen Kommunen die Benennung eines ISB mit einem für den Bereich der IT-Sicherheit angemessenen prozentualen Stellenanteil.

Der Landesrechnungshof empfiehlt neben der Prüfung einer interkommunalen Zusammenarbeit im Bereich der IT-Sicherheit auch eine regelmäßige Prüfung der IT-Sicherheit durch das zuständige RPA der Kommunen.

Der Landesrechnungshof hält es auch aus haftungsrechtlichen Gründen für dringend erforderlich, dass der HVB die notwendigen Maßnahmen veranlasst. Insbesondere sind umgehend die notwendigen dienstlichen Regelungen zu erlassen. Außerdem haben die Hauptverwaltungsbeamten dafür Sorge zu tragen, dass regelmäßig die dienstlichen Regelungen auf Wirksamkeit und Aktualität überprüft und deren Einhaltung kontrolliert werden. Die Ergebnisse der Überprüfung und Kontrollen sind zu dokumentieren.

Kay Barthel
Präsident

Florian Philipp
Mitglied des Landesrechnungshofes