Deutscher Städtetag

Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen

Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen

Herausgeber:
Deutscher Städtetag

Initiiert von:
Deutscher Landkreistag, Deutscher Städtetag, Deutscher Städte- und Gemeindebund gemeinsam mit der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister in Deutschland (VITAKO)

Bearbeitet von:
- Kommunale Praktiker im Rahmen des Forums der IT-Sicherheitsbeauftragten von Ländern und Kommunen (IT-SiBe-Forum)
- Gemeinsame Unterarbeitsgruppe der AG Cybersicherheit der Innenministerkonferenz und AG der infoSic des IT-Planungsrates

Hauptgeschäftsstelle:
Peter te Reh, Hauptreferent Deutscher Städtetag

Stand: November 2014

ISBN 978-3-88082-275-7

Leitung der Arbeitsgruppe:

Dr. Lutz Gollan, Behördlicher Informationssicherheitsbeauftragter der Behörde für Inneres und Sport, Hamburg,
Markus Albert, IT-Sicherheitsbeauftragter der Stadt Frankfurt,
Stefan Wojciechowski, IT-Sicherheitsbeauftragter, Landkreis Oberhavel

Mitglieder der Arbeitsgruppe:

Rico Anker, IT-Sicherheitsbeauftragter Landkreis Meißen
Michael Baumann, Kreis Viersen
Christina Borrmann, Behördliche Datenschutz- und IT-Sicherheitsbeauftragte der Stadt Hagen
Dr. Michael Bungert, IT-Sicherheitsmanagement, Landeshauptstadt München
Anton Graf, Landkreis Starnberg
Peter Herz, Kreis Mettmann,
Ilka Jentsch, Landkreis Hameln-Pyrmont
Bernd Lehmann, Kreisstadt Siegburg
Guido Maurer, Leiter des Fachdienstes IuK-Technik im Salzlandkreis
Steven Müller, IT-Leiter, Stadt Gera
Peter Nehl, Bereichsleiter Technik KID Magdeburg
Uwe Nikol, Sächsischen Anstalt für kommunale Datenverarbeitung SAKD
Dr. Danny Pannicke, VITAKO
Heino Reinartz, Städteregion Aachen
Volker Rombach, Citkomm, Iserlohn
Thorsten Roßkamp, Leiter Datenschutz & IT-Sicherheit KDO
Robert Schmid, verantwortlich für Betreuung Kunden der AKDB im Bereich IT-Sicherheit
Marc Schörshusen, IT-Sicherheitsbeauftragter, Landkreis Harburg
Thorsten Sitzmann, IT-Sicherheitsbeauftragter, Landeshauptstadt Saarbrücken
Karsten Stöck, Landkreis Hameln-Pyrmont
Joachim Wetzel, Stadtverwaltung Rees

Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen

Inhalt

I. Zusammenfassung ... 4
II. Einleitung ... 5
III. Begriffe ... 6
1. Informationssicherheit ... 6
2. Informationssicherheits-Organisation ... 6
3. Informationssicherheits-Managementsystem ... 6
IV. Ausgewählte Standards für ein ISMS ... 7
1. ISIS12 ... 7
2. ISO 27001 ... 8
3. IT-Grundschutz ... 8
4. Gegenüberstellung ... 9
V. Die Leitlinie des IT-Planungsrates ... 10
1. Formale Eigenschaften ... 10
2. Inhaltliche Diskussion ... 11
3. Fazit ... 12
VI. Einführung eines ISMS ... 13
1. Planung (Plan) ... 13
a) Informationssicherheitsleitlinie ... 14
b) Organisation der Informationssicherheit ... 15
c) Sicherheitskonzept ... 18
2. Umsetzung (Do) ... 18
a) Informationssicherheitsleitlinie (MUSTERTEXTE) ... 18
b) Übergreifende Aspekte der Informationssicherheit ... 22
c) Priorisierung und Abgrenzung kritischer Prozesse und Informationen ... 23
d) Sicherheitskonzepte ... 23
e) Beispiel zum IT-Grundschutzvorgehen ... 24
3. Prüfen und Überwachen (Check) ... 27
a) Behandlung von Sicherheitsvorfällen ... 27
b) Berichtswesen zur Informationssicherheit ... 27
4. Verbessern (Act) ... 28
VII. Fazit ... 29
VIII. Glossar und Abkürzungen ... 30

I. Zusammenfassung

Die Informationssicherheit in Kommunen ist eng mit deren Aufgabenerfüllung verbunden. Sie ist mittlerweile zum kritischen Schlüssel für verlässliches und nachvollziehbares Verwaltungshandeln geworden. Über die letzten Jahrzehnte hat dabei die Sicherheit der Informationstechnik (IT) einen größeren Stellenwert eingenommen. Die Komplexität der IT, der hohe Grad der Vernetzung und die Abhängigkeit der Verwaltung von IT-gestützten Verfahren verlangen nach einer Systematisierung und Organisation der Informationssicherheit – nach einem Informationssicherheits-Managementsystem (ISMS). Die Grundlage für ein solches ISMS ist ein Bekenntnis der Behördenleitung zur Informationssicherheit. Dieses Bekenntnis wird durch eine Informationssicherheitsleitlinie (ISLL) verbrieft.

Die Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit darf nicht als ein Projekt angesehen werden, das nach einem festen Terminplan durchgeführt wird und die Zielstellung hat, für mehr Informationssicherheit zu sorgen. Vielmehr handelt es sich um einen Prozess zur Feststellung des aktuellen Sicherheitsniveaus und daraus resultierenden Festlegungen zur Verbesserung. Die Einführung und Aufrechterhaltung dieses Sicherheitsprozesses ist Aufgabe der Behördenleitung. Sie muss den Sicherheitsprozess initiieren, steuern und auch überprüfen, ob die Sicherheitsziele in allen Bereichen umgesetzt werden. Nur wenn sie voll hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann diese Aufgabe erfolgreich wahrgenommen werden. Dafür ist eine systematische Herangehensweise an einen kontinuierlichen Überwachungs- und Optimierungsprozess nötig, mit dem sowohl die Technik als auch die Beschäftigten und weitere Einflussfaktoren berücksichtigt werden.

Die vorliegende Handreichung erläutert, wie ein kommunales Informationssicherheitsmanagement-System aufgebaut und unterhalten werden kann, und es beschreibt, wie eine dahinter stehende Informationssicherheitsleitlinie konzipiert und gestaltet werden kann.

Die Handreichung wurde von kommunalen Praktikern erstellt und orientiert sich zum einen an den in Deutschland verbreiteten Standards zur Informationssicherheit und den Vorgaben, die der IT-Planungsrat als verfassungsrechtlich legitimiertes Gremium über seine Leitlinie zur Informationssicherheit erstellt hat. Zum anderen hat sie die kommunalen Realitäten im Blick und nimmt Rücksicht auf die Besonderheiten der Gebietskörperschaften.

II. Einleitung

Bei der Einführung eines ISMS spielt die örtliche Informationssicherheitsleitlinie eine wesentliche Rolle. Die vorliegende Handreichung enthält eine Hilfestellung zur Erarbeitung einer solchen Informationssicherheitsleitlinie und Mustertexte (Kapitel VI), die den Hauptteil der Handreichung bildet. Kapitel III erörtert Begriffe der Informationssicherheit. Im Kapitel 0 werden drei Standards für Informationssicherheits-Managementsysteme vorgestellt, anschließend (Kapitel V) wird die Leitlinie des IT-Planungsrats dargestellt.

Die rechnergestützte Informationsverarbeitung stellt die öffentliche Verwaltung vor immer größere Herausforderungen. Über die Jahre hinweg haben sich die technischen Möglichkeiten, aber auch die Anforderungen an die Informationstechnik (IT) stetig weiter entwickelt. Während am Anfang nur eine durch wenige, spezialisierte Beschäftigte erfolgte Nutzung von IT-Systemen oder der Empfang und das Versenden von einfachen digitalen Nachrichten standen und die Gefahren als beherrschbar galten, wachsen die Bedrohungen für die Informationssicherheit in den Kommunalverwaltungen, die sich aus der immer komplexeren Vernetzung der Informationstechnik ergeben. Neben den elementaren Gefährdungen und technischem Versagen spielen dabei zunehmend Schwachstellen in IT-Systemen und Anwendungen, organisatorische Mängel, menschliche Fehlhandlungen, aber auch vorsätzliche Handlungen eine wesentliche Rolle.

Mit dem vorliegenden Dokument soll der Einstieg zum Aufbau eines ISMS in der Kommunalverwaltung unterstützt werden. Ein ISMS bietet Chancen, strukturiert die oben geschilderten Bedrohungen zu erkennen und ihnen angemessen zu begegnen. Das Dokument richtet sich in erster Linie an die Leitungsebene der Kommunalverwaltung und deren Informationsmanagement, durch die alle notwendigen Schritte zum Aufbau und Betrieb eines ISMS einzuleiten und im weiteren Verlauf zu überwachen sind.

Die Vorteile eines ISMS sind insbesondere:

- die organisierte und nachvollziehbare Abwehr von Bedrohungen der Informationssicherheit,
- die Sicherstellung gesetzlicher Anforderungen,
  u. a. bei ebenenübergreifenden Verfahren und bei der Anbindung an das Verbindungsnetz,
- die Optimierung der Kosten beim IT-Einsatz,
- die planbare Nutzung der IT für alle Verwaltungsabläufe,
- die Minimierung der Risiken für den Umgang mit Informationen,
- die Steigerung des Vertrauens in der Öffentlichkeit,
- die Integration in das übergeordnete Managementsystem.

III. Begriffe

1. Informationssicherheit

Informationssicherheit kann als der Zustand beschrieben werden, in dem die drei Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität von Informationen durch angemessene Maßnahmen gewährleistet sind. Dabei umfasst Informationssicherheit den Schutz von jeglichen Informationen (einschließlich personenbezogener Daten), jeglicher Art und Herkunft, unabhängig davon, ob sie auf Papier oder digital gespeichert sind.

Die beiden Begriffe Informationssicherheit und IT-Sicherheit werden sehr häufig auch synonym verwendet. In der vorliegenden Handreichung wird der Begriff Informationssicherheit verwendet, um zu verdeutlichen, dass elektronische wie auch „nicht-“elektronische Informationen schützenswert sind, die z.B. auch in Aktenform vorliegen können.

Vertraulichkeit	Integrität	Verfügbarkeit
Zugang zu Informationen nur für Befugte	**Unversehrtheit und Korrektheit von Informationen**	**Informationen bei Bedarf bereitstellen**
Es gibt klar festgelegte Berechtigungen, welche Personen auf welche Informationen (z.B. sensitive Daten, persönliche Informationen, Verschlusssachen) zugreifen dürfen.	Die Informationen sind vollständig und richtig; unautorisierte Änderungen gespeicherter oder übertragener Daten werden ausgeschlossen bzw. erkannt.	IT-Systeme, Anwendungen und Informationen sind verfügbar, wenn sie gebraucht werden.

Abbildung 1: Grundwerte der Informationssicherheit

2. Informationssicherheits-Organisation

Die Informationssicherheits-Organisation (IS-Organisation) ist eine speziell mit Aufgaben zur Informationssicherheit betraute Einheit, die aus bestehenden Organisationsstrukturen und festzulegenden Rollen und Aufgaben gebildet wird. Die IS-Organisation ist keine eigenständige Organisationseinheit. Sie setzt sich in der Regel aus Mitgliedern unterschiedlichster Organisationseinheiten zusammen. Die IS-Organisation sollte mindestens aus einer verantwortlichen Führungskraft der Behördenleitung sowie einer auf die Informationssicherheit fachlich spezialisierten Person bestehen.

3. Informationssicherheits-Managementsystem

Das Informationssicherheits-Managementsystem (ISMS) umfasst alle Anforderungen zum Umgang mit Informationen an die Behörde, ihre Organisationsstrukturen, ihre Geschäftsprozesse, die genutzte Informationstechnik sowie die Bedrohungsszenarien, die allesamt einem ständigen Wandel unterworfen sind. Ein angemessenes Sicherheitsniveau wird nur durch eine kontinuierliche, ganzheitliche Betrachtung des gesamten Informationsflusses sowie aller daran Beteiligter gewährleistet.

Die Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit darf nicht als ein Projekt angesehen werden, das nach einem festen Terminplan durchgeführt wird und die Zielstellung hat, für mehr Informationssicherheit zu sorgen. Vielmehr handelt es sich um einen Prozess zur Feststellung des aktuellen Sicherheitsniveaus und daraus resultierenden Festlegungen zur Verbesserung. Die Einführung und Aufrechterhaltung dieses Sicherheitsprozesses ist Aufgabe der Behördenleitung. Sie muss den Sicherheitsprozess initiieren, steuern und auch überprüfen, ob die Sicherheitsziele umgesetzt werden. Nur wenn sie hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann diese Aufgabe erfolgreich wahrgenommen werden. Dafür ist eine systematische Herangehensweise an einen kontinuierlichen Überwa-

chungs- und Optimierungsprozess nötig, mit dem sowohl die Technik als auch die Beschäftigten und weitere Einflussfaktoren berücksichtigt werden.

Das aus dem Qualitätsmanagement bekannte "PDCA-Modell" (engl. „Plan-Do-Check-Act“ – „Planen, Umsetzen, Prüfen, Verbessern“) hat sich in der Praxis für diesen kontinuierlichen Verbesserungsprozess bewährt.

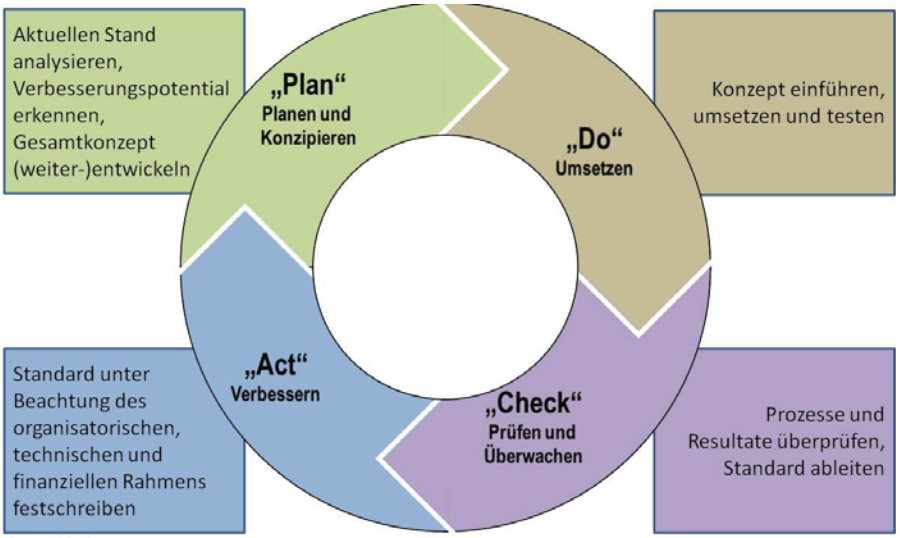

Abbildung 2: PDCA-Modell zur Einführung eines ISMS

IV. Ausgewählte Standards für ein ISMS

Ein ISMS soll für die Behörde ein angemessenes Niveau an Informationssicherheit bewirken, was durch eine Zertifizierung des ISMS bestätigt werden kann, jedoch nicht zwingend erfolgen muss. Aus diesem Grund werden nachfolgend drei wesentliche Standards zum Aufbau eines zertifizierbaren ISMS dargestellt. Die Aufstellung erhebt keinen Anspruch auf Vollständigkeit. Die für eine Zertifizierung notwendigen Schritte und möglichen Kosten werden ebenso nicht betrachtet. Die abschließende Gegenüberstellung soll die Vorzüge, aber auch die Unterschiede verdeutlichen. Auch wenn keine Zertifizierung angestrebt wird, bilden die genannten Standards die Grundlage zum erfolgreichen Betrieb eines ISMS.

1. ISIS12

ISIS12[1] steht für „Informations-SIcherheitsmanagementSystem in 12 Schritten". Mit ISIS12 sollen kleine und mittlere Unternehmen erreicht werden, die in der Regel keine fachspezifischen IT-Kenntnisse bzw. nicht ausreichend ausgebildetes Personal abstellen können. ISIS12 ist ein Dienstleistungsprodukt, das durch das Netzwerk Informationssicherheit für den Mittelstand[2] (NIM) entwickelt wurde.

Das aus dem IT-Grundschutz und der ISO 27001 abgeleitete und auf 12 Schritte reduzierte Modell hat den Anspruch, mit klaren Handlungsanweisungen und in allgemein verständlicher Sprache die Einführung eines ISMS in begrenztem Umfang zu ermöglichen. Die Dokumentation umfasst mit dem Handbuch zur effizienten Gestaltung der Informationssicherheit und dem ISIS12-Katalog ca. 170 Seiten. Der Katalog stellt eine Reduktion des IT-Grundschutzkataloges dar und beschränkt sich auf die typischerweise in mittelständischen Unternehmen vorzufindende, weitestgehend homogene IT-Infrastruktur. Somit werden nicht alle Aspekte der Informationssicher-

[1] ISIS12 – Informations-Sicherheitsmanagement System in 12 Schritten http://www.it-sicherheit-bayern.de/itsecurity/120678-669,1,0.html. ISIS12 unterliegt einer ggf. kostenpflichtigen Lizenz des Bayerischen IT-Clusters e.V., wird aber für Kommunalverwaltungen kostenlos zur Verfügung gestellt. Diese können das ISIS12-Handbuch und die Kataloge kostenlos bei sandra.wiesbeck@it-sec-cluster.de bestellen oder - falls Mitglied - im IT-SiBe-Forum herunterladen.

[2] Netzwerk Informationssicherheit im Mittelstand https://www.it-sicherheit-bayern.de/kompetenz/104782-587,1,0.html.

heit abschließend beantwortet. ISIS12 kann eine Grundlage für den Ausbau zu einem mit der ISO 27001 bzw. dem IT-Grundschutz konformen ISMS darstellen.

ISIS12 steht auch stellvertretend für weitere Vorgehensweisen zur Einführung eines ISMS, die in der Regel auf dem ISO 27001-Standard basieren.

2. ISO 27001

Ein international anerkannter Standard findet sich in der Norm ISO/IEC 27001[3], die unabhängig von der Organisationsart die Anforderungen an ein funktionierendes ISMS beschreibt. Dabei wird eine risikobasierte Herangehensweise gewählt. Hierbei bleiben in der Regel genügend Freiräume für die Umsetzung von Sicherheitsmaßnahmen mit Berücksichtigung von Wirtschaftlichkeitsaspekten. Risikobasierend bedeutet, dass nur jene Bestandteile der Informationsverarbeitung betrachtet und durch weiterführende Sicherheitsmaßnahmen berücksichtigt werden, die besonderen Risiken ausgesetzt sind.

In der Norm ISO/IEC 27002:2013 sind 14 Steuerungselemente mit insgesamt 114 Maßnahmen zusammengefasst, die auf der oben angegebenen Norm aufbauen und empfehlenden Charakter haben. Der Standard wurde speziell für die Industrie entwickelt und bietet höchstmögliche Flexibilität für die unterschiedlichsten Anwendungsbereiche. Ein einheitliches Mindestsicherheitsniveau wird durch die ISO 27001 jedoch nicht vorgegeben. Bei der Anwendung der ISO 27001 legt die anwendende Organisation das Sicherheitsniveau individuell unter Berücksichtigung bestehender und möglicher Risiken fest.

3. IT-Grundschutz

Einen weiteren Standard hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der Reihe 100[4] beschrieben. Dieser Standard ist Teil des IT-Grundschutzes, der derzeit auf der Norm ISO/IEC 27001:2005 aufbaut.

Der IT-Grundschutz wurde von der Verwaltung (nicht nur) für die Verwaltung entwickelt. Durch ein Ausleseverfahren konkret formulierter Sicherheitsmaßnahmen der „IT-Grundschutzkataloge“ kann ein einheitliches Mindestsicherheitsniveau etabliert werden und gleichzeitig erleichtern diese die gesteuerte Einführung und Umsetzungen. Darüber hinaus gehende Risiken sind zusätzlich zu betrachten.

Das IT-Grundschutz-Vorgehen wird meist als sehr aufwendig angesehen, da die IT-Grundschutzkataloge mittlerweile ca. 4.500 Seiten umfassen. Die Anzahl der Maßnahmen und der Umfang reduzieren sich jedoch, sobald bestimmte Aspekte, Systeme und Anwendungen nicht zum Einsatz kommen. Darüber hinaus stellt das BSI mit den Goldenen Regeln[5] eine vereinfachte Version der IT-Grundschutzkataloge zur Verfügung, um den leichten Einstieg in das Thema IT-Grundschutz zu ermöglichen.

In den IT-Grundschutzkatalogen wurden nicht alle möglichen technischen Systeme sowie Spezialanwendungen katalogisiert. Fehlende Objekte sind durch eine Risikoanalyse (vergleichbar zum ISO-Standard) zu berücksichtigen und ggf. durch eigene Bausteine abzusichern.

Die Leitlinie zur Informationssicherheit des IT-Planungsrates[6] vom März 2013 bezieht sich ausdrücklich auf den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Festlegung eines einheitlichen Mindestsicherheitsniveaus. Ebenso orientieren sich die

---

[3] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534; ISO/IEC 27001 unterliegt der Lizenz der Internationalen Organisation für Normung (ISO). Für die Hauptdokumente ISO/IEC 27001 und ISO/IEC 27002 fallen Gebühren in Höhe von etwa 300 Euro an.

[4] IT-Grundschutz-Standards kostenlos verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

[5] Goldene Regeln zu den IT-Grundschutzkatalogen https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/GoldeneRegeln.html.

[6] http://www.it-planungsrat.de/DE/Entscheidungen/2013/10_Sitzung/10_Sitzung_Entscheidungen.html?nn=1852114#doc3348826bodyText1.

unter Praktikern häufig diskutierten Beispiele ebenenübergreifender Verfahren der EU-Zahlstellen[7] und das Nationale Waffenregister[8] am IT-Grundschutzvorgehen.

4. Gegenüberstellung

Die oben dargestellten Standards sind hier tabellarisch gegenüber gestellt, um die Unterschiede und ggf. die Vorzüge zu verdeutlichen.

Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand[9]	International Standards Organisation[10]	Bundesamt für Sicherheit in der Informationstechnik[11]
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 170 Seiten	ca. 400 Seiten	ca. 4.500 Seiten
Detaillierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Umfang des Maßnahmenkataloges	ca. 400 Maßnahmen	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

Tabelle 1: Gegenüberstellung ausgewählter ISMS-Standards

7 http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32006R0885&from=DE.
8 Vgl. Günther Ennen, BSI; "IT-Grundschutz praktisch im Projekt Nationales Waffenregister"; http://www.infora-mc.de/Vortrag-Guenther-Ennen-810759.pdf.
9 http://www.it-sicherheit-bayern.de/isis/109790-669,1,0.html.
10 http://www.iso.org/iso/home/standards/management-standards/iso27001.html.
11 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

V. Die Leitlinie des IT-Planungsrates

Die Leitlinie des IT-Planungsrats trägt den Titel „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ und befasst sich laut Einleitung mit der Etablierung eines einheitlichen und einvernehmlichen Mindestsicherheitsniveaus zwischen Bund und Ländern unter Berücksichtigung des Grundsatzes der Wirtschaftlichkeit. Dieses Kapitel analysiert den formalen Aufbau. Zusätzlich enthält der zweite Abschnitt eine mehr inhaltliche Diskussion der Forderungen aus der Leitlinie.

1. Formale Eigenschaften

Die Leitlinie des IT-Planungsrates adressiert inhaltlich die Punkte einer Informationssicherheitsleitlinie (ISLL), allerdings nicht in der allgemein bekannten Struktur und Reihenfolge.

Die Leitlinie gilt nicht für eine abgeschlossene Behörde oder Organisation, sondern dient dem IT-Planungsrat, der für die Vereinbarung gemeinsamer Mindestsicherheitsstandards zwischen Bund und Ländern zuständig ist, als Mittel, um diese Standards zu etablieren. Die Einleitung gibt eine kurze und verständliche Einordnung der Themen elektronische Kommunikation und Informationssicherheit im Rahmen des Verwaltungshandelns. Die Sicherheitsziele werden in Kapitel 3 auf einem angemessenen Abstraktionsniveau dargestellt. Hier werden auch die Kernelemente der Umsetzungsstrategie festgelegt. Das Vorgehen beruht auf den fünf Säulen

- Informationssicherheitsmanagement
- Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung
- Einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren
- Gemeinsame Abwehr von IT-Angriffen (mittels eines VerwaltungsCERT[12]-Verbundes)
- Standardisierung und Produktsicherheit.

Diese fünf Säulen werden in Kapitel 3 ausführlicher dargestellt, wodurch im Wesentlichen der Umfang von 13 Seiten entsteht. Nach Kapitel 2 obliegt die Umsetzung der Vorgaben der Leitlinie dem Bund und den Ländern im jeweiligen Zuständigkeitsbereich. Der IT-Planungsrat setzt eine eigene Arbeitsgruppe ein, in die jedes Mitglied des Planungsrates einen Vertreter entsendet, der als zentraler Ansprechpartner für die Umsetzung der Leitlinie im jeweiligen Zuständigkeitsbereich fungiert. Die Arbeitsgruppe erarbeitet Vorschläge zur Weiterentwicklung der Leitlinie und verfasst einen jährlichen Bericht zur Erfolgskontrolle für den IT-Planungsrat. Damit werden auch die Verpflichtung zur Weiterentwicklung und die IS-Organisation in einer der speziellen Situation angemessenen Form adressiert.

Formal sind die Elemente einer ISLL vorhanden. Allerdings kann diese Leitlinie nicht als Blaupause für eine ISLL einer Kommunalverwaltung herangezogen werden, da sie nicht aus Sicht einer Behörde formuliert ist und wesentliche Elemente wie die konkrete Verpflichtung der Behördenleitung und eine möglichst direkte Ansprache der Beschäftigten nicht enthält und – aus Gründen der Zielrichtung – nicht enthalten kann.

Von Belang sind jedoch die Inhalte dieser Leitlinie, da sie zumindest im Falle einer direkten Anbindung an das Verbindungsnetz oder im Falle ebenenübergreifender Verfahren auch für Kommunalverwaltungen verbindlichen Charakter hat.

[12] CERT = Computer Emergency Response Team (“Computer-Notfall-Team”).

2. Inhaltliche Diskussion

Die Leitlinie fordert die Umsetzung der oben benannten fünf Säulen, die im Folgenden kurz inhaltlich diskutiert werden.

Informationssicherheitsmanagement

Es ist heute der als Stand der Technik akzeptierte Ansatz, ein für den jeweiligen Bereich passendes Informationssicherheitsmanagement einzuführen und sich des Werkzeugs eines ISMS zur Etablierung und zur Weiterentwicklung des Managements zu bedienen. Der weltweit akzeptierte Standard hierzu ist die Norm ISO 27001 mit seinen weiteren Dokumenten. Die Leitlinie formuliert im Abschnitt 3.1 als Ziel, ein am IT-Grundschutz des BSI orientiertes ISMS aufzubauen und zu betreiben, wobei ein ISMS nach ISO 27001 als erster Schritt genügt. ISO 27001 ist auch vom BSI als Rahmenwerk für ein ISMS in seiner Reihe 100-x[13] akzeptiert. Sowohl für kleine als auch für große und komplexe Organisationen ist es aus wirtschaftlichen und terminlichen Gründen anspruchsvoll, ein ISMS nach IT-Grundschutz flächendeckend aufzubauen und zu betreiben. Es steht außer Frage, dass die IT-Grundschutzbausteine für Risikobetrachtungen (zumindest für Standardrisiken) oder Herleitungen von (standardisierten) Sicherheitsmaßnahmen Beachtung finden sollten, dies muss allerdings in einer flexiblen und den konkreten Anforderungen entsprechenden Weise möglich sein. Entsprechend hat sich das BSI entschlossen, den IT-Grundschutz und damit das am IT-Grundschutz orientierte ISMS zu überarbeiten. Damit sollte es gelingen, die positiven Elemente der ISO 27001 mit dem IT-Grundschutz zu vereinen und damit einen Standard in Deutschland zu definieren, dessen Anwendung noch attraktiver ist.

Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung

Die Forderung nach einer geeigneten Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung ist zu begrüßen. Der Abschnitt 3.2 der Leitlinie für ein direkt am Verbindungsnetz angeschlossenes Netz enthält die Forderung, die BSI-Standards 100-x umzusetzen. Der Absatz mit dieser Forderung enthält den Nachsatz „Bei Anschluss eines Netzes sind die Teile des direkt angeschlossenen Netzes, für die diese Verpflichtung gilt, festzulegen. Sollten diese Standards auch im Rahmen eines angemessenen Stufenplans nicht umsetzbar sein, werden in den Anschlussbedingungen geeignete Maßnahmen festgelegt“. Diese Passage eröffnet möglicherweise Spielräume, die von der Kommunalverwaltung berücksichtigt werden sollten.[14]

Einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren

Nach Kapitel 2 der Leitlinie ist bei ebenenübergreifenden Verfahren die Umsetzung der Vorgaben der Leitlinie – auch über Bund und Länder hinaus – im notwendigen Umfang auf die jeweiligen Verfahrensbeteiligten auszudehnen. Damit gelten die Vorgaben in diesem Umfeld auch für die Kommunalverwaltung. Für die Verfahren selbst fordert die Leitlinie in Abschnitt 3.3, dass

- der Datenaustausch über die Verwaltungsgrenze über das Verbindungsnetz realisiert wird und
- bei der Planung und Anpassung der IT-Grundschutz nach BSI anzuwenden ist.

Diese Forderungen ergeben bei sinnvoller Anwendung des IT-Grundschutzes wie oben beschrieben Sinn, können aber bei konservativer Auslegung des IT-Grundschutzes zu erheblichen Mehraufwänden führen, wenn nicht bereits flächendeckend der IT-Grundschutz realisiert wurde.

[13] Reihe der IT-Grundschutz-Standards: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

[14] Allerdings sind die Regeln für den Übergang zum Verbindungsnetz nach IT-Netzgesetz noch nicht abschließend diskutiert; es liegt lediglich ein Vorschlag des Bundes vom September 2014 vor.

Gemeinsame Abwehr von IT-Angriffen (mittels eines VerwaltungsCERT-Verbundes)

Die Einführung eines VerwaltungsCERT-Verbundes von Bund und Ländern ist zu begrüßen. Der Kommunalverwaltung sollte ein geeigneter Zugang zu den CERTs der Länder gewährt werden, damit der Verbund zu einem umfassenden und schnellen Informationsfluss führt.

Standardisierung und Produktsicherheit

Das in Abschnitt 3.5 geäußerte Ziel

„Zur Vereinfachung und Stärkung ebenenübergreifender Verfahren sollen gemeinsame Basiskomponenten angeboten werden, die Grundfunktionen wie z. B. Verschlüsselung bereitstellen. Hierzu sind die Durchführung einer Bedarfsermittlung und die gemeinsame Festlegung von Mindestsicherheitsanforderungen für sichere Produkte, Systeme und Verfahren notwendig mit dem Ziel, gemeinsame Basiskomponenten einzusetzen."

ist nachvollziehbar und sinnvoll. Aus Sicht der Kommunalverwaltung muss aber sichergestellt sein, dass eine Beteiligung bei der Bedarfsermittlung und Festlegung von Mindestsicherheitsanforderungen erfolgt, um unnötige Zusatzinvestitionen zu vermeiden.

3. Fazit

Die fünf Säulen der Leitlinie des IT-Planungsrates sind vom Ansatz her sinnvoll und entsprechen den heute üblichen Vorgehensweisen. Der BSI-Standard zum Aufbau eines ISMS wurde auf der Basis der ISO 27001 entwickelt, erzeugt jedoch in der Umsetzung größeren Aufwand. Kommunen, die erst beginnen, ein verbindliches Rahmenwerk für ein ISMS zu entwickeln, sollten daher die ISO 27001 in der aktuellen Version anwenden – mit der Option, BSI-Grundschutz zu realisieren. Die Anwendung von IT-Grundschutz hat aufgrund des einheitlichen Ansatzes für ein Mindestsicherheitsniveau Vorteile.

VI. Einführung eines ISMS

Dieses Kapitel ist eine Hilfestellung für die Einführung eines ISMS. Konkret werden die wesentlichen Handlungsschritte mit den Vier-Phasen des PDCA-Modells aus strategischer Sicht dargestellt.

Auf die drei Säulen des Regelwerkes zur Informationssicherheit (Informationssicherheitsleitlinie, Organisation der Informationssicherheit und Sicherheitskonzept) wird jeweils gesondert eingegangen. Das Zusammenspiel dieser Werkzeuge ist existenziell für ein funktionierendes ISMS.

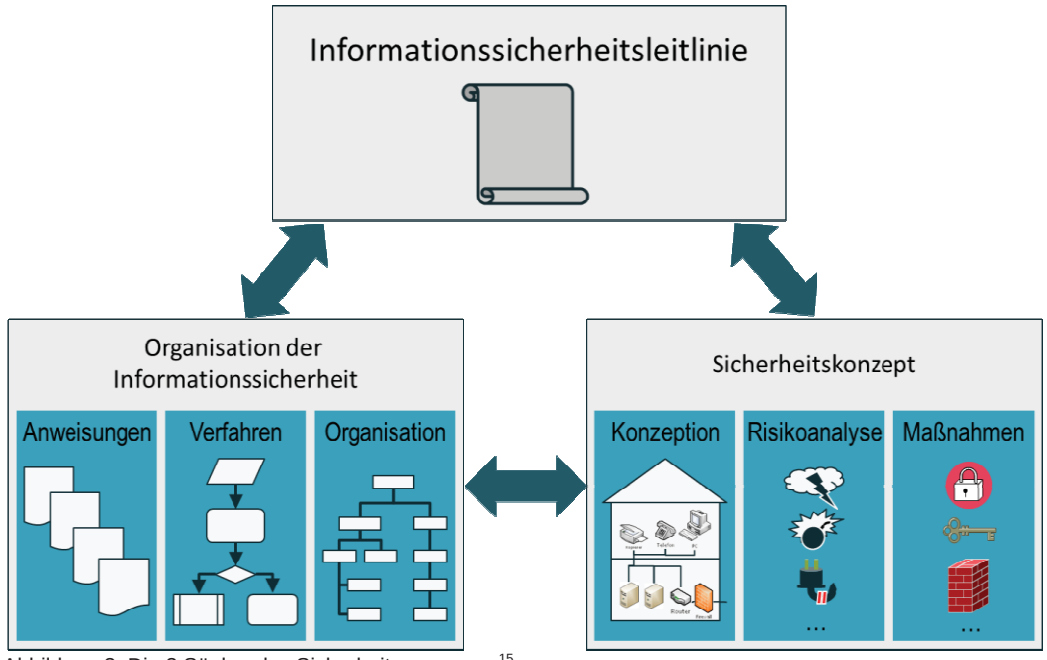

Abbildung 3: Die 3 Säulen des Sicherheitsprozesses[15]

1. Planung (Plan)

Bei der Festlegung der Sicherheitsziele und der Sicherheitsstrategie ist zu berücksichtigen, dass der Aufwand des Sicherheitsprozesses von der Größe der Behörde, der Ausgangssituation und den Sicherheitsanforderungen abhängt.

In einer sehr großen Behörde mit mehreren Hierarchieebenen sollte die für den Sicherheitsprozess notwendige Steuerung und Auditierung formal festgelegt werden. Dazu zählen insbesondere:

- welche Prüfungs- und Überwachungsmaßnahmen zu berücksichtigen sind,
- wer an wen zu welchen Themen der Informationssicherheit berichtet,
- wer Entscheidungsvorlagen zu erstellen hat und
- wann die Behördenleitung über den Sicherheitsprozess berät.

Dagegen kann in kleinen Verwaltungen der Erfolg des Sicherheitsprozesses kritisch begleitet werden, indem regelmäßige Gespräche zwischen der Behördenleitung und der eigenen IT bzw. dem IT-Verantwortlichen stattfinden. Inhalt der Gespräche sollten unter anderem festgestellte Probleme, entstandene Kosten und technische Weiterentwicklungen sein.

Der Basisaufwand für ein ISMS wird so gestaltet, dass dieser sinnvoll und tragbar erscheint. IT-Grundschutz kann hierbei als Option gesehen werden. ISO 27001 genügt bei der erstmaligen Einführung eines skalierbaren ISMS. Ein Einstieg könnte über ISIS12 gesucht werden.

[15] Vgl. BSI: BSI-Standard 100-1, Managementsysteme für Informationssicherheit (ISMS), 2008, Seite 14: Abbildung 4 – Umsetzung der Sicherheitsstrategie mit Hilfe des Sicherheitskonzeptes und einer Informationssicherheitsorganisation.

Zur Steuerung und Umsetzung sollte ein IT-Sicherheitsbeauftragter[16] benannt werden. Sofern die Ernennung eines IT-Sicherheitsbeauftragten nicht in Frage kommt, kann das ISMS auch ohne diesen eingeführt werden. Hierbei ist zu beachten, dass die Leitung eines IS-Management-Teams durch entsprechenden Sachverstand gewährleistet werden muss und die Behördenleitung, als für die Sicherheit verantwortliche Stelle, stärker einbezogen wird. Die Funktion des IT-Sicherheitsbeauftragten kann auch an einen externen Dienstleister übertragen werden. In jedem Falle müssen die Rollen und Verantwortlichkeiten klar definiert sein.

Das BSI hat im Jahresbericht 2010[17] eine Roadmap und die Verantwortlichkeiten für ein ISMS grafisch dargestellt. Dieser grobe Plan kann ggf. als Vorlage für die Einführung eines ISMS dienen und ist kompatibel mit dem IT-Grundschutz-Vorgehen.

Die Behördenleitung muss jedoch individuell festlegen, konkretisieren und verantworten, in welcher Ausprägung der Sicherheitsprozess als angemessen gelten kann, unter Berücksichtigung der Gesetze, Richtlinien und betrieblichen Vereinbarungen. Festzulegen sind,

- die Sicherheitsziele und Rahmenbedingungen der eigenen Behörde,
- der Ablauf zur Behandlung von Risiken,
- die Verantwortungen und Zuständigkeiten,
- die Durchführung von Schulungen und Sensibilisierungen,
- die Planung von Überprüfungen, Notfallübungen und Reserven,
- der Prozess möglicher Veränderungen.

a) Informationssicherheitsleitlinie

Die behördliche Informationssicherheitsleitlinie[18] (ISLL) stellt die formale Grundlage zur Einführung eines ISMS dar. Sie wird von der Behördenleitung vorgegeben und sollte neben den Sicherheitszielen, also den Erwartungen und Anforderungen an die Beteiligten, auch den Umgang mit möglichen Risiken und die Verantwortlichkeiten vorgeben.

Die ISLL sollte unter Berücksichtigung der beiden anderen Säulen (Organisation und Sicherheitskonzept) des Sicherheitsprozesses erstellt werden. Sie ist Teil des Sicherheitsprozesses und unterliegt einem Lebenszyklus, wobei sie regelmäßig aktualisiert bzw. fortgeschrieben werden sollte.

Eine ISLL sollte möglichst prägnant und übersichtlich die von ISO und BSI vorgegebenen Inhalte adressieren, d.h. die einzelnen Punkte sollten in eben dieser Form behandelt werden. Mustertexte befinden sich unter VI. 2a.

(1) Stellenwert der Informationssicherheit und zu schützende Objekte

Eine kurze Darstellung, dass heutiges Verwaltungshandeln mehr und mehr auf IT-Diensten beruht und auf diese aufbaut. Die von der Behörde zu erhebenden und zu verarbeitenden Informationen werden zunehmend auf IT-Systemen verarbeitet und gespeichert. Diese Informationen sind die wesentlichen zu schützenden Objekte der modernen Verwaltung.

(2) Bezug der Informationssicherheit zu den Geschäftszielen oder Aufgaben der Institution

In der ISLL wird dargestellt, wie sich die Informationssicherheit und die behördenspezifischen Organisationsziele wechselseitig beeinflussen.

---

[16] IT-Sicherheitsbeauftragte/r werden auch als "Beauftragte/r für die Informationssicherheit" oder "Informationssicherheitsbeauftragte/r" bezeichnet.

[17] BSI Jahresbericht 2010, Seite 25 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Jahresberichte/BSI-Jahresbericht_2010_pdf.html [02.08.2011].

[18] Informationssicherheitsleitlinien wurden in der Vergangenheit auch unter der Bezeichnung "IT-Sicherheitsleitlinie" erlassen.

(3) Sicherheitsziele

In diesem Abschnitt können Sicherheitsziele aufgelistet werden, die über das allgemeine Ziel, ein geeignetes Niveau der Informationssicherheit zu erreichen, hinaus konkreter gefasst werden sollen (z. B. Vertraulichkeit, Integrität, Verfügbarkeit). Da es sich um eine ISLL handelt, sollte eine zu große Detailtiefe vermieden werden. Es kann auch ausreichen aufzuzeigen, wie und unter welchen Rahmenbedingungen die Organisation die eigenen Ziele herleiten will.

(4) Kernelemente der Sicherheitsstrategie

Hier wird aufgezeigt, wie die Organisation die Ziele erreichen will. Auch dies sollte auf einem hohen Abstraktionsniveau erfolgen. Zum Beispiel könnte hier aufgeführt werden, dass die Organisation ein Sicherheitsmanagement mit einem ISMS einführt und Sicherheitsrichtlinien erlässt.

(5) Verpflichtung zur Umsetzung der ISLL

Wichtig ist, dass die Behördenleitung klar formuliert, dass sie hinter den Sicherheitszielen steht und unter Beachtung der Kompetenzen die benötigten Ressourcen zur Verfügung stellt.

(6) IS-Organisation

Die ISLL sollte den Rahmen aufzeigen, wie das Thema Informationssicherheit in der Organisation verankert wird. Die Gesamtverantwortung für die Informationssicherheit liegt bei der Behördenleitung. Es kann zielführend sein, die Zuständigkeit für die Informationssicherheit zu delegieren. Hierfür kommen das IS-Management-Team und/oder der IT-Sicherheitsbeauftragte in Betracht. Die Ausgestaltung der IS-Organisation hängt von der Größe und Komplexität der Behörde ab. Unter diesem Punkt kann auch auf die Verantwortung der Führungskräfte und aller Beschäftigten für das Erreichen der Sicherheitsziele explizit verwiesen werden. Auch disziplinarische Folgen können aufgeführt werden.

(7) Verpflichtung zur kontinuierlichen Verbesserung

Wie in Punkt 5 braucht es eine klar formulierte Aussage zur Fortentwicklung der Strategie zur Informationssicherheit.

(8) Inkraftsetzung

Hier erfolgt eine Darstellung, wie die ISLL in Kraft gesetzt wird.

b) Organisation der Informationssicherheit

Die Umsetzung der Informationssicherheit kann nicht allein durch die für die IT zuständige Organisationseinheit erfolgen. Es handelt sich vielmehr um eine interdisziplinäre Aufgabe, bei der neben der IT auch weitere Bereiche, z.B. Gebäudemanagement (z.B. Zutrittsregelungen, Notstrom), Organisation (z.B. Zuständigkeiten, Rechte), aber auch die Technik (z.B. Telekommunikation, Arbeitsplatzrechner) einzubeziehen sind.

Der Aufbau einer geeigneten Organisationsstruktur und eines Regelwerkes für das Sicherheitsmanagement hat wesentlichen Einfluss auf die Erreichung der gesteckten Sicherheitsziele. Praktisch ist es nicht möglich, eine für jede Behörde unmittelbar anwendbare Organisationsstruktur anzugeben. Hinzu kommt, dass regelmäßig Anpassungen an spezifische Gegebenheiten erforderlich sein können.

Abhängig von der Größe der Behörde sollte ein unabhängiger IT-Sicherheitsbeauftragter bzw. ein IS-Management-Team benannt werden. Mitglieder des IS-Management-Teams können unter anderem Verantwortliche der IT, des Gebäudemanagements und der Organisation sein. Bei Bedarf sollten der Beauftragte für den Datenschutz und ein Vertreter des Personalrates hinzugezogen werden.

Das IS-Management-Team sollte sich unter dem Vorsitz des IT-Sicherheitsbeauftragten regelmäßig mit dem Ziel der kontinuierlichen Verbesserung der Informationssicherheit treffen. Weitere

Aufgaben (beispielhaft), die durch den IT-Sicherheitsbeauftragten bzw. das IS-Management-Team wahrgenommen werden sollten, sind:

- Einbindung und Steuerung des Sicherheitsprozesses,
- Entwickeln der Sicherheitsziele und Sicherheitsstrategie für die ISLL mit der Behördenleitung,
- Überprüfen der Umsetzung der ISLL,
- Festlegen von Schutzbedarfskategorien für Prozesse bzw. Informationen zur Verabschiedung durch die Behördenleitung,
- Entwickeln von Sicherheitskonzepten,
- Überprüfen der im Sicherheitskonzept geplanten Sicherheitsmaßnahmen auf Vollständigkeit, Funktionsfähigkeit und Wirksamkeit,
- Unterstützen der Wirtschaftlichkeitsbetrachtungen der Sicherheitsmaßnahmen,
- Entwickeln von Konzepten von Schulungen und Sensibilisierungen zur Informationssicherheit,
- Beraten und Unterrichten der Behördenleitung zu Themen der Informationssicherheit,
- Fortschreiben der Sicherheitsleitlinie und der Sicherheitskonzepte.

Um einen Interessenkonflikt und eine reine Selbstkontrolle zu vermeiden, sollte die Aufgabe des IT-Sicherheitsbeauftragten mit Bedacht vergeben werden, da auch Interessenkonflikte Risiken für die Informationssicherheit darstellen. Die folgende Tabelle gibt Hinweise, inwieweit die Aufgabe des IT-Sicherheitsbeauftragten mit anderen Rollen kombiniert werden kann.

Rolle / Aufgabenbereich[19]	Beschreibung	Ernennung als IT-Sicherheitsbeauftragten
Anwendungsverantwortlicher	Ist zuständig für den reibungslosen Betrieb.	nicht zu empfehlen
Datenschutzbeauftragter	Ist verantwortlich für den gesetzeskonformen Umgang mit personenbezogenen Daten.[20]	viele Überschneidungen, unter Umständen möglich, wenn ausreichend Kapazitäten vorhanden
Geheimschutzbeauftragter	Hat für die Durchführung der VS-Anweisung zu sorgen und die Behörde in allen Fragen des Geheimschutzes zu beraten.[21]	wenige Überschneidungen auf kommunaler Ebene, unter Umständen möglich
IT-Betrieb/Administrator	Betreibt, überwacht und wartet IT-Systeme.	nicht zu empfehlen
IT-Leiter	Ist verantwortlich für die Organisation der IT und deren Betrieb.	nicht zu empfehlen, da u.a. verantwortlich für die Verfügbarkeit der Anwendungen.
Personalrat	Vertritt die Interessen der Beschäftigten gegenüber der Behördenleitung.	nicht möglich
Revision/Rechnungsprüfungsamt	Kontrolliert, ob die geplanten Maßnahmen wirtschaftlich und sparsam umgesetzt wurden, um den ordnungsgemäßen und sicheren Einsatz zu gewährleisten.[22]	Interessenkonflikt zwischen Prüf- und Beratungsauftrag, unter Umständen möglich
Rechtsabteilung	Liefert Hinweise, ob Sicherheitsmaßnahmen rechtlich umgesetzt werden dürfen, da die Komplexität von Gesetzen um das Thema Informationssicherheit von IT-Spezialisten oft schwer zu analysieren ist.	möglich, wenn ausreichend technisches Verständnis und eine Unabhängigkeit in der Organisation gewährleistet werden kann.

Tabelle 2: Vereinbarkeit des IT-Sicherheitsbeauftragten

Erfahrungen aus den Sicherheitsvorgaben zu den EU-Zahlstellen und dem Nationalen Waffenregister (NWR) haben gezeigt, dass einzelne Sicherheitsvorgaben Einfluss auf behördenübergreifende Prozesse haben können. Es ist sinnvoll, die daran Beteiligten an den Planungen zu beteiligen.

Informationssicherheit kann nicht allein durch den Betreiber der Technik sichergestellt werden. Technische Maßnahmen allein zeigen kaum Wirkung, wenn diese nicht genutzt oder womöglich umgangen werden können. Es müssen beispielsweise Angriffe auf das Behördennetzwerk, Datendiebstähle und auch menschliches Fehlverhalten bedacht und verhindert werden.

[19] Die Tabelle listet die Rollen in alphabetischer Reihenfolge und stellt keine Wertung dar.
[20] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile Seite 28 ff.
[21] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/VSA.pdf?__blob=publicationFile.
[22] https://www.bundesrechnungshof.de/de/veroeffentlichungen/broschueren/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik/at_download/file; http://www.diir.de/fachwissen/revisionshandbuch-marisk/.

c) Sicherheitskonzept

Wesentlicher Bestandteil der Planung ist die Erstellung eines Sicherheitskonzeptes, das den IST-Stand der maßgeblichen Geschäftsprozesse einer Behörde und die diese unterstützende Infrastruktur, IT-Systeme und Anwendungen abbildet. Hierbei sind die jeweiligen Schutzbedarfe und die bereits vorhandenen Sicherheitsmaßnahmen zu dokumentieren. Die fehlenden Maßnahmen und deren Umsetzung sind in einem weiteren Schritt (DO) zu planen. Dazu zählen insbesondere auch die Sicherheitsmaßnahmen, die aus einer Risikoanalyse heraus entwickelt wurden.

2. Umsetzung (Do)

a) Informationssicherheitsleitlinie (MUSTERTEXTE)

Nachfolgend wird auf den Aufbau und den Inhalt einer Informationssicherheitsleitlinie (ISLL) speziell eingegangen, wobei der Text als Vorlage für die Erstellung einer behördenspezifischen ISLL genutzt werden kann.

In eckigen Klammern dargestellter Text ist durch eigene Angaben der Behörde zu ersetzen.

Die nachfolgend angegebenen Textvorschläge können nach eigenem Ermessen und in Abhängigkeit der Größe der Behörde ausgewählt werden. Die Einleitung zu einem Textbaustein und der nicht zutreffende Textbaustein sind zu entfernen.

Die Definition der Schutzbedarfskategorien wurde in einer Anlage dargestellt.

(1) Stellenwert der Informationssicherheit und zu schützenden Objekten

Die [Name der Behörde] besitzt eine enorme Aufgabenvielfalt – von der Daseinsfürsorge bis zu Dienstleistungen für Bürgerinnen und Bürger, die zusätzlich permanenten Änderungen unterliegt. Eine wirtschaftliche, zeitnahe Aufgabenerfüllung stützt sich dabei zunehmend auf die Möglichkeiten der Informationstechnologien.

Aufgaben, Prozesse und die Aufbauorganisation unterliegen einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten.

In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen, Informationen und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen.

Modernes Verwaltungshandeln erfordert den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung der Kommunalverwaltung im Sinne der Bürgerinnen und Bürger, ortsansässiger Unternehmen oder weiterer Partner effizient und effektiv zu gestalten. Dies trifft auch auf die [Name der Behörde] zu. Beim Einsatz von Informationstechnologie muss die [Name der Behörde] darauf achten, dass der Sensibilität der ihr übertragenen und von ihr verarbeiteten Informationen mit der nötigen Sorgfalt Rechnung getragen wird. Die Informationssicherheit wird in zunehmendem Maße zu einer unverzichtbaren Grundlage für ein Verwaltungshandeln, dem die Bürgerinnen und Bürger, die Unternehmen und alle unsere Partner ihr Vertrauen schenken können. Daher muss sich die [Name der Behörde] dem Thema Sicherheit in der Informationstechnik in geeigneter Form stellen und die verarbeiteten Informationen geeignet schützen.

(2) Bezug der Informationssicherheit zu den Geschäftszielen oder Aufgaben der Institution

Es ist notwendig, das Zusammenspiel der Informationen, IT-Fachverfahren, Aufgaben und Produkte sowie der Infrastruktur der Informationstechnik und Kommunikationskanälen ganzheitlich zu betrachten. Informationssicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um diese Ziele zu erreichen.

Sowohl bei der Erbringung der Pflichtaufgaben als auch der Aufgaben, die die [Name der Behörde] auf freiwilliger Basis übernimmt, werden Informationen erhoben und verarbeitet, deren Vertraulichkeit, Integrität und Verfügbarkeit ein hohes Gut darstellen. Hierbei handelt es sich z.B. um Daten, die entsprechend gesetzlicher Anforderungen geschützt werden müssen, oder auch um

wettbewerbsrelevante Informationen ortsansässiger Unternehmen, die Unberechtigten nicht bekannt werden dürfen.

(3) Sicherheitsziele

Für den IT-Einsatz sind die Grundwerte der Informationssicherheit: Verfügbarkeit, Vertraulichkeit und Integrität im jeweils erforderlichen Maße zu erreichen.

Jede Leistung, Aufgabe oder Information wird nach einem Schutzbedarf eingestuft. Die Einstufung gibt die Anforderungen bezüglich der Grundwerte wieder. Die Feststellung des Schutzbedarfes erfolgt gemäß der [Anlage Schutzbedarfskategorien].

Damit ist es ein grundlegendes Ziel der Aufgabenerfüllung, die Schutzbedürfnisse der verarbeiteten Informationen zu wahren. Über geeignete Sicherheitsmaßnahmen muss dafür gesorgt werden, dass die Vertraulichkeit, die Integrität und die Verfügbarkeit der Informationen ihrem Schutzbedarf entsprechend gewährleistet werden können. Hierbei sind rechtliche Bestimmungen zu berücksichtigen. Um dies in einer auch wirtschaftlich angemessenen Form zu tun, ist es unabdingbar, den Schutzbedarf der Informationen zu kennen und dann die zu diesem Schutzbedarf passenden Maßnahmen zu ergreifen.

Neben den Informationen müssen auch [weitere Schutzobjekte benennen, falls diese explizit erwähnt werden sollen].

(4) Kernelemente der Sicherheitsstrategie

Die ISLL ist ein Rahmenwerk.

Die [Name der Behörde] erlässt nach Bedarf weitere Richtlinien zur Aufrechterhaltung der Informationssicherheit. Die Kommunalverwaltung führt eine Bedarfsermittlung durch und legt die Mindestsicherheitsstandards für ihre eigenen Verfahren fest. Bei ebenenübergreifenden Verfahren sind die entsprechenden Festlegungen des Bundes oder des Landes umzusetzen.

Als zentrale Sicherheitsinstanz ernennt die Behördenleitung eine/n IT-Sicherheitsbeauftragte/n und eine/n Stellvertreter/Stellvertreterin, der für alle Belange und Fragen der Informationssicherheit zuständig ist.

Der IT-Sicherheitsbeauftragte ist unabhängig und weisungsfrei. Er ist der Behördenleitung in dieser Rolle direkt unterstellt. Berichtswege sind festzulegen.

Ein Austausch mit der Leitung der Informationstechnik findet regelmäßig statt.

Dem IT-Sicherheitsbeauftragten sind geeignete Qualifizierungsmaßnahmen zu ermöglichen, um seine Verantwortung fachlich und zeitlich zu erfüllen.

Ein Informationssicherheits-Managementsystem (ISMS) ist zu etablieren. In regelmäßigen Abständen ist zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind. Der IT-Sicherheitsbeauftragte leitet das IS-Management-Team und entwickelt die notwendigen Maßnahmen fort.

Bei Gefahr im Verzug ist die/der IT-Sicherheitsbeauftragte/n oder sein/e Stellvertreter/in berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Das kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzübergängen führen.

Personen und Unternehmen, die nicht zur [Name der Behörde] gehören, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser ISLL einzuhalten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung.

Sicherheitsanforderungen von übergeordnetem Interesse, für deren Umsetzung eine vertragliche oder gesetzliche Verpflichtung besteht, sind zu erfüllen. Entsprechende Vorschriften und Maßnahmen stellen den Mindeststandard bei der Formulierung behördeninterner Vorschriften und Maßnahmen dar. Gemeinsame Basiskomponenten innerhalb der Behörde zur Vereinfachung und Stärkung der ebenenübergreifenden Verfahren sind zu nutzen.

Die Beschäftigen werden regelmäßig zu Fragen der Informationssicherheit sensibilisiert und qualifiziert.

Die vorliegende ISLL gibt den Rahmen für das Management der Informationssicherheit bei der [Name der Behörde] vor. Die wesentlichen Eckpunkte und Kernelemente der Strategie zur Informationssicherheit sind:

Textvorschlag 1 für eine mittlere bis große Kommunalverwaltung:

- Die [Name der Behörde] etabliert ein Informationssicherheitsmanagementsystem (ISMS) mit einem geeigneten Werkzeug zur Steuerung.
- Die [Name der Behörde] verankert das Thema Informationssicherheit in der Organisation über
  - eine geeignete IS-Organisation, die aktiv das Thema Informationssicherheit betreibt,
  - klar formulierte Sicherheitsvorgaben, die für alle Beschäftigten verbindlich sind,
  - die Integration von Sicherheitsaspekten in alle aus Sicht der Informationssicherheit relevanten Prozesse,
  - kontinuierliche und flächendeckende Sensibilisierungsmaßnahmen für alle Beschäftigten.
- Die [Name der Behörde] sorgt sukzessive für eine Absicherung der IT-Infrastruktur durch Umsetzung geeigneter Sicherheitsmaßnahmen auf der Infrastrukturebene.
- Die [Name der Behörde] orientiert sich bei allen Aktivitäten zur Informationssicherheit an den aktuellen Standards und Best Practices.

Textvorschlag 2 für eine kleine Kommunalverwaltung:

- Die für die [Name der Behörde] notwendigen Themen eines Informationssicherheitsmanagements werden in angemessener Form adressiert. Hierzu wird ein IT-Sicherheitsbeauftragter ernannt, der die notwendigen Maßnahmen mit der Behördenleitung abstimmt und für deren Umsetzung verantwortlich zeichnet.

(5) Verpflichtung zur Umsetzung der ISLL

Die Behördenleitung trägt die Gesamtverantwortung für die Informationssicherheit. Es obliegt ihr, für die Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit zu sorgen und die dafür benötigten Ressourcen bereitzustellen.

Die/Der [Name der Behörde] orientiert sich für die Umsetzung von Informationssicherheit am IT-Grundschutz und der Norm ISO/IEC 27001 der „International Organization for Standardization“ (ISO), der mindestens dem Standard-Schutzbedarf des BSI entspricht.

Der Aufwand für die Bereitstellung von Personal und Finanzmitteln zur Gewährleistung der Informationssicherheit soll für die eingesetzten und geplanten IT-Systeme ein angemessenes Informationssicherheitsniveau schaffen. Zur Umsetzung der Maßnahmen sind erforderliche Ressourcen und Investitionsmittel einzuplanen.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser definiert sich durch den Wert der zu schützenden Informationen und der IT-Systeme selbst. Zu bewerten sind die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigung der Aufgabenerfüllung, Beeinträchtigungen des Ansehens der Behörde und die Folgen von Gesetzesverstößen.

Es sind Regelungen für ein angemessenes Risikomanagement und ein internes Kontrollsystem (IKS) zu berücksichtigen. Die Behördenleitung ist zu informieren, falls notwendige Sicherheitsmaßnahmen aus bestimmten Gründen nicht umgesetzt werden können.

(6) Informationssicherheits-Organisation

Für bereits betriebene und für geplante Informationstechnik sind Sicherheitskonzepte zu erstellen. Der Schutzbedarf ist zunächst aus fachlicher Sicht für die Leistungen und Aufgaben zu erstellen. Anschließend wird der Schutzbedarf auf die Zielobjekte der Informationstechnik und Infrastruktur übertragen (vererbt).

Die Maßnahmen sind auch dann umzusetzen, wenn sich Beeinträchtigungen für die Nutzung ergeben. Bleiben Risiken untragbar, ist an dieser Stelle auf den Einsatz von Informationstechnik zu verzichten.

Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des Betriebes und der Informationssicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.

Unabhängig davon, ob und in welcher Weise Teilaufgaben delegiert werden, verbleibt die Gesamtverantwortung für die Gewährleistung der Informationssicherheit immer bei der Behördenleitung.

Textvorschlag 1 für eine mittlere oder große Kommunalverwaltung:

Die Behördenleitung kann die Verantwortung für die laufenden Angelegenheiten zum Informationssicherheitsmanagement an eine oder mehrere Verantwortliche in der [Name der Behörde] delegieren. Sie ernennt eine/n für die gesamte Kommunalverwaltung zuständigen IT-Sicherheitsbeauftragte/n. Das ISMS wird durch ein IS-Management-Team aufgebaut und betrieben, das die für das Informationssicherheitsmanagement notwendigen Aufgaben und Maßnahmen definiert und koordiniert. Hierzu gehören auch Vorschläge für die weitere Ausgestaltung der IS-Organisation. Die Informationssicherheit gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beschäftigten ihre Verantwortung in der täglichen Arbeit wahrnehmen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

Textvorschlag 2 für eine kleine Kommunalverwaltung:

Die Behördenleitung ernennt einen IT-Sicherheitsbeauftragten, der alle notwendigen Maßnahmen mit der Behördenleitung abstimmt und für deren Umsetzung verantwortlich zeichnet. Die Informationssicherheit gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beschäftigten ihre Verantwortung in der täglichen Arbeit wahrnehmen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

(7) Verpflichtung zur kontinuierlichen Verbesserung

Die Behördenleitung verpflichtet sich, sich an der Optimierung der Informationssicherheit zu beteiligen. Sie ist regelmäßig bzw. im Einzelfall akut über den aktuellen Sicherheitszustand durch die/den IT-Sicherheitsbeauftrage/n zu informieren und ist für die Absicherung der Kontinuität des Sicherheitsprozesses verantwortlich.

Die Sicherheitsmaßnahmen sind regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Beschäftigten bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Zur Erhaltung und Verbesserung der Informationssicherheit bedient sich der IT-Sicherheitsbeauftragte einer Arbeitsgruppe „Informationssicherheit", die aus Vertretern der Ämter oder Fachbereiche besteht.

Der IT-Sicherheitsbeauftragte ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig einzubinden. Er hat ein Vetorecht.

Durch eine kontinuierliche Betrachtung der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.

Verantwortlich für die Weiterentwicklung der ISLL und der IT-Sicherheitskonzepte ist der IT-Sicherheitsbeauftragte, wobei er von den Fachverantwortlichen bestmöglich unterstützt wird. Die

Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Begebenheiten und Einflüssen ab, wie z. B. neuen Bedrohungen, neuen Gesetzen oder auch der Entwicklung neuer technischer Lösungen. Diesen Entwicklungen müssen sich die Ansätze zum Management der Informationssicherheit anpassen. Aus diesem Grund muss dafür Sorge getragen werden, dass sich die Sicherheitsstrategie der [Name der Behörde] kontinuierlich fortentwickelt.

(8) Inkraftsetzung

Diese ISLL gilt für die gesamte Behörde.

Die ISLL tritt mit Unterschrift der Behördenleitung / Wirkung vom […] in Kraft und wird allen Beschäftigten nach Unterschrift umgehend zur Kenntnis gebracht.

(9) Anlage Schutzbedarfsdefinition

Definition der Schutzbedarfskategorien

Ziel: Auswahl eines dreistufigen Bewertungsmodelles für die Schutzbedarfskategorien in Anlehnung an den IT-Grundschutz nach BSI-Standard 100-2 für die Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Schutzbedarf	Schadensauswirkung
Normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können beträchtlich sein.
Sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 3: Schutzbedarfsdefinition

Hinweise zur Festlegung

Folgende Schadensszenarien sind zu berücksichtigen. Im Einzelfall wird geprüft, ob ggf. weitere Schadensszenarien möglich sind:

1. Beeinträchtigung von Leib- und Leben (persönliche Unversehrtheit)
2. Verursachung finanzieller Schäden (Grundsatz der Wirtschaftlichkeit und Sparsamkeit)
3. Beeinträchtigung des Ansehens der Behörde
4. Verletzung des Rechts auf informationelle Selbstbestimmung (BDSG und LDSG)
5. Verletzung von Gesetzten, Vorschriften oder Verträgen
6. Beeinträchtigung der Aufgabenerfüllung (Intern, Extern)

Es können ein oder mehrere Schadensszenarien einzeln oder zur gleichen Zeit auftreten.

Verantwortlich für die Festlegung ist der Prozessverantwortliche. Zur Unterstützung bei dieser Abgrenzung ist eine enge Kommunikation mit der Behördenleitung erforderlich. Die Notwendigkeit der Einbindung der IT-Leiters, des IT-Sicherheitsbeauftragten oder des Datenschutzbeauftragten ist zu empfehlen.

b) Übergreifende Aspekte der Informationssicherheit

Mit den „Übergreifenden Aspekten der Informationssicherheit" (Schicht 1 der IT-Grundschutzkataloge des BSI) werden bereits große Teile des Regelwerkes zur Informationssicherheit erfasst. Diese Aspekte bestehen aus 16 Bausteinen, in denen etliche Gefährdungen und korrespondierende Maßnahmen beschrieben werden. Mit diesen Bausteinen lässt sich ein Regelwerk für die Informationssicherheit hinreichend aufbauen bzw. lassen sich bestehende Regelungen dahingehend anpassen.

Art und Umfang der Regelungen richten sich nach den behördenspezifischen Rahmenbedingungen, den Sicherheitszielen sowie den zu berücksichtigenden Bausteinen der Schicht 1 des IT-Grundschutzes. Als Beispiel sei der Baustein „B 1.11 Outsourcing" genannt, in dem 26 Gefährdungen und 17 korrespondierende Maßnahmen gelistet sind. Dieser ist entbehrlich, wenn keiner der vorhandenen oder geplanten Geschäftsprozesse in der Behörde an externe Dienstleister vergeben wurde.

Darüber hinaus sind mehrere Bausteine während der Planungsphase nur einmal anzuwenden. Das bedeutet, dass die dafür notwendigen Regelungen an zentraler Stelle nur einmal erarbeitet werden müssen. Dazu zählen u.a. die Bausteine Sicherheitsmanagement, Organisation, Personal, Sensibilisierung und Schulung, Datensicherungskonzept, Löschen und Vernichten von Daten sowie der Schutz vor Schadprogrammen. Natürlich ist die Umsetzung der Regelungen regelmäßig zu prüfen und ggf. anzupassen. Diese Aufgabe lässt sich jedoch in bereits bestehende Managementprozesse integrieren.

c) Priorisierung und Abgrenzung kritischer Prozesse und Informationen

Ein funktionierendes Sicherheitsmanagement ist dadurch gekennzeichnet, dass im Hinblick auf das Schadenspotenzial kritische Geschäftsprozesse und Informationen bereits in der Planungsphase erfasst und im Sicherheitsprozess vorrangig berücksichtigt werden, da für diese in der Regel höhere Anforderungen an die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) bestehen.

Hierfür sind die Prozesse bzw. Informationen und deren Schutzbedarf zu erfassen. Der Schutzbedarf kann durch die drei Kategorien „normal", „hoch" und „sehr hoch" abstrakt und allgemeinverständlich dargestellt werden. Die Festlegung der Kategorien basiert auf der Betrachtung möglicher Schadensauswirkungen für die Kommunalverwaltung. Je höher mögliche Schäden ausfallen können, desto kritischer ist der genutzte Prozess bzw. der Umgang mit den Informationen.

Der IT-Sicherheitsbeauftragte bzw. das IS-Management-Team sollte die Schutzbedarfskategorien erarbeiten und der Behördenleitung zur Entscheidung vorlegen. Dieser Ablauf ist auch bei der Priorisierung der Prozesse und Verfahren zweckmäßig.

d) Sicherheitskonzepte

Das Sicherheitskonzept ist ein Hilfsmittel zur Umsetzung der Sicherheitsstrategie. Bei der Erarbeitung von Sicherheitskonzepten kann das PDCA-Modell genutzt werden, da diese auch einem Lebenszyklus unterliegen.

Im Sicherheitskonzept werden die Abhängigkeiten zwischen den Geschäftsprozessen (Aufgabenerfüllung) und den Gefährdungen (Höhere Gewalt, technische Mängel, menschliche Fehlhandlungen, etc.) analysiert, und es werden geeignete Maßnahmen zur Vermeidung, Reduzierung, Überwälzung oder Übernahme der erkannten Risiken festgelegt. Die damit verbundenen Aufgaben sollten durch einen dafür qualifizierten Beschäftigten wahrgenommen werden, wobei die Qualitätssicherung und Kontrollmöglichkeiten unabhängig bleiben sollten, z. B. durch den IT-Sicherheitsbeauftragten.

Bei der Dokumentation von Sicherheitskonzepten besteht in der Regel Formfreiheit. Die ISO/IEC 27001 stellt jedoch konkrete Mindestanforderungen zur Dokumentation[23].

Zur Erstellung, Verwaltung, Fortschreibung und Dokumentation von Sicherheitskonzepten bietet das BSI derzeit noch[24] das sogenannte GSTOOL an und nennt weitere Tools[25] .

[23] Mindestanforderungen zur Dokumentation der Informationssicherheit gemäß ISO/IEC 27001:2013. http://blog.iso27001standard.com/2013/09/30/list-of-mandatory-documents-required-by-iso-27001-2013-revision/.

[24] Der Support für das GSTOOL läuft nach Angaben des BSI voraussichtlich Ende 2016 aus.

[25] Toolangebote anderer Firmen https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/AndereTools/anderetools_node.html.

e) Beispiel zum IT-Grundschutzvorgehen

Durch eine optimale Zusammenstellung der technischen und organisatorischen Maßnahmen kann ein angemessenes Sicherheitsniveau erreicht und ausgebaut werden. Um Erfolg dabei zu haben, bedarf es der engen Zusammenarbeit aller Beteiligten. Dies soll anhand des Beispiels der Stadt Kassel verdeutlicht werden.

Der IT-Sicherheitsbeauftragte der Stadt Kassel betreut das ISMS. Er ist dem Personal- und Organisationsamt – Abteilung Informationstechnologie – zugeordnet. In der Stadtverwaltung gibt es eine Arbeitsgruppe Informationssicherheit (AG IS), die den IT-Sicherheitsbeauftragten unterstützt, übergreifende Maßnahmen initiiert und steuert. Diese Arbeitsgruppe setzt sich zusammen aus Vertretern aus jedem Dezernat sowie Mitgliedern mit IT-Kenntnissen oder mit Organisations- und Verwaltungserfahrung. Wichtig bei der Zusammensetzung war es, einen Querschnitt im „Lebensraum“ der Verwaltung mit unterschiedlichen Blickwinkeln einzubeziehen.

Für die ISLL wurde das Muster der Leitlinie des Landes Hessen genutzt und durch die Arbeitsgruppe an die eigenen Bedürfnisse angepasst. Sie wird in einem Pilotprojekt auf Anwendbarkeit, Zuverlässigkeit und Vollständigkeit überprüft. Die ISLL wird durch den Oberbürgermeister der Stadt Kassel mit einer Verfügung in Kraft gesetzt.

In den Grundsätzen wurde festgelegt, dass nach IT-Grundschutz unter Abwägung der Werte, Risiken und des Aufwands vorzugehen ist. Ein wesentlicher Grundsatz ist die Gewährleistung der Leistungsfähigkeit und Funktionsfähigkeit der Behörde, wobei die durch bestimmte Maßnahmen möglicherweise eintretenden Beeinträchtigungen, durch alle Beschäftigten zu akzeptieren sind. In Fällen, in denen die Risiken für die Informationssicherheit nicht beherrscht werden können oder untragbar sind, ist auf die IT-Nutzung zu verzichten!

Als Sicherheitsziel haben alle Beschäftigten der Stadt Kassel den Bürgerinnen und Bürgern zu vermitteln, dass ihre Daten vor Dritten geschützt sind (Vertraulichkeit), sie Dienste in Anspruch nehmen können, wenn sie sie benötigen (Verfügbarkeit), und dass die Daten korrekt sind (Integrität). Da sich der Sicherheitsprozess am IT-Grundschutz orientiert, wurden drei Schutzbedarfskategorien festgelegt.

Szenario	Schutzbedarfskategorie		
	normal	**hoch**	**sehr hoch**
1. Beeinträchtigung der persönlichen Unversehrtheit (Leib- und Leben)	Keine Beeinträchtigung	Beeinträchtigung möglich	Gravierende Beeinträchtigungen sind möglich; Gefahr für Leib und Leben droht.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts (Datenschutz)	Durch die Verarbeitung personenbezogener Daten könnten Betroffene gesellschaftlich oder wirtschaftlich beeinträchtigt werden; Hier nur mit geringfügigen Konsequenzen.	Beeinträchtigung hätten erhebliche wirtschaftliche oder soziale Konsequenzen und würden nicht toleriert.	Beeinträchtigungen hätten gravierende wirtschaftliche oder soziale Konsequenzen und sind unter keinen Umständen zu tolerieren.
3. Verstoß gegen Gesetze, Vorschriften und Verträge	Nur geringe Konsequenzen mit geringen Konventionalstrafen (bis zu 10.000 Euro)	Erhebliche Konsequenzen mit hohen Konventionalstrafen (bis zu 100.000 Euro)	Fundamentale Gesetzesverstöße mit ruinösen Haftungsschäden (weit über 100.000 Euro)
4. Finanzielle Auswirkungen (finanzrelevante Regressforderungen)	Nur geringe Schäden (bis zu 10.000 Euro)	Große Schäden (bis zu 100.000 Euro)	Sehr große Schäden (weit über 100.000 Euro)

Tabelle 4: Beispiel der Schutzbedarfskategorien der Stadt Kassel

Als Verantwortliche für die Informationssicherheit sind die Behördenleitung und die Führungskräfte benannt. Sie legen die im Sicherheitsprozess zu erfassenden Geschäftsprozesse sowie die Art und den Umfang von Sicherheitskontrollen fest.

Die Beschäftigten haben alle Sicherheitsmaßnahmen einzuhalten. Falls Sicherheitsvorfälle eintreten, sind diese unverzüglich zu melden, wobei die dafür notwendige Unterstützung durch Sensibilisierungsmaßnahmen zugesagt wird.

Weitere Verantwortliche sind die/der Sicherheitsbeauftragte/r und die AG IS. Ihre Mitglieder sollten Kenntnisse der IT oder der Organisation und der Behörde haben. Darüber hinaus ist jedes Dezernat in der AG IS vertreten.

Da auch Externe und Dritte sich an die Vorgaben zu halten haben, wird die Behörde zur Verpflichtung von Auftragnehmern aufgefordert, sich an die Ziele und Vorgaben der Informationssicherheit zu halten und erkennbare Mängel oder Risiken mitzuteilen.

Die ISLL hat verpflichtenden Charakter für alle Beschäftigten. Um dies zu verdeutlichen, werden Verstöße und deren Folgen beispielhaft aufgeführt. So ist das vorsätzlich oder grob fahrlässige Handeln, mit den möglichen Folgen des Schadenersatzes, disziplinar- oder arbeitsrechtliche Ahndung und u. U. der Ordnungswidrigkeit oder einer Straftat aufgeführt.

Der Prozess zur Erstellung von Sicherheitskonzepten wurde grafisch in einem Ablaufdiagramm erfasst und stellt anschaulich die Phasen, die Verantwortlichkeiten und die Teilprozesse dar. Die Darstellung stellt den Idealfall dar, da Maßnahmen, die aus unterschiedlichsten Gründen nicht umgesetzt werden können, im Rahmen einer Risikobewertung dem Fachamt bzw. der Behördenleitung zur Entscheidung vorzulegen sind.

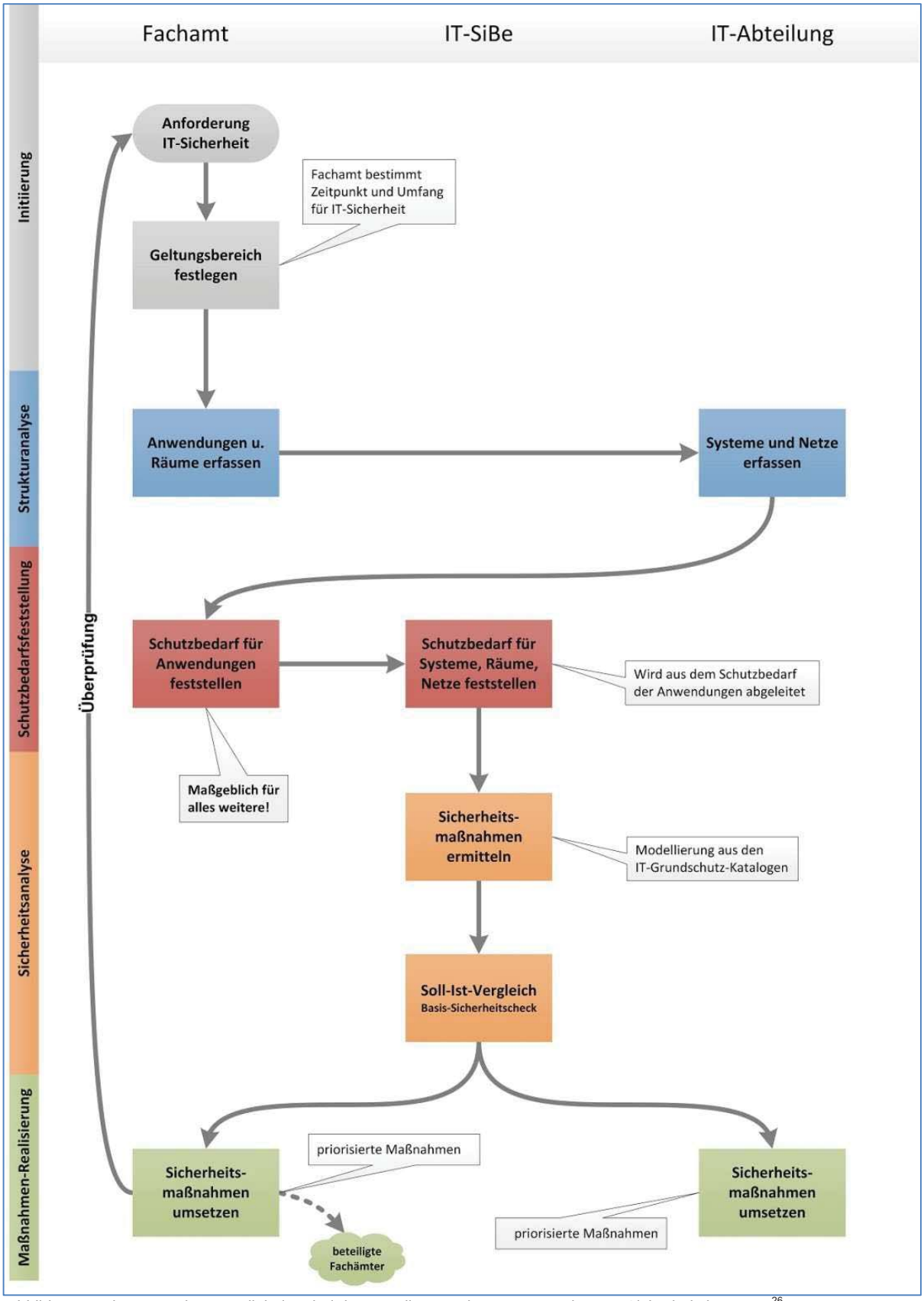

Abbildung 4: Phasen und Zuständigkeiten bei der Erstellung und Umsetzung eines IT-Sicherheitskonzepts[26]

[26] Lange, Jens (IT-Sicherheitsbeauftragter); Stadt Kassel [12.03.2013] aus "Richtlinie Informationssicherheit" [Grafik]; (Genehmigung zum Abdruck zu nicht kommerziellen Zwecken).

3. Prüfen und Überwachen (Check)

Ein wichtiger Bestandteil eines funktionierenden ISMS ist die Erfolgskontrolle. Dabei erscheinen der Umsetzungsstand festgelegter Sicherheitsmaßnahmen, aber auch die Erfassung und Auswertung von Sicherheitsvorfällen als geeignete Hilfsmittel. Diese Aufgaben sollte dem IT-Sicherheitsbeauftragten übertragen bzw. einem für die Informationssicherheit Verantwortlichen, der ein hohes Maß an Vertrauen bei den Beschäftigten genießt und gleichzeitig Unabhängigkeit in Bezug auf die Umsetzung der Informationssicherheit hat. Dadurch kann eine neutrale Auswertung des Erfolges erreicht werden.

Gegenüber der Behördenleitung sollten die Ergebnisse der Erfolgskontrollen regelmäßig in geeigneter Form mitgeteilt werden, um das Sicherheitsniveau durch geeignete Maßnahmen zu steuern und dadurch kontinuierlich zu verbessern. Dem zuständigen Beschäftigten sollte explizit gegenüber der Behördenleitung ein direktes Vortragsrecht eingeräumt werden.

Indikatoren für den Stand der Informationssicherheit sollten festgelegt und vom IS-Management-Team analysiert werden. Dazu zählen unter anderem die Ergebnisse von Sensibilisierungsmaßnahmen und internen Audits. Weiterhin sollten alle Sicherheitsvorfälle, Ausnahmeregelungen im Umgang mit Informationen und Fehlreaktionen von Beschäftigten ausgewertet werden, um Schwachstellen zu identifizieren und abzustellen.

a) Behandlung von Sicherheitsvorfällen

Sicherheitsvorfälle sind unter anderem das Auftreten von Computerviren, die Offenlegung von Informationen und der Ausfall existenzieller IT-Dienste. Die mit einem Sicherheitsvorfall verbundenen Schäden können weitreichende Auswirkungen haben. Sie führen unter anderem zu einer Einschränkung der Aufgabenerfüllung, können hohe Kosten verursachen und sind in der Regel geschäftsschädigend.

Sicherheitsvorfälle lassen sich nicht immer sofort erkennen. Durch Fehlplanungen, mangelnde Steuerung und falsche Entscheidungen ergeben sich Risiken, die ein Sicherheitsproblem darstellen können. Schnell wird aus einem Sicherheitsvorfall ein größeres Sicherheitsproblem. Somit ist es wichtig, Sicherheitsvorfälle frühzeitig zu erkennen und umgehend zu behandeln.

Die Behördenleitung sollte eine Anlaufstelle zur Meldung von eingetretenen aber auch vermuteten Sicherheitsvorfällen festlegen. Falls ein Service Desk (auch Help Desk genannt) existiert, kann dieser benannt werden. In kleineren Behörden können die Meldungen z. B. auch direkt an den IT-Sicherheitsbeauftragten oder den IT-Leiter erfolgen. Die Beschäftigten sind darüber zu informieren und sollten motiviert werden, dass die Meldung von Sicherheitsproblemen und Sicherheitsvorfällen zur Lösungsstrategie zählt und sich daraus keinesfalls Schuldzuweisungen ergeben. So können Bedrohungen schneller erkannt und berücksichtigt werden.

Bei der Festlegung der Meldewege ist eine Eskalationsstrategie vorzusehen, wodurch beim Auftreten von schwerwiegenden Sicherheitsvorfällen bzw. für den Fall, dass für die Behörde kritische Sicherheitsprobleme eingetreten sind, die Behördenleitung und andere Stellen durch die zentrale Meldestelle einzubeziehen sind.

b) Berichtswesen zur Informationssicherheit

Die Leitungsebene sollte in regelmäßigen Abständen über die Probleme, die Erfolge und die Verbesserungsmöglichkeiten der Informationssicherheit schriftlich vom IT-Sicherheitsbeauftragten bzw. dem IS-Management-Team informiert werden. Der Bericht sollte mindestens einmal jährlich erstellt und der Behördenleitung vorgelegt werden.

Neben dem Sicherheitsstatus zu kritischen Prozessen und Informationen sind weitere Punkte aufzunehmen. Dazu zählen unter anderem Ergebnisse interner und ggf. externer Audits, Folgemaßnahmen aufgrund vorheriger Sicherheitsbewertungen, Ergebnisse der Beratungen des IS-Management-Team, ein Überblick aller Sicherheitsvorfälle des Berichtszeitraumes und ggf. zur allgemeinen Sicherheitslage.

Der Bericht dient insbesondere als Entscheidungsgrundlage für die Behördenleitung.

4. Verbessern (Act)

Im Planungsprozess zum ISMS ist die Informationssicherheitsrevision zu berücksichtigen. Nur durch regelmäßige Überprüfung und Bewertung des etablierten Sicherheitsprozesses und der Sicherheitsmaßnahmen können Aussagen zur Konformität, Effizienz und Effektivität getroffen werden.

Die Revisionen und deren Ergebnisse sind durch den IT-Sicherheitsbeauftragten bzw. durch das IS-Management-Team auszuwerten. Daraus ergeben sich Vorschläge zur Verbesserung der Informationssicherheit. Die im Kapitel VI. 2a dargestellten übergreifenden Aspekte der Informationssicherheit bieten einen Ansatz für die Themenbereiche, wozu die Punkte Sicherheitsmanagement, Organisation und Personal zählen. Weitere Themenschwerpunkte für Vorschläge zur Verbesserung können unter anderem auch die Prozesse, Verfahren und die Technik berücksichtigen. Die Vorschläge sollten in das Berichtswesen integriert werden.

Zielsetzung ist die stetige Verbesserung des ISMS. Dies kann durch Korrekturen zur Vermeidung bestehender Ursachen, aber auch durch Verhindern weiterer Einflüsse geschehen. Die Behördenleitung übernimmt dabei die Steuerung des Prozesses und hat im Rahmen ihrer Managementverantwortung die Ergebnisse zu prüfen und die Vorschläge zu bestätigen.

VII. Fazit

100% Sicherheit gibt es nicht! Bestimmten Risiken kann man nicht wirtschaftlich sinnvoll entgegentreten. Das Management hat die verbleibenden Risiken in Erfahrung zu bringen, mit geeigneten Mitteln entgegenzusteuern (etwa durch Umstrukturierungen) oder diese unter bestimmten Umständen zu akzeptieren. Je nach Größe, Organisationsstruktur, Sicherheitsbedürfnis bzw. Reifegrad und finanziellen Möglichkeiten werden die Anforderungen an das ISMS unterschiedlich ausfallen.

Größtmögliche Sicherheit ist nicht im Rahmen eines einmal zu durchlaufenden Projektes zu erreichen. Die stetige Verbesserung der Sicherheit stellt einen Regelkreis dar. Gemäß dem Paretoprinzip können 80% der Ergebnisse in 20% der Gesamtzeit eines Projektes erreicht werden, wobei für die verbleibenden 20% der Ergebnisse insgesamt 80% der Zeit zu berücksichtigen sind und dadurch die meiste Arbeit verursachen. Steigende Anforderungen an die Informationssicherheit sind mit einem höheren Bedarf an Ressourcen verbunden – dies ist bei der Planung des ISMS zu berücksichtigen.

Unabhängig von der Organisation der IT (Betrieb in Eigenregie oder durch IT-Dienstleister) kann keine pauschale Empfehlung zum ISMS und dem erreichbaren Sicherheitsniveau gegeben werden. Auch bei der Zusammenarbeit mit IT-Dienstleistern ist die Behörde nicht vom Informationssicherheitsmanagement entbunden, die Verantwortung und die Kontrollpflichten verbleiben beim Auftraggeber. Die übergreifenden Aspekte der Informationssicherheit (z. B. Sicherheitsmanagement, Organisation, Personal etc.) und die Risiken für die Geschäftsprozesse sind auch durch einen IT-Dienstleister nicht oder nur teilweise zu beeinflussen. Nichtsdestotrotz reduziert die Übertragung von Aufgaben des IT-Betriebs an einen IT-Dienstleister die Komplexität des Informationsverbundes deutlich und erleichtert die Beherrschung der Informationssicherheit. Den Aufbau eines ISMS können IT-Dienstleister unterstützen, da die notwendigen Kompetenzen hier standardmäßig vorhanden sind und durch vertragliche Regelungen eingefordert werden sollten.

Vor dem Hintergrund der weiter zunehmenden Komplexität der kommunalen IT-Infrastrukturen, der prognostizierbaren weiteren Öffnung der Verwaltung nach außen (Open Data, E-Government-Services etc.), der wachsenden Intransparenz vielgestaltiger Bedrohungen und schließlich der zunehmenden Aufmerksamkeit der Bürgerinnen und Bürger (und der Medien) sollten Verwaltungen, die ihre IT allein betreiben, intensiv prüfen, ob eine Zusammenarbeit mit einem professionellen kommunalen IT-Dienstleister zu einer Verbesserung der Informationssicherheit beiträgt.

Generell bedarf es des Bekenntnisses der Behördenleitung zur Informationssicherheit und eines klaren Regelwerkes unter Berücksichtigung der Verantwortlichkeiten. Alle Beschäftigten der Behörde sind in den Sicherheitsprozess einzubeziehen. Bestimmten Gefährdungen, wie z. B. dem Social Engineering[27], kann nur zusammen mit organisatorischen Maßnahmen wirksam entgegengewirkt werden.

Die Leitlinie für die Informationssicherheit des IT-Planungsrates fordert ebenenübergreifende Informationssicherheit für Bund, Länder und Kommunalverwaltungen. Dabei ist die interkommunale Zusammenarbeit zur Umsetzung einheitlicher Sicherheitsmaßnahmen nicht nur unter Berücksichtigung von Wirtschaftlichkeitsaspekten nötig. Die kommunalen Spitzenverbände sind die Interessenvertreter in den Steuerungsgremien von Bund und Ländern. Mit dem nicht öffentlichen IT-SiBe-Forum[28] bieten sie zudem eine Austauschplattform für IT-Sicherheitsbeauftragte und Praktiker in den Kommunalverwaltungen.

[27] Unter diesem Begriff werden allgemein Angriffstechniken zusammengefasst, die sich auf die gezielte Manipulation von Menschen beziehen, um Zugang zu Computersystemen zu erlangen. Ein Beispiel bildet die Vortäuschung bestimmter Identitäten, um angriffsrelevante Informationen von Mitarbeitern zu erhalten.

[28] Link zum IT-SiBe-Forum, Betreiber: Deutscher Landkreistag; http://it-sibe-forum.de/.

VIII. Glossar und Abkürzungen

AG IS	Arbeitsgruppe Informationssicherheit
BDSG	Bundesdatenschutzgesetz
Bedrohung	Umstand, der zur Schädigung der Grundwerte (Verfügbarkeit, Vertraulichkeit und Integrität) führen kann.
Best Practice	Gängige Praxis
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-Standard	Reihe der Veröffentlichungen zur Einführung eines ISMS, zum IT-Grundschutzvorgehen, zur Risikoanalyse auf Basis von IT-Grundschutz und zum Notfallmanagement
CERT	Computer Emergency Response Team (Computer-Notfall-Team)
E-Government-Services	Dienstleistungen der öffentlichen Verwaltung durch Einsatz moderner Informations- und Kommunikationstechniken
EU-Zahlstellen	Öffentliche Stelle zur Bewilligung, Kontrolle und Zahlungen von EU-Fördergeldern
Gefährdung	Stellt eine Bedrohung dar, falls Schwachstellen existierten und ausgenutzt werden.
Geschäftsprozess	Abfolge von Arbeitsschritten eines Verwaltungsvorganges.
GSTOOL	Grundschutz-Tool: Hilfsmittel zur Verwaltung und Dokumentation von Sicherheitskonzepten und Risikoanalysen
IKS	Internes Kontrollsystem, auch Revision
IS	Informationssicherheit
ISLL	Informationssicherheitsleitlinie
ISMS	Informationssicherheits-Managementsystem
ISO	International Standards Organisation
IS-Organisation	Allgemeine Bezeichnung der aktiv am ISMS beteiligten Personen und des IT-Sicherheitsbeauftragten
IT	Informationstechnik
IT-Grundschutz	Empfehlungen des BSI für ein Standard-Sicherheitsniveau mit ganzheitlichem Ansatz bezüglich organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen
LDSG	Landesdatenschutzgesetze
Nationales Waffen Register	Zentrale Komponente zur Verwaltung von Schusswaffen, an die alle Waffenbehörden angeschlossen sind
Open Data	Bereitstellung allgemein zugänglicher Daten und Informationen zur Weiternutzung
Outsourcing	Auslagerung von Geschäftsprozessen an externe Dienstleister
Paretoprinzip	Nach Vilfredo Pareto (1848–1923) benanntes Prinzip, dass 80% der Ergebnisse in 20% der Gesamtzeit erreicht werden können.
PDCA-Zyklus	Auch als Deming-Rad bezeichnet, ist ein nach William Edwards Deming (1900–1993) benannter iterativer vierphasiger Problemlösungsprozess mit Ursprüngen in der Qualitätssicherung
Qualitätssicherung	Sammelbegriff zur Sicherstellung festgelegter Qualitätsanforderungen
Ressourcen	Gesamtheit aller zur Aufgabenerfüllung notwendiger materieller und immaterieller Mittel
Risikoanalyse	Mittel zur Feststellung und Bewertung von Gefährdungen und Bedrohungen im Risikomanagement

Risiko-management	Prozess zur Behandlung von Risiken, wobei Maßnahmen festgelegt werden, um verbleibende Risiken zu vermeiden, zu reduzieren, auf Dritte abzuwälzen oder ggf. die damit verbunden Konsequenzen zu tragen.
Roadmap	Synonym für eine zeitliche Darstellung eines geplanten Ablaufes
Schad-programme	Computerprogramme mit unerwünschten und meist schädigenden Funktionen
Sicherheits-konzept	Dokument zur Umsetzung der Sicherheitsstrategie und zur Erreichung der Sicherheitsziele
Sicherheits-strategie	Abstrakte Festlegung, mit welchen Mitteln die Organisation die Sicherheitsziele erreichen will.
Sicherheits-ziele	Festlegungen zum angestrebten Sicherheitsniveau
Social Engineering	Ausnutzen persönlicher Umstände oder des persönlichen Umfeldes einer Person zur Erlangung vertraulicher Informationen
Verbindungs-netz	Informationstechnisches Netz, welches die Netze des Bundes und der Länder verbindet (§ 2 IT-NetzG)
Verwaltungs-netz	Kommunikationsnetz des Bundes oder der Länder im Verbund der öffentlichen Verwaltung