Technische Hochschule
Brandenburg
University of
Applied Sciences

Anwendung der IT-Grundschutz-Methodik auf die IT-gestützte Personal- und Gebäudeverwaltung einer Landesbehörde

Bachelorarbeit
zur Erlangung des Grades Bachelor of Science
des Fachbereichs Informatik und Medien der
Technischen Hochschule Brandenburg

vorgelegt von:
Maik Henker

Betreuer: Prof. Dr. Michael Pilgermann
Zweitgutachter: Dipl.-Ing. (FH) Ines Lehnert (LASuV)

Brandenburg an der Havel, 21. Juli 2022

Sperrvermerk

Die Anlagen der vorliegenden Bachelorarbeit enthalten institutionsinterne Informationen und vertrauliche Sachverhalte. Sie sind daher nur den Gutachtern zu Prüfungszwecken zugänglich zu machen. Veröffentlichungen und Vervielfältigungen dieser Anlagen – auch auszugsweise – sind ohne ausdrückliche Genehmigung des Landesamtes für Straßenbau und Verkehr nicht gestattet.
Ausgenommen vom Sperrvermerk sind Auszüge dieser Anlagen im Text selbst, sowie der gesamte Text der Bachelorarbeit.

Dresden, 21.07.2022

Ort, Datum Unterschrift Verfasser

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Dresden, 21.07.2022

Ort, Datum Maik Henker

Kurzfassung

Eine Landesbehörde in Sachsen ist zum Schutz vor Cyberangriffen gesetzlich verpflichtet ein Informationssicherheitsmanagementsystem zu errichten. Die dafür nötigen Voraussetzungen wie die Einbindung der Leitungsebene und die Erstellung eines Sicherheitskonzeptes liegen bisher nicht vor. Für den Einstieg in die Informationssicherheit veranschaulicht diese Bachelorarbeit die Anwendung der IT-Grundschutz-Methodik des BSI. Zur Komplexitätsreduzierung wurde methodisch die Kernabsicherung nach BSI 200-2 zunächst für die Personalverwaltung und die Gebäudeverwaltung durchgeführt. Im Anschluss wurden Teile der unterstützenden IT-Systeme analysiert. Als Ergebnis der Strukturanalyse, Schutzbedarfsfeststellung, Risikoanalyse und des interviewgestützten Soll-Ist-Vergleiches entstand ein Sicherheitskonzept. Aus dessen Umsetzungstand wurde ein Umsetzungsplan entwickelt.

Schlüsselwörter

IT-Grundschutz
BSI-Standard 200
Informationssicherheit
Informationssicherheitskonzept
Öffentliche Verwaltung

Abstract

A state authority in saxony is obligated by law to establish a Management Systems for Information Security to protect them against cyber-attacks. The necessary pre-conditions like accepting the responsibility by the top management and drawing up a security concept are not present yet. To initiate information security these bachelor thesis shows the usage of IT-Grundschutz Methodology. Cause for reducing complexity the core protection from BSI 200-2 was proceeded for personnel administration and for building management for the moment. Afterward parts of the supporting IT systems have been analysed. In result of structure analysis, protection needs, risk analysis and interview-based gap analysis a security concept was developed. On its state an implementation order has been developed.

Keywords

IT-Grundschutz
BSI Standards 200
information security
security concept
public administration

Gender Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Bachelorarbeit auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Formulierungen gelten gleichermaßen für alle Geschlechter.

Inhaltsverzeichnis

1 Einleitung

»Der nächste Tsunami kommt bestimmt. Diesmal werden die Ursache nicht Kreditrisiken sein, sondern Risiken im Bereich Cyber-Sicherheit«, sagte Peter Hiekann vom FinTech-Unternehmen NDGIT bei der Konferenz *Banking & Technology*. Die Krone dieses Tsunamis wächst jeden Tag um 394.000 neue Schadprogramm-Varianten laut Lagebericht zur IT-Sicherheit in Deutschland 2021 vom Bundesamt für Sicherheit in der Informationstechnik – BSI (2021b, S. 9). Prägende Angriffsarten im Berichtszeitraum waren unter anderem Schutzgelderpressung, Lösegelderpressung und Schweigegelderpressung (BSI, 2021b, S. 9–10). Dies alles ausschließlich im Cyberraum. Für den Autor dieser Arbeit sehr prägend war die Log4j-Schwachstelle zum Jahreswechsel 2021/2022. Die Schwachstelle ermöglichte das Ausführen von beliebigen Java-Code auf den betroffenen Systemen. Auch das Einschleusen von Schadcode war denkbar einfach, wie Schmidt auf Heise.de im Dezember 2021 berichtete. Die betroffene Java-Bibliothek steckt in vielen Programmen (Schmidt, 2021). Hektische Aktivitäten zur Meldung betroffener Software führten die Lücken in der eigenen Dokumentation vor Augen. Seit 2020 berichtet der Beauftragte für Informationssicherheit des Landes Sachsen regelmäßig über veröffentlichte Schwachstellen und das Computer Emergency Response Team (CERT) des Freistaates Sachsen muss immer wieder die Ausführung zeitkritischer Updates einfordern. Berichte in der Presse über Lösegelderpressungen von verschlüsselten Dateien in Anhalt-Bitterfeld, der Angriff auf das Universitätsklinikum in Düsseldorf und auch neu aufkommende Sicherheitsfragen für das Arbeiten im Home-Office beim eigenen Arbeitgeber machten deutlich, dass hierfür bisher keine geeigneten Prozesse zur Verfügung stehen.

Die immer kürzere Schlagfolge von gemeldeten Sicherheitsproblemen, die immer komplexer werdende eigene IT-Infrastruktur und nicht zuletzt gesetzliche Forderungen für den Schutz der IT-Systeme drängten das Thema umfassender Sicherheitsmechanismen immer weiter in den Vordergrund.

Im Landesamt für Straßenbau und Verkehr – LASuV – konnte bisher aus Zeitgründen kein Sicherheitskonzept erarbeitet und umgesetzt werden. Die IT-Stellen der 6 Standorte arbeiten eng bei Planung, Beschaffung und Betrieb der IT-

Systeme zusammen. Die meist operativ geprägte Arbeit führte bisher zu Sicherheitsmaßnahmen aus eigenem Wissen und Ermessen. Das Sächsische Informationssicherheitsgesetz fordert jedoch eine umfassende und konzeptgetriebene Etablierung der Informationssicherheit nach dem IT-Grundschutz des BSI. Die nötigen Voraussetzungen wie die Verantwortungsübernahme durch die Leitungsebene, ein kontinuierlicher Informationssicherheitsprozess und ein aktuelles Sicherheitskonzept fehlen bisher. Unter diesen Rahmenbedingungen soll das LASuV in den IT-Grundschutz einsteigen. Hierzu wird die gesetzlich vorgeschriebene IT-Grundschutzmethodik zunächst auf einen eng abgegrenzten Bereich angewandt. Dies entspricht im Vorgehen der sogenannten *Kernabsicherung*. Die Durchführung der Einzelschritte *Strukturanalyse, Schutzbedarfsfeststellung*, *Modellierung, IT-Grundschutz-Check* und *Risikoanalyse* nach BSI 200-2 werden für das LASuV erstmalig durch den Autor durchgeführt. Dabei soll auch Erfahrung für die Ausweitung und kontinuierliche Verbesserung des so entstehenden Sicherheitskonzeptes gesammelt werden. Konkrete Maßnahmen und Umsetzungen müssen außerhalb der Arbeit schrittweise erarbeitet werden.

Neben grundlegenden Begriffen zeigt die Arbeit zunächst weitere Standards mit Bezug zur Informationssicherheit auf. Einem genauen Blick auf die Rahmenbedingungen und den bisherigen Zustand folgt die Erklärung der IT-Grundschutz-Methodik und die weitere Vorgehensweise. Hieran schließt sich die Darstellung der praktisch geleisteten Anwendung der IT-Grundschutz-Methodik an. Das im Resultat entstandene Sicherheitskonzept zeigt noch offene Maßnahmen auf, welche in einem priorisierten Plan künftig zur Umsetzung gebracht werden sollen.

Informationssicherheit ist ein permanenter Prozess und bedarf nicht nur der ständigen Verbesserung, sondern auch des beständigen Lernens.

2 Begriffe

Bei der Kommunikation mit Fachfremden wie der Leitungsebene, Mitarbeitern oder weiteren Interessensgruppen wie Personalvertretungen oder Dritten, ist eine allgemeinverständliche Begriffsdefinition und -abgrenzung notwendig. Dies hilft Missverständnisse und ein aneinander vorbeireden zu vermeiden. Es ist sinnvoll die Bedeutung von ähnlichen Begriffen so aufzufassen, dass diese der Bedeutung in Normen, Standards, Gesetzen und Verordnungen möglichst genau entspricht. Auch bei der Kommunikation mit Fachleuten ermöglicht insbesondere die Abgrenzung von Begriffen, nötige Aufgaben aus der komplexen Gesamtsicht kleinteilig genug definieren zu können. (Kersten & Klett, 2015, S. 9–10)

2.1 Daten und Information

Nach Witt sind Daten „…kontextfreie Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen.“. Er merkt an, dass diese Definition dem informationstechnischen Sinn entspricht, dabei aber bei der Verwendung insbesondere im Sinne von Datenschutzgesetzen eher dem Begriff Information entspricht. Erst durch die Interpretation von Daten in einem Kontext werden daraus Informationen. Im Sinne der Datenschutzgesetze setzt der Bezug zur Person den Kontext und macht damit aus einem Datum eine Information. „39“ ist ein Datum, erst der Kontext „Alter des Autors“ macht daraus eine personenbezogene Information, welche durch den Datenschutz geschützt wird. (Witt, 2010, S. 4–5)

2.2 Datenschutz

Der Begriff Datenschutz enthält zwei Sichtweisen. Zum einen den eigentumsgeprägten Schutz der Daten vor unerwünschten Zugriff oder Verlust. Zum anderen soll der Bürger vor den Folgen der zweckwidrigen Verwendung seiner Daten bzw. Informationen geschützt werden. (Witt, 2010, S. 4–5)

Im Sinne der zweiten Sichtweise sichert in der Europäischen Union seit 2016 die Datenschutzgrundverordnung (DSGVO) den Bürgern umfassende Rechte über sie gespeicherte Informationen zu. Hier sind eine strenge Zweckbindung, Auskunftsrechte der Bürger und Pflichten der datenverarbeitenden Institutionen

geregelt. Institutionen, die Daten mit Personenbezug erheben oder verarbeiten, müssen laut Artikel 24 und 37 DSGVO einen Beauftragten für Datenschutz benennen und geeignete Maßnahmen zum Schutz der personenbezogenen Daten ergreifen.

2.3 Datensicherheit

Die Datensicherheit stellt die erste Sichtweise des Begriffs Datenschutz dar. Entsprechende Maßnahmen zielen darauf ab, die Daten vor unerlaubten Zugriff und Missbrauch zu schützen. Aber auch der Verlust oder Beeinträchtigung durch höhere Gewalt, durch menschliche oder technische Fehler sollen verhindert werden. (Witt, 2010, S. 3)
Das BSI sieht diesen Begriff hingegen als Synonym für Informationssicherheit (BSI, 2022a).

2.4 Informationssicherheit

Aus Sicht der Informationssicherheit liegen Daten und Informationen auch außerhalb von IT-Systemen vor. Informationen können auch in Papierform oder aber in den Köpfen der Mitarbeiter vorliegen (BSI, 2022a). Auch können Informationen unbewusst erzeugt werden. Zum Beispiel sind Verbindungsdaten Informationen, die notwendigerweise zum Betrieb von Systemen ohne bewusste Entscheidung erzeugt werden. Für die Aufrechterhaltung der Informationssicherheit werden die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit definiert. Unbefugter Zugriff oder Manipulation von Daten soll vorbeugend verhindert werden, um wirtschaftliche Schäden zu verhindern. (Hanschke, 2020, S. 2)
Hier zeigt sich, dass Datensicherheit eine Teilmenge der Informationssicherheit ist. Die Informationssicherheit fasst ihre Aufgaben jedoch weiter. Ein nicht abschließendes Beispiel: Daten bzw. Informationen, die auf einer USB-Festplatte gespeichert sind, welche jedoch mit keinem PC verbunden ist, erfüllt die Anforderungen der Datensicherheit. Befindet sich diese USB-Festplatte im berechtigten Besitz sind deren Daten im Sinne des Eigentumsrechts und der Existenz der Daten gesichert. Nämlich auf der USB-Festplatte. Das Ziel der Verfügbarkeit aus der Informationssicherheit ist jedoch nicht erfüllt. Ohne PC-System kann auf die Daten trotz Berechtigung nicht zugegriffen werden.

2.5 IT-Sicherheit

Dieser Begriff beschäftigt sich gezielt mit der Sicherheit der IT-Systeme mit denen Informationen gespeichert und verarbeitet werden. Er ist Teilbereich der Informationssicherheit und betrachtet vor allem alle technischen und organisatorischen Maßnahmen, welche direkt auf IT-Systeme und Geräte angewandt werden. Ziele sind hier ebenso die Vertraulichkeit, Verfügbarkeit und Integrität der elektronischen Systeme und Daten. (BSI, 2017b, S. 11)

2.6 Bedrohung

Im IT-Kontext ist eine Bedrohung „…ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann.“ (BSI, 2021c) Bedrohungen sind abstrakt immer vorhanden.

2.7 Schwachstelle

Das BSI definiert eine Schwachstelle als Fehler in einem IT-System oder einer Institution, der sicherheitsrelevant ist. Ursachen können in einer fehlerhaften oder ungenügenden Konzeption, Implementierung, Konfiguration, Organisation oder in unsachgemäßem Betrieb liegen. Schwachstellen können technischer oder organisatorischer Natur sein. Erst das Vorhandensein einer Schwachstelle kann eine Bedrohung wirksam machen. (2021c)

2.8 Gefährdung

Das Vorhandensein einer Schwachstelle per se ist noch keine Gefährdung. Existiert jedoch eine Bedrohung, die diese Schwachstelle ausnutzt, entsteht eine Gefährdung. „Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt.“ sagt das BSI in seinem Glossar (2021c).

2.9 Risiko

Die ISO-Definition gemäß dem ISO/IEC Guide für den Begriff *Risiko* lautet: „Risiko ist die Auswirkung von Ungewissheit auf Ziele“ (2009, S. 73). Dies impliziert sowohl positive als auch negative Aspekte. Für den Kontext der Informationssicherheit ist eine engere Begriffsfassung zweckmäßiger. Dabei werden lediglich die zu Verlusten führenden negativen Abweichungen betrachtet (Königs, 2017, S. 14). Eckert definiert Risiko als „…Wahrscheinlichkeit (oder negative Häufigkeit) des Eintritts eines Schadensereignisses und die Höhe des potenziellen Schadens, der dadurch hervorgerufen werden kann.“ (2018, S. 17). Risiko ist somit eine Art „Produkt“ von Eintrittswahrscheinlichkeit einer relevanten Gefährdung und der Größe der Auswirkung (BSI, 2021c).

Anhand von zwei Beispielen wird der Zusammenhang der Begriffe Bedrohung, Schwachstelle, Gefährdung und Risiko verdeutlicht:

Die Existenz von Verschlüsselungstrojanern im Internet ist eine Bedrohung. Eine fehlerhafte Programmierung im Internetbrowser stellt eine Schwachstelle dar. Nutzt der Trojaner diese Schwachstelle aus, um auf den Computer zu gelangen, entsteht daraus eine Gefährdung. Dass dies passiert, ist sehr wahrscheinlich, der zu erwartende Schaden durch Verschlüsselung aller Daten ist beträchtlich oder gar existenzbedrohend. Somit ergibt sich ein sehr hohes Risiko einer Datenverschlüsselung durch einen Trojaner.

Ein Feuer stellt eine Bedrohung dar. Das Versäumnis, geeignete Brandmelder im Serverraum zu installieren ist eine Schwachstelle. Bricht ein Feuer unbemerkt aus, kann dieses wegen der fehlenden Brandmeldeanlage sehr lange auf die IT-Systeme im Raum einwirken. Die Bedrohung wird zur Gefährdung. Der Ausbruch eines Feuers wird als unwahrscheinlich eingeschätzt, die Auswirkung jedoch als beträchtlich. Regelmäßige Datensicherungen in einem anderen Brandabschnitt sind vorhanden, die Wiederherstellung der IT-Systeme würde jedoch viel Zeit in Anspruch nehmen. Insgesamt ergibt sich ein mittleres Risiko, einen Schaden durch ein Feuer zu erleiden.

Aus den zwei Beispielen könnten diese Anforderungen abgeleitet werden:

- regelmäßige Installation von Sicherheitsupdates auf den Computern
- Konzeption und Installation einer Brandmelde- und Löschanlage

Die erste Maßnahme verringert die Eintrittshäufigkeit, Opfer eines Verschlüsselungstrojaners zu werden. Die Brandmeldeanlage verringert die Schadensauswirkung eines Feuers durch rechtzeitiges Alarmieren und Einleiten von Gegenmaßnahmen wie zum Beispiel Löschen durch eine Halogenlöschanlage. In beiden Fällen wird das „Produkt“ *Risiko* verkleinert.

2.10 Wert der IT in Behörden

Der Wert von Informationstechnik wird meist erst dann sichtbar, wenn sie ausfällt. Auch Behörden können längst nicht mehr einfach in Papier weiterarbeiten. Dies spiegelt sich im 2019 veröffentlichten *Masterplan „Digitale Verwaltung Sachsen“* wider. Er zielt auf die Digitalisierung der öffentlichen Verwaltung sowohl aus Sicht der Bürger als auch aus Sicht der Verwaltung ab. Dabei sollen „Alle Verwaltungsverfahren […] so weit als möglich innerhalb der Verwaltung durchgängig elektronisch bearbeitet werden.“ (Sächsische Staatskanzlei, 2019, S. 7). Damit unterstreicht der Masterplan die bereits 2014 gefassten Ziele der *Strategie für IT und E-Government des Freistaates Sachsen* des Sächsischen Staatsministerium der Justiz und für Europa u. a.*:*

- Medienbruchfreie elektronische Zusammenarbeit
- Arbeit von unterwegs und zu Hause aus
- vollständige elektronische Abwicklung von Verwaltungsakten
- mit umfassender Informationssicherheit und Datenschutz (2014, 10-16)

Das damals gesetzte Ziel der einheitlichen elektronischen Vorgangsbearbeitung und Aktenführung mit eVA.SAX (SMJ, 2014, S. 17) ist mittlerweile nahezu vollständig umgesetzt.

Die Optimierung der Verwaltung hin zu automatisierten Erlassen von Verwaltungsakten und elektronischen Bekanntgaben benötigt neben optimierten Prozessen eine leistungsfähige IT (Sächsische Staatskanzlei, 2019, 8-15).

Eine derart bedeutende und leistungsfähige Arbeitsbasis muss jedoch auch umfassend geschützt werden (SMJ, 2014, S. 33).

3 Standards und Normen

Sehr hilfreich für die Bearbeitung des komplexen Themas Informationssicherheit sind Normen, Rahmenwerke und „De-facto-Standards“. Diese entstehen aus „Best-Practices“ eines breiten Fachpublikums. Dessen Vorgehensweisen, Maßnahmen und Umsetzungen haben sich in der Praxis bewährt und empfehlen sich zur Nachahmung oder wurden zu offiziellen Normen. Die folgende Aufzählung ist nicht abschließend, zeigt aber u. a. die wichtigsten Standards auf (Grünendahl et al., 2017, S. 16). Nach welchem Standard vorgegangen wird, hängt stark von der Institution und äußeren Einflüssen ab:

- welche Kundenanforderungen gibt es?
- welche kompatiblen Standards werden bereits eingesetzt?
- erfordern Gesetze bestimmte Standards? (Königs, 2017, S. 197)

3.1 ISO 27001

Die ISO 27001 ist die Hauptnorm einer ganzen Normreihe, der ISO 27000. Sie reicht, Stand 2022, mit vielen Lücken in der Nummerierung von der ISO 27000 bis zur ISO 27799. Die Normreihe basiert auf der älteren BS 7790 der British Standards Institution, nicht zu verwechseln mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI). Die für den allgemeinen Aufbau eines Informationssicherheitsmanagementsystems (ISMS), sowie geeignete Maßnahmen relevanten Normen ISO 27000 bis ISO 27008 sind in Tabelle 1 aufgeführt. Weitere Normen der Reihe zielen auf spezifische Branchen oder Bereiche ab. Die Reihe hat den Charakter einer Meta-Norm und enthält allgemein gehaltene Anforderungen und Maßnahmen an ein ISMS. Die Ausführungen sind abstrakt und ohne technische Konkretisierung. (Kersten et al., 2020, S. 3; Königs, 2017, S. 199–213)

Norm	Inhalt
ISO 27000	Überblick und Begriffe
ISO 27001	ISMS-Anforderungen
ISO 27002	Leitfaden für Maßnahmen
ISO 27003	Anleitung zur Umsetzung
ISO 27004	Messen der ISMS-Leistung
ISO 27005	Risikomanagement
ISO 27007	Auditierung des ISMS
ISO 27008	Auditierung technischer Maßnahmen

Tabelle 1: Inhalt der Normreihe ISO 27000 nach Kersten et al., 2020

3.2 COBIT

COBIT (früher auch Control Objectives for Information and Related Technology) ist ein Rahmenwerk, mit dem die IT aus Unternehmenssicht gesteuert wird. Dabei sind die Unternehmensziele, die Wertschöpfung der IT, Metriken und das Management von IT-Risiken im Fokus. Die Ziele des Unternehmens werden dabei auf IT-Ziele und Prozesse heruntergebrochen, welche die Erreichung der Unternehmensziele unterstützen. Die Datensicherheit und die Verfügbarkeit von Daten spiegeln dabei Teilbereiche der Informationssicherheit wider. Das COBIT-Rahmenwerk formuliert Prozesse allgemein. Zur praktischen Umsetzung werden weitere Methoden benötigt. (Grünendahl et al., 2017, S. 15–16)

3.3 ISO/IEC 15408 Common Criteria

Die Common Criteria wurden aus mehreren multinationalen Normen entwickelt (Königs, 2017, S. 230). Sie stellen einen Nachweis dar, dass ein IT-Produkt einem bestimmten Sicherheitsniveau entspricht. Ziel ist, dass IT-Produkte, welche sehr häufig eingesetzt werden, bei einem Angriff nicht zu globalen Bedrohungsszenarien führen. Dazu definieren die Common Criteria unterschiedliche Anforderungen an ein IT-System bzw. eine Software. Sie bietet damit auch einen Anforderungskatalog bei der Entwicklung eines IT-Systems. Durch die Evaluation eines IT-Systems nach Common Criteria soll Vertrauen in die Sicherheit des Produktes geschaffen werden.

Das Untersuchungsergebnis wird in 7 Stufen bewertet. Je höher die Stufe desto aufwendiger und komplexer ist die Untersuchung. Aus diesem Grund wird meist nur bis zur Stufe 4 untersucht. (Königs, 2017, S. 232–234)

3.4 ITIL

Aus der IT Infrastructure Library können Best Practices für ein prozessorientiertes Service-Management für IT-Dienstleistungen entnommen werden. Die beschriebenen Prozesse zielen auf einen kontinuierlichen und integrierten Zyklus der Planung, Implementierung, Betrieb und Überwachung von IT-Dienstleistungen ab. Insbesondere externe Anbieter und Kunden solcher Dienste profitieren von festgeschriebenen verlässlichen Prozessen. Zur Zertifizierung dieser Maßnahmen wird die ISO/IEC 20000 herangezogen. Diese definiert Muss-Anforderungen an die Verwaltung der Dienste. Ein Baustein davon sind auch Anforderungen an ein Informationssicherheitsmanagement. (Grünendahl et al., 2017, S. 16, 2017, S. 16)

3.5 BSI 200

Die BSI 200-Reihe ist ein Defacto-Standard des Bundesamtes für Sicherheit in der Informationstechnologie – BSI. Sie ist ursprünglich entstanden, um deutschen Behörden und Unternehmen eine praxisnahe Methode zur Umsetzung der Informationssicherheit an die Hand zu geben (BSI, 2020, S. 6). In der aktuellen Fassung ist der „Standard“ des BSI kompatibel mit der ISO 27000 Reihe. Er untersetzt die allgemein gehaltenen Anforderungen der ISO 27000 mit konkreten Maßnahmen, Empfehlungen und Best-Practices. Hervorzuheben ist, dass im BSI 200 bereits ein Großteil der nötigen Vorarbeit erbracht wurde. So sind Risikobetrachtung, Abgrenzung, Anforderungen sowie Handlungsleitfäden für eine Absicherung mit normalem Schutzbedarf in konkreter Ausprägung enthalten. Nur für Objekte mit höherem Schutzbedarf sind eine Risikoanalyse und Erarbeitung weiterer Maßnahmen durchzuführen (BSI, 2017b, S. 15). Für die Risikoanalyse bietet der BSI 200-3 eine Methodik an. Eine Zertifizierung erfolgt für den BSI 200-2, der sogenannten IT-Grundschutz-Methodik. BSI 200-1 beschreibt den Aufbau eines Informationssicherheitsmanagementsystems. Da der IT-Grundschutz auf dem ISO 27001 basiert, ist eine Zertifizierung nach IT-Grundschutz gleichzeitig eine Zertifizierung nach ISO 27001 (BSI, 2017b, S. 8).

3.6 Gesetze

Bestimmte Institutionen sind durch den Gesetzgeber verpflichtet Informationssicherheit herzustellen und aufrecht zu erhalten. So gibt es für Banken den § 25, Abs. 1 KWG. Einrichtungen, die als kritische Infrastruktur (KRITIS) identifiziert wurden, müssen laut § 8a, Abs. 1 BSIG organisatorische und technische Vorkehrungen im Sinne der Informationssicherheit umsetzen. Für sächsische Landesbehörden sind u. a. das Sächsische E-Government-Gesetz (SächsEGovG), das Onlinezugangsgesetzt (OZG) und das sächsische Gesetz zur Informationssicherheit (SächsISichG) einschlägig.

Der Freistaat Sachsen verpflichtet nach § 2 SächsISichG, mit wenigen Ausnahmen, alle sächsischen Behörden, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts zur Gewährleistung der Informationssicherheit. Dabei soll das jeweils geltende IT-Grundschutz-Kompendium des BSI Berücksichtigung finden (§ 4 SächsISichG). Die § 7 und § 14 SächsISichG fordern u. a. die Ernennung eines Beauftragten für Informationssicherheit, die Errichtung eines Informationssicherheitsmanagementsystems, die Erstellung eines Sicherheitskonzeptes sowie dessen regelmäßige Revision.

4 Vorstellung LASuV

Das Landesamt für Straßenbau und Verkehr (LASuV) – wurde 2012 gegründet und ist aus dem Autobahnamt Sachsen sowie den sächsischen Straßenbauämtern Bautzen, Leipzig, Meißen, Meißen-Dresden, Plauen, Chemnitz und Döbeln hervorgegangen. Ziel der Neugründung war eine Zentralisierung der Organisation, Vereinheitlichung von Verwaltungsabläufen, Verschlankung der Belegschaft, Abbau redundanter Organisationseinheiten und eine bessere Zusammenarbeit.
Die Zentrale des LASuV befindet sich in Dresden und übernimmt steuernde und weisende Aufgaben gegenüber ihren fünf Niederlassungen in Bautzen, Leipzig, Meißen, Plauen und Zschopau (Sitz Chemnitz). Im Zuge der Verwaltungsreform 2012 wurden außerdem Aufgaben mit Verkehrsrelevanz mitsamt den mit diesen Aufgaben betrauten Mitarbeitern aus den drei Landesdirektionen ins LASuV eingegliedert. Zuständige Aufsichtsbehörde ist das Sächsische Staatsministerium für Wirtschaft, Arbeit und Verkehr (SMWA). Rechenschaftsbehörde über den Haushalt des LASuV ist der Landesrechnungshof, welcher regelmäßig Stichprobenkontrollen in verschiedenen Organisationseinheiten das LASuV durchführt. (LASuV, 2020)
Organisatorisch sind sowohl Zentrale als auch die Niederlassungen, denen die Amtspräsidentin bzw. die Niederlassungsleiter vorstehen, in vier bzw. drei Abteilungen aufgegliedert. Hinzu kommen eine Controllingstelle und die Innenrevision, welche jeweils direkt der Präsidentin unterstehen. Die einzelnen Abteilungen sind in Fachreferate unterteilt, die ihre jeweiligen „Spiegelreferate“ in den Niederlassungen anweisen. Große Fachreferate mit mehreren abgegrenzten Zuständigkeiten sind nochmals in Sachgebiete unterteilt. Jeder Organisationseinheit steht ein Leiter in Form des Abteilungsleiters, des Referatsleiters und bei großen Referaten dem Sachgebietsleiter vor. Abbildung 1 zeigt ein stark vereinfachtes Organigramm der LASuV Zentrale. (LASuV, 2020)
2018 wurde die Autobahn GmbH des Bundes gegründet. Diese übernahm von allen Bundesländern Planung, Bau und Instandhaltung der Bundesautobahnen. Somit ist das LASuV nur noch für alle Bundes- und Staatsstraßen des Freistaates Sachsen zuständig.

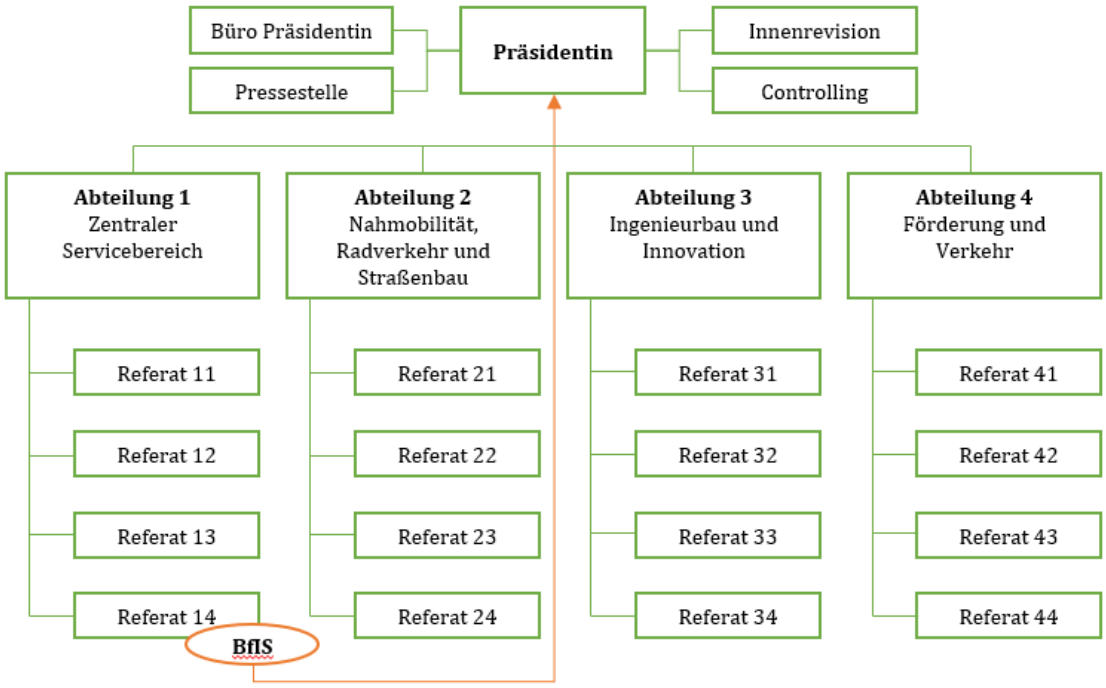

Abbildung 1: vereinfachtes Organigramm der LASuV Zentrale

4.1 Rahmenbedingungen der IT im LASuV

Jeder Standort des LASuV hat seine eigene IT – hier IuK genannt. Diese ist jeweils als Teil des Referates 14 (Organisation, IuK, Innerer Dienst und Registratur) bzw. Referates 12 (Organisation, Haushalt und IuK) der Niederlassungen eingegliedert und grundsätzlich nur für den eigenen Standort zuständig. Bereits vor der Gründung des LASuV aus den Straßenbauämtern, wurde eine kollegiale und in Teilbereichen kooperative Zusammenarbeit gepflegt. Diese Zusammenarbeit wurde mit LASuV-Gründung intensiviert. Für technische Belange hat die Zentrale Weisungsbefugnis und treibt damit die Homogenisierung der IT-Landschaft voran.

Wie jede Landesbehörde Sachsens ist auch das LASuV am Sächsischen Verwaltungsnetz (SVN) angeschlossen. Dieses stellt über Proxyserver den einzigen Internetzugang dar. Das Sächsische Verwaltungsnetz wird durch den staatseigenen Betrieb SID – Sächsische Informatik Dienste – betrieben. Der SID fungiert auch als Dienstleister für zentrale Netzwerkdienste wie Active Directory, Exchange, Webserver, Telefonie, Routing und Firewall (SID, 2018). Darüber hinaus können weitere Fachverfahren hinzugebucht werden. Nach VwV SID, Abs. 3 gilt für einige Fachverfahren ein Kontrahierungszwang, d.h. alternative Anbieter bzw.

Technologien sind nicht gestattet. Für die Informationssicherheit solcher zentralen Dienste ist der SID bis zur Schnittstelle der nutzenden Behörde zuständig.

Zusätzlich existiert die landeseigene LISt GmbH, die Gesellschaft für Verkehrswesen und ingenieurtechnische Dienstleistungen mbH. Diese bietet neben den hauptsächlichen Straßenbaudiensten auch IT-Verfahren mit Straßenbaubezug, wie GIS-Systeme, Straßendatenbanken und Abrechnungsverfahren an (LISt GmbH, 2017). Viele dieser Dienste werden durch das LASuV genutzt, dabei kommt eine LISt-eigene Citrix-Farm zum Einsatz.

Die Hausnetzte der LASuV-Standorte werden als Teil des SVN durch den SID betrieben. Eine direkte Administration der Netzwerkkomponenten ist der LASuV-IuK somit nicht möglich.
Im Zuge der Homogenisierung der LASuV-IuK konnten bereits viele Verfahren vereinheitlicht werden. So existieren eine gemeinsame Virtualisierungsplattform für Server, eine einheitliche Client-Plattform sowie zentral betriebene Softwareverteilung, Antiviruslösung und Beschaffung.

Die Arbeitsweise der LASuV-IuK ist bisher eher bedarfsgetrieben. Die Einführung von Fachverfahren, Konfiguration von Systemen sowie strategische Ausrichtungen laufen häufig auf Zuruf oder informellen Abstimmungen. Eine konzeptgetriebene Arbeitsweise konnte bisher nicht etabliert werden. Dies stellt bei der zunehmenden Komplexität von Systemen auch in Hinblick auf Sicherheitskonfigurationen ein Problem dar. Zuletzt wurde beschlossen, die eigene Arbeitsweise auf zu erstellende und niedergeschriebene Konzepte zu stützen.

4.2 Stand Informationssicherheitsprozess

Die Amtsleitung des LASuV hat eine Beauftragte für Informationssicherheit benannt. Ein Stellvertreter, wie im Sächsischen Informationssicherheitsgesetz § 7 gefordert, wurde bisher nicht benannt. Die Beauftragte hat gleichzeitig die Position der Sachgebietsleiterin der IuK Zentrale inne und damit die technische Weisungsbefugnis gegenüber der IuK der Niederlassungen. Dies kann einen Interessenskonflikt bergen. Bei der Entscheidung zu Sicherheitsmaßnahmen könnten Maßnahmen ergriffen werden, welche den Komfort der Systemadministration nicht zu stark verringern, jedoch die Sicherheit nicht effektiv genug erhöhen. Wie in Abbildung 1 erkennbar, berichtet die BfIS direkt gegenüber

der Präsidentin, ist aber gleichzeitig den Weisungen des Referatsleiters und des Abteilungsleiters 1 unterworfen.
In der ersten Recherche wurde dargestellt, dass das LASuV keine Informationssicherheitsleitlinie aufgestellt hat. Nach weiteren Recherchen ergab sich, dass das übergeordnete Staatsministerium für Wirtschaft, Arbeit und Verkehr (SMWA) bereits 2012 eine solche Leitlinie aufgestellt hat. Diese gilt auch für das LASuV. Dem LASuV wird darin das Recht zugebilligt, Sicherheitsziele zu präzisieren und die Wahl der Mittel frei zu wählen, Regelungen dürfen aber nach Abs 3.5 VwV Leitlinie Informationssicherheit SMWA nicht den Vorgaben des SMWA widersprechen. Von diesem Recht wurde bisher kein Gebrauch gemacht.

Die Initiierung eines Informationssicherheitsmanagementsystems nach § 4 Abs. 1 SächsISichG wurde bisher nicht durchgeführt. Die Verantwortungsübernahme der Amtsleitung für die Informationssicherheit sowie regelmäßige Berichte zwischen Amtsleitung und BfIS fanden bisher nicht statt. Im Jahr 2012 wurde ein Sicherheitskonzept durch die LISt GmbH aufgestellt. Dieses basiert auf dem veralteten BSI-100 Standard und wurde nie mit konkreten Maßnahmen untersetzt. Insgesamt fehlte Zeit, um konzeptionelle Arbeiten zur Stärkung der Informationssicherheit durchzuführen.

Ziel dieser Arbeit ist, trotz der benannten Rahmenbedingungen, einen Einstieg in den IT-Grundschutz für das LASuV zu erarbeiten.

5 IT-Grundschutz-Methodik

Wie in der Einleitung dargestellt, kommen auf IT-Systeme immer mehr Gefahren zu. Das Onlinezugangsgesetz verpflichtet Behörden zur Digitalisierung ihrer Bürgerdienste. Aber auch Institutionen ohne direkte Bürgerdienste werden durch immer komplexere IT-Systeme mit potenziell immer mehr Sicherheitslücken zur Zielscheibe von Angriffen. Die hohe Durchdringung und Vernetzung von Systemen führt zu Abhängigkeiten der Geschäftsprozesse von diesen Systemen. (Allianz ACGS, 2022)

Um dieses komplexe Geflecht umfassend und strukturiert gesichert betreiben zu können, ist ein konzeptionelles und methodisches Vorgehen notwendig. Das BSI hat hierfür die BSI-200 Standards und das IT-Grundschutzkompendium entwickelt. Teil des Standards ist die Grundschutzmethodik. Sie ermöglicht, dass Institutionen nach bewährten Methoden und „Best-Practices“ vorgehen. Die Vorarbeiten des BSI sparen Zeit und stellen eine möglichst umfassende Betrachtung durch Expertenwissen zur Verfügung. Die BSI-Standards sind eine Umsetzung der ISO 27000 Normreihe und untersetzt die allgemein gehaltene Norm mit konkreten Anforderungen und teilweise mit Umsetzungshinweisen (BSI, 2017a, S. 11). Dies ermöglicht eine schnellere und praxisorientierte Umsetzung eines Informationssicherheitsprozesses. Adressaten der BSI-Standards sind kleine und mittlere Unternehmen, Einrichtungen und Behörden. Für Kleinstunternehmen sollten vereinfachte Methoden herangezogen werden (BSI, 2021e).

Darüber hinaus können Institutionen ihre umgesetzte Informationssicherheit durch eine Zertifizierung überprüfen und nach außen darstellen lassen. Eine BSI-Zertifizierung findet im europäischen und auch internationalen Bereich große Akzeptanz (BSI, 2021d). Grund ist unter anderem, dass eine BSI-Zertifizierung gleichzeitig eine Zertifizierung nach ISO 27001 darstellt. (BSI, 2017b, S. 8)

5.1 Aufbau des IT-Grundschutz

Der IT-Grundschutz des BSI bildet eine thematische Zusammenstellung. Ziel ist eine ganzheitliche und erprobte Betrachtung, um Informationssicherheit zu etablieren und zu erhalten. Dabei versteht sich der IT-Grundschutz als Standard, Vorgehensmodell und praktische Umsetzungshilfe in Einem (BSI, 2021d).

Bestandteile sind vier BSI-Standards, das IT-Grundschutz-Kompendium mit seinen Bausteinen, Grundschutz-Profile und ein Zertifizierungsprozess. Ergänzend kommen Umsetzungshinweise und ein Online-Kurs hinzu.

5.1.1 Managementsysteme für Informationssicherheit – BSI 200-1

Fundament sind die BSI-Standards 200-1, 200-2, 200-3 und derzeit noch 100-4. Der Standard 100-4 wird demnächst vom 200-4 abgelöst. BSI 200-1 „Managementsysteme für Informationssicherheit (ISMS)“ beschreibt wie ein Informationssicherheitsmanagementsystem aussehen sollte, welche Komponenten und Prozesse enthalten sein sollen und welche Aufgaben dabei die Managementebene übernehmen muss. Es wird dargestellt, dass ein ISMS dauerhaft Ressourcen, Mitarbeiter und eine Strategie benötigen (BSI, 2017a, S. 14). Herausgestellt wird die Verantwortung der Leitungsebene für die Informationssicherheit. Auch bei Ernennung eines Beauftragten für Informationssicherheit verbleibt die Gesamtverantwortung bei der Leitungsebene. Die Leitungsebene muss eine Strategie zur Informationssicherheit erarbeiten, kommunizieren und anpassen (BSI, 2017a, S. 19). Dabei muss eine Informationssicherheitsleitlinie erarbeitet werden, die zur Gesamtstrategie und zur Risikoneigung der Institution passt (BSI, 2017b, S. 32). In der Leitlinie wird dargestellt, mit welchen Mitteln und Organisationsstrukturen die Informationssicherheit hergestellt werden soll und für welchen Geschäftsbereich sie Gültigkeit hat. Bei Änderungen der Geschäftstätigkeit, der Risikoneigung, der IT-Strategie oder der Sicherheitslage, jedoch spätestens aller 2 Jahre, wird die Anpassung der Leitlinie empfohlen. Welche Dokumentationen, Rollen und Prozesse benötigt werden, beschreiben Kapitel 4 und 5 des BSI 200-1.
Der Sicherheitsprozess wird als Querschnittsprozess dargestellt, der in allen wesentlichen Geschäftstätigkeiten einzubeziehen ist. Die Aufrechterhaltung der Informationssicherheit ist ein fortlaufender Prozess der ständigen Anpassungen, Revisionen und der der Kontrolle durch die Leitungsebene unterworfen ist. (BSI, 2017a, S. 19–20)

5.1.2 IT-Grundschutz-Methodik – BSI 200-2

Die „IT-Grundschutz-Methodik“, das konkrete Vorgehen, beschreibt der BSI-Standard 200-2. Zuerst wird auf die Initiierung des Sicherheitsprozesses eingegangen. Kapitel 3 und 4 formulieren die Konzeption und den Aufbau einer Informationssicherheitsorganisation. Für das weitere Vorgehen muss die Entscheidung für die Vorgehensweise gefällt werden. Die IT-Grundschutz-Methodik ermöglicht auf drei Wegen die Etablierung von Informationssicherheit. Die Basis-, Kern- und Standardabsicherung. (BSI, 2017b, S. 13–14)

Basisabsicherung

Die Basisabsicherung ist ausschließlich als Einstieg gedacht. Sie soll ein möglichst breit und relativ einfach erreichbares Grundniveau an Informationssicherheit herstellen. Die geforderten Maßnahmen und Umsetzungen zielen darauf ab, die größten Risiken zu senken. Eine umfassende Absicherung auf dem Stand der Technik stellt dies nicht dar. Der nächste Schritt muss der Ausbau hin zur Standardabsicherung sein. Als Zwischenschritt kann die Kernabsicherung für besonders gefährdete Geschäftsprozesse durgeführt werden. Eine Zertifizierung der Basisabsicherung ist nicht möglich (BSI, 2017a, S. 38). Die Basisabsicherung kann sowohl für die gesamte Institution als auch für bestimmte Geschäftsbereiche oder zusammenhängende Prozesse gelten. (BSI, 2017b, S. 28)

Empfehlenswert ist die Basisabsicherung nach BSI 200-2 (2017b, S. 28), wenn:

- die Umsetzung zur Informationssicherheit noch am Anfang steht
- kein erhöhtes Gefährdungspotential für Geschäftsprozesse besteht
- das angestrebte Sicherheitsniveau normal ist
- die Zerstörung, Diebstahl oder die Kompromittierung von Assets für die Institution nicht existenzgefährdend sind
- kleinere Sicherheitsvorfälle toleriert werden können bzw. auffangbaren Schaden verursachen

Notwenige Schritte sind:

1. Ersterfassung vorhandener Assets als Übersicht
2. Festlegung des Informationsverbundes. Soll die Basisabsicherung für die gesamte Institution oder bestimmte Geschäftsbereiche gelten?
3. Modellierung. Nachbau des Informationsverbundes mithilfe der Bausteine des IT-Grundschutz-Kompendiums
4. IT-Grundschutz-Check. Soll-Ist-Vergleich auf umgesetzte Basismaßnahmen

5. Auswahl und Umsetzung von Maßnahmen, die bisher nicht umgesetzt wurden
6. Entscheidung zum Ausbau nach Kern- oder Standardabsicherung (BSI, 2017b, S. 60–61)

Kernabsicherung

Besitzt eine Institution Assets, deren Verlust die Existenz der Institution bedrohen oder ist das Geschäftsmodel bei Ausfall bestimmter Prozesse besonders gefährdet, kann eine Kernabsicherung diese sogenannten Kronjuwelen rasch schützen. Die wichtigsten Assets werden dabei abgesichert, indem Basis-, Standard- und erweiterte Maßnahmen auf diesen eng abgegrenzten Informationsverbund angewandt werden. Da solche wichtigen Assets meist einen hohen Schutzbedarf aufweisen, wird zusätzlich eine Risikoanalyse durchgeführt, um weitere Anforderungen und Maßnahmen ableiten zu können. Um die Absicherung der wichtigen Assets aufrechtzuerhalten, muss für diesen abgegrenzten Informationsverbund bereits ein kontinuierlicher Revisionsprozess stattfinden. Ergriffene Maßnahmen müssen auf Wirksamkeit, Aktualität und Angemessenheit überprüft und verbessert werden (BSI, 2017b, S. 73). Zu einem späteren Zeitpunkt kann die Informationssicherheit auf alle Ressourcen und Prozesse ausgeweitet werden, um eine Standardabsicherung zu etablieren. Die Kernabsicherung kann für den abgegrenzten Informationsverbund der Kronjuwelen nach ISO 27001 zertifiziert werden. (BSI, 2017b, S. 28–29)

Die Kernabsicherung empfiehlt sich laut BSI (2017b, S. 28), wenn:

- die Anzahl der Assets mit hohem oder sehr hohem Schutzbedarf überschaubar ist
- diese Assets und Prozesse zügig identifiziert werden können und eindeutig abgrenzbar sind
- eine Zerstörung oder Kompromittierung dieser Assets existenzbedrohend sind
- kleinere Sicherheitsvorfälle toleriert werden können bzw. auffangbaren Schaden verursachen

Notwenige Schritte nach BSI-Standard 200-2 (BSI, 2017b, S. 68) sind:

1. Festlegung des Informationsverbundes. Dieser sollte möglichst klein sein und die kritischen Assets enthalten
2. Benennung der kritischen Geschäftsprozesse (Kronjuwelen)

3. Strukturanalyse des Informationsverbundes. Darstellung der Abhängigkeiten
4. Schutzbedarfsfeststellung der Kronjuwelen und weiterer Assets im Informationsverbund
5. Modellierung. Nachbau des Informationsverbundes mithilfe der Bausteine des IT-Grundschutz-Kompendiums. Auswahl und Anpassung von Anforderungen
6. IT-Grundschutz-Check. Soll-Ist-Vergleich auf umgesetzte Maßnahmen
7. Risikoanalyse und Ableitung weiterer Maßnahmen
8. Auswahl und Umsetzung von Maßnahmen, die bisher nicht umgesetzt wurden
9. Kontinuierlicher Prozess zur Verbesserung der Kernabsicherung
10. Entscheidung zum Ausbau nach Standardabsicherung

Standardabsicherung

Um umfassende und tiefgehende Informationssicherheit zu etablieren, müssen alle Assets und Geschäftsprozesse des definierten Informationsverbundes betrachtet und abgesichert werden. Die Standardabsicherung ist auch das Ziel bei Einstiegen über die Basis- oder Kernabsicherung. Zum Erreichen der Standardabsicherung müssen zunächst alle Assets erfasst werden. Hierbei können vorhandene Listen und Übersichten eine wertvolle Quelle sein. Um die Komplexität nicht unnötig zu erhöhen, sollten an diesem Punkt Assets als Gruppen zusammengefasst werden. Merkmale zur Gruppenbildung können sein:

- gleicher Typ
- ähnliche Aufgaben
- ähnliche Rahmenbedingungen
- gleicher Schutzbedarf
- gleiche Netzanbindung
- ähnliche Konfiguration
- ähnliche Anwendungen (BSI, 2017b, S. 78–79)

Assets mit hohem oder sehr hohem Schutzbedarf werden einer Risikoanalyse unterzogen. Daraus können weiteren Schutzmaßnahmen abgeleitet werden, welche nicht in den Bausteinen des IT-Grundschutz-Kompendiums genannt werden.

Die Etablierung eines kontinuierlichen Prozesses stellt die Aufrechterhaltung und Verbesserung der Standardabsicherung sicher. Für die Standardabsicherung kann die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz erlangt werden. (BSI, 2017a, S. 38, 2017b, S. 151–152)

Das BSI (2017b, S. 29) empfiehlt den direkten Einstieg in die Standardabsicherung, wenn:

- bereits der IT-Grundschutz nach BSI 100-2 zur Anwendung kommt
- ein Sicherheitskonzept nach ISO 27001 erstellt wurde
- in wesentlichen Bereichen Sicherheitsmaßnahmen bereits umgesetzt sind und die Informationssicherheit einen gewissen Reifegrad erreicht hat
- kein Handlungsbedarf besteht, einzelne wichtige Geschäftsprozesse abzusichern (siehe Kernabsicherung)
- keine Assets oder Prozesse existieren, deren Zerstörung oder Kompromittierung die Existenz der Institution gefährden
- auf lange Sicht Sicherheitsvorfälle, die den Geschäftsbetrieb beeinträchtigen, zwar die Existenz nicht bedrohen, jedoch als nicht akzeptabel angesehen werden

Notwenige Schritte nach BSI-Standard 200-2 (BSI, 2017b, S. 75) sind:

1. Festlegung des Informationsverbundes. Die gesamte Institution oder bestimmte Organisationseinheiten oder Geschäftsbereiche
2. Strukturanalyse des Informationsverbundes. Darstellung der Abhängigkeiten
3. Schutzbedarfsfeststellung der Assets im Informationsverbund
4. Modellierung. Nachbau des Informationsverbundes mithilfe der Bausteine des IT-Grundschutz-Kompendiums. Auswahl und Anpassung von Anforderungen
5. IT-Grundschutz-Check. Soll-Ist-Vergleich auf umgesetzte Maßnahmen
6. Risikoanalyse und Ableitung weiterer Maßnahmen
7. Auswahl und Umsetzung von Maßnahmen, die bisher nicht umgesetzt wurden
8. Kontinuierlicher Prozess zur Verbesserung der Kernabsicherung

Allen drei Vorgehensweisen gemein ist die Definition des Geltungsbereichs. Das Informationssicherheitskonzept kann für die gesamte Institution, einzelne Organisationseinheiten oder Geschäftsbereiche gelten. Für die Kernabsicherung soll

der Geltungsbereich möglichst eng abgegrenzt sein und dabei die besonders schützenswerten Kronjuwelen enthalten. Die klare Abgrenzung dieses so definierten Informationsverbundes kann insbesondere bei Outsourcing von Prozessen schwierig sein (BSI, 2017b, S. 30). Im Anschluss der Definition des Informationsverbundes folgt die Strukturanalyse. Für die Basisabsicherung genügt hier eine Übersicht. In der Strukturanalyse werden, ausgehend von den Prozessen, Abhängigkeiten zu anderen Prozessen, Anwendungen und IT-Systemen deutlich. Hilfreich für die Strukturanalyse kann ein Netzplan sein (BSI, 2017b, S. 26). Für die erhobenen Prozesse, Anwendungen und Systeme wird nun der Schutzbedarf erhoben. Bei der Basisabsicherung wird auf die Schutzbedarfsfeststellung verzichtet. Hier wird von einem normalen Schutzbedarf ausgegangen (BSI, 2017b, S. 28).

Es folgt die Modellierung des Informationsverbundes mithilfe der Bausteine des IT-Grundschutz-Kompendiums. Dabei werden passende Bausteine den Assets zugewiesen. Jeder Baustein enthält hierzu eine beschreibende Abgrenzung. Die Bausteine enthalten Anforderungen, deren Erfüllung die Informationssicherheit für diese Assets erhöht. Für die Basisabsicherung werden nur die Basisanforderungen herangezogen. Für Assets mit normalem Schutzbedarf zusätzlich die Standardanforderungen und für Objekte mit erhöhtem Schutzbedarf wie auch für die Kronjuwelen aus der Kernabsicherung müssen zusätzlich die erweiterten Anforderungen erfüllt sein. Durch die Zuordnung der Bausteine zu den Assets wird deutlich, welche Anforderungen für ein konkretes Objekt zu erfüllen sind. Um festzustellen, welche der Anforderungen bereits voll, teilweise oder noch nicht erfüllt sind, wird der sogenannte IT-Grundschutz-Check durchgeführt. Dies ist ein Soll-Ist-Vergleich, welcher zum Beispiel in Form eines Interviews, einer Dokumentensichtung oder einer Begehung erfolgen kann. Assets mit erhöhtem Schutzbedarf bedürfen einer Risikoanalyse, da die erweiterten Anforderungen aus den zugeordneten Bausteinen nicht abschließend sind. Aus der Risikoanalyse werden Risiken für besonders wichtige Objekte ersichtlich. Gegen diese Risiken müssen weitere Maßnahmen erarbeitet werden. Nach dieser Analyse sind die noch nicht oder nur teilweise erfüllten Anforderungen durch entsprechende Maßnahmen zu untersetzen. Dabei können die vom BSI veröffentlichten Umsetzungshinweise zu Rate gezogen werden. Für viele Bausteine gibt es solche Umsetzungshinweise, welche konkrete Maßnahmen zur Erfüllung der Anforderungen des Bausteines vorschlagen. Für andere Bausteine muss die Institution für sich passende Maßnahmen erarbeiten. (BSI, 2017b, S. 153, 2022a, S. 2–3)

5.1.3 Risikoanalyse auf der Basis von IT-Grundschutz – BSI 200-3

Wie eine „*Risikoanalyse auf der Basis von IT-Grundschutz*“ durchgeführt werden kann, zeigt der BSI-Standard 200-3. Im ersten Schritt werden aus dem IT-Grundschutz-Kompendium die Gefährdungen ermittelt, welche das betrachtete Asset direkt bedrohen können. Indirekt relevante Gefährdungen werden nicht betrachtet, da diese keine neuen Aspekte zu den direkten Gefährdungen liefern. Ggfs. können zusätzliche Gefährdungen, die nicht im IT-Grundschutz-Kompendium genannt werden, erkannt werden. (BSI, 2017c, S. 15)
Es folgt die Risikoeinschätzung mit vorher zu definierenden qualitativen oder quantitativen Kategorien der Eintrittshäufigkeit und der Schadensauswirkung. Der Vorschlag des BSI teilt die Eintrittshäufigkeit und Schadensauswirkung jeweils in vier Kategorien. Die Risikobewertung ergibt sich als Produkt von Eintrittshäufigkeit und Schadensauswirkung wie in Abbildung 2 dargestellt. Die gefundenen Risiken müssen laut BSI (2017c, S. 32–34) behandelt werden:

- Ursachen können soweit möglich ausgeschlossen werden
- Eintrittshäufigkeiten können verringert werden
- Auswirkungen können abgeschwächt werden
- finanzielle Schäden können durch eine Versicherung transferiert werden

Verbleibende Risiken und solche, bei denen sich die Institutionsleitung gegen bestimmte Maßnahmen entschieden hat, müssen bewusst akzeptiert werden. Nicht akzeptabel ist das Betreiben von Risikoignoranz. (BSI, 2017c, S. 32–34)

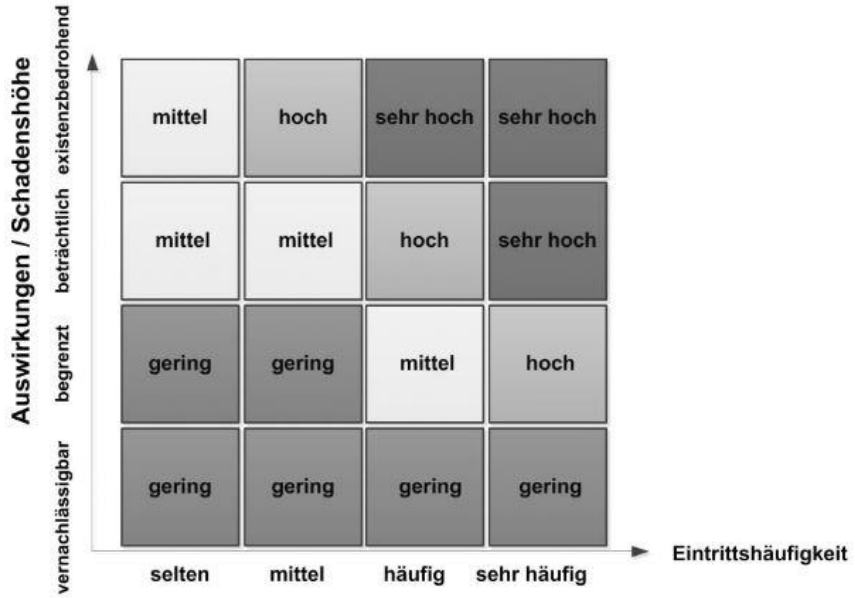

Abbildung 2: Risikobewertungsmatrix des BSI-Standard 200-3 (2017c, S. 26)

Die Risikoanalyse ist Teil des IT-Grundschutz-Checks. Alle in der Risikoanalyse zusätzlich erarbeiteten Anforderungen und Maßnahmen müssen in den Soll-Ist-Vergleich integriert werden. Das entstehende Informationssicherheitskonzept muss bei Hinzukommen neuer Maßnahmen konsolidiert werden. (BSI, 2017c, S. 38–40)

5.1.4 IT-Grundschutzkompendium

Das IT-Grundschutz-Kompendium ist neben den BSI-Standards elementarer Bestandteil des IT-Grundschutzes. Als eigenständige Monografie des BSI behandelt es die elementaren Gefährdungen und enthält alle offiziellen Bausteine mit ihren Anforderungen. Im Kompendium sind alle Gefährdungen, Bausteine und Maßnahmen mit einem eindeutigen Schlüssel, einer Art Nummerierung, versehen. Die elementaren Gefahren sind Grundlage der geforderten Maßnahmen der Bausteine. Außerdem werden die Beschreibungen während der Risikoanalyse herangezogen. Sie zeigen mögliche konkrete Gefährdungsszenarien auf, welche zur eigenen Einschätzung von Gefährdungen hilfreich sein können. Beispiele für elementare Gefährdungen aus dem IT-Grundschutz-Kompendium (2022a) sind:

- G 0.1 Feuer
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.22 Manipulation von Informationen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.39 Schadprogramme

Den Großteil des IT-Grundschutz-Kompendiums machen die Bausteine aus. Jeder Baustein beschäftigt sich mit einem spezifischen Thema oder einem spezifischen Objekt. Er enthält jeweils eine Einleitung und Abgrenzung bzw. Verweise auf andere Bausteine. Anschließend wird die Gefährdungslage durch mögliche Gefahrenszenarien verdeutlicht. Es folgen die Anforderungen für die Basisabsicherung, Anforderungen für eine Standardabsicherung mit normalem Schutzbedarf und nicht abschließende Anforderungen für Assets mit erhöhtem Schutzbedarf. Die Standardanforderungen bauen auf die Basisanforderungen auf. Für eine Standardabsicherung für Objekte mit normalem Schutzbedarf müssen sowohl Basisanforderungen als auch Standardanforderungen erfüllt sein. Wurde in der Schutzbedarfsfeststellung ein Objekt mit mindestens hohem Schutzbedarf identifiziert, gelten für dieses Objekt zusätzlich die Anforderungen für hohen

Schutzbedarf. Objekte mit hohem Schutzbedarf liegen auch bei der Kernabsicherung vor. Je nach Ergebnis der anschließenden Risikoanalyse müssen weitere Anforderungen für hohen Schutzbedarf definiert werden.
Ein Großteil der Anforderungen besteht aus Unteranforderungen, welche dazugehörige Einzelaufgaben festlegen. Die Anforderungen werden mit Modalverben formuliert. (BSI, 2017b, S. 131–133)

Modelverben

MUSS / DARF NUR:
Anforderung muss unbedingt uneingeschränkt erfüllt werden

DARF NICHT / DARF KEIN:
etwas darf in keinem Fall getan werden.

SOLLTE:
Anforderung muss normalerweise erfüllt sein. Es kann jedoch sorgfältig zu prüfende Gründe geben, die Anforderung nicht zu erfüllen. Die Gründe müssen stichhaltig dokumentiert werden.

SOLLTE NICHT / SOLLTE KEIN:
etwas sollte normalerweise nicht getan werden.
Es kann jedoch sorgfältig zu prüfende Gründe geben, die Anforderung nicht zu erfüllen. Die Gründe müssen stichhaltig dokumentiert werden. (BSI, 2022a, 5-6)

Das Modalverb SOLLTE kann dazu verleiten, dass eine Anforderung als optional angesehen wird. Tatsächlich ist SOLLTE jedoch eher mit MUSS GRUNDSÄTZLICH gleichzusetzen. Gründe für eine Nichterfüllung einer Anforderung können enormer Aufwand oder Kosten in Relation zum Sicherheitsgewinn sein. Auch wenn Anforderungen die Innovationskraft oder Marktmacht von Unternehmen nachhaltig schädigen, kann das Grund sein, Anforderungen nicht oder nur teilweise zu erfüllen. Die Entscheidung und Abwägung für diese Risikoakzeptanz muss die Leitungsebene treffen. (BSI, 2017b, S. 142–143, 2017c, S. 33–34)

Bausteine

Die Bausteine sind in Schichten gruppiert. Als oberste Schicht stehen die Bausteine, die die Errichtung eines ISMS beschreiben. Derzeit *ISMS.1 Sicherheitsmanagement.* Darunter folgen die weiteren Prozessbausteine der Kategorien *ORP – Organisation*

und Personal, *CON – Konzepte und Vorgehensweisen, OPS - Betrieb* und *DER – Detektion und Reaktion.* Diese Bausteine sind im Allgemeinen auf den ganzen Informationsverbund anzuwenden oder decken einen großen Bereich der Organisation ab. Für einzelne ggfs. gruppierte Objekt sind Systembausteine *APP - Anwendungen*, *SYS – IT-Systeme*, *IND – Industrielle IT*, *NET – Netze und Kommunikation*, sowie *INF - Infrastruktur* anzuwenden. Einige Prozessbausteine wie OPS.2.2 Cloud-Nutzung oder *OPS.3.1 Outsourcing für Dienstleister* sind jedoch pro Cloudnutzung bzw. pro Dienstleister anzuwenden. Abbildung 3 verdeutlicht die Gruppierung der Bausteine und gibt Beispiele für einzelne Bausteine. Bausteine der Kategorie *DER – Detektion und Reaktion* sind als Fundament dargestellt. Dies stellt den Übergang zu einem kontinuierlichen Prozess dar: Sind alle Maßnahmen umgesetzt, müssen Sicherheitsvorfälle detektiert, mögliche Notfallreaktionen festgelegt und Verbesserungen des ISMS vorgenommen werden. (BSI, 2022a, S. 1–2)

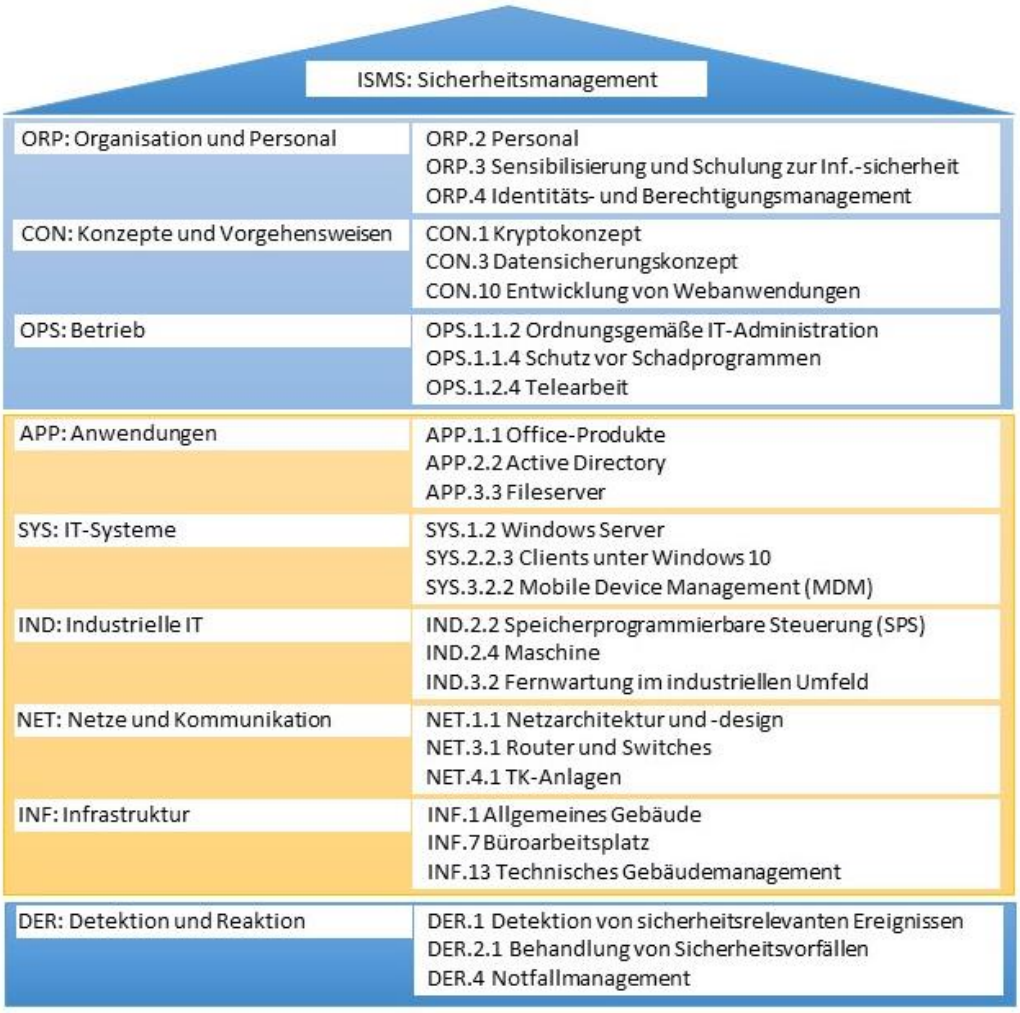

Abbildung 3: Kategorien der Bausteine als Schichtenmodell mit beispielhaften Bausteinen nach BSI (2022a)

Umsetzungshinweise
Insbesondere zu Bausteinen, welche ein eng begrenztes Thema bearbeiten, gibt es zusätzlich Umsetzungshinweise. Diese zeigen konkret auf, mit welchen Maßnahmen die Anforderungen der Bausteine erfüllt werden können. Sie richten Sich an die Personengruppe, die mit der Umsetzung beauftragt wurde. Die Umsetzungshinweise sind nicht Bestandteil des IT-Grundschutz-Kompendiums. (BSI, 2021d)

5.1.5 Business Continuity Management – BSI 100-4 / BSI 200-4

Was zu tun ist, sollte ein Schadens- oder Notfallereignis eintreten, wird strukturiert im Business Continuity Management (BCM) erarbeitet. Es soll sicherstellen, dass kritische Geschäftsprozesse einer Institution nicht unterbrochen werden oder in akzeptabler Zeit wiederhergestellt werden können. Dafür bedient sich das BCM Methoden der Prävention und der Reaktion. Diese sollen die Widerstandskraft (Resilienz) der Institution stärken. Derzeit ist noch der BSI 100-4 *Notfallmanagement* gültig. Dieser wird demnächst durch den erweiterten BSI 200-4 abgelöst. Der Standard setzt kein ISMS voraus, dennoch können beide Managementsysteme voneinander profitieren und aufeinander aufbauen. (BSI, 2021a)
Der IT-Grundschutz-Baustein *DER.4 Notfallmanagement* bildet hier die Schnittstelle zwischen beiden Standards. Auch fordert *DER.4* die Erstellung eines Notfallhandbuches, welches im Rahmen des BCM erstellt werden kann. (BSI, 2022a, S. 343)

5.2 Vorgehensweise im LASuV

Von den drei Herangehensweisen, die das BSI vorschlägt, muss eine geeignete für die vorliegende Arbeit ausgewählt werden. Für einen zeitlich begrenzten Rahmen ist eine Standardabsicherung zu umfangreich. Der zu untersuchende Informationsverbund ist zu groß und zu komplex, um von Beginn an eine umfassende Absicherung anzustreben. Möglich wäre eine Basisabsicherung für einen eng abgegrenzten Bereich. Der dabei erforderliche IT-Grundschutz-Check würde nur auf Basisanforderungen prüfen. Da eine Basisabsicherung als permanenter Prozess der Informationssicherheit nicht ausreichend ist, muss im Anschluss die Standardabsicherung angestrebt werden. Für diese müsste wiederum der IT-Grundschutz-Check für Standardanforderungen und hohe Anforderungen

durchgeführt werden. Diese doppelte Interviewführung kann umgangen werden, indem gleich die Umsetzungen aller Anforderungen abgefragt werden. Zudem kann auf diese Weise die Schutzbedarfsfeststellung zeitlich später oder zeitgleich zum IT-Grundschutz-Check erfolgen. Ein separater Workshop zur Schutzbedarfsfeststellung direkt nach der Strukturanalyse entfällt somit. Der so erhobene Ist-Zustand kann in späteren Umsetzungsprojekten für Standard- und erhöhte Maßnahmen als Grundlage dienen. Die Abfrage für alle Anforderungstypen für einen eng begrenzten Bereich ähnelt der Kernabsicherung. Da im LASuV keine spezifische Leitlinie zur Informationssicherheit vorhanden ist, sind somit auch keine Kronjuwelen benannt. Dennoch bietet die Methodik der Kernabsicherung alle Schritte für das weiteren Vorgehen. Aus diesem Grund wird in der vorliegenden Arbeit die Kernabsicherung aus der IT-Grundschutz-Methodik nach BSI 200-2 angewandt.

6 Zu untersuchender Informationsverbund

Das Landesamt für Straßenbau und Verkehr wurde mit seinem IT-spezifischen Rahmenbedingungen in Kapitel 4.1 vorgestellt. Das Verfahren der Kernabsicherung verlangt eine enge Abgrenzung des zu untersuchenden Informationsverbundes. Es wird die Annahme getroffen, dass ein Großteil der Aufgaben des LASuV IT-gestützt ausgeführt werden. Als eng abgegrenzte Prozesse werden die Personalverwaltung sowie die Gebäudeverwaltung der LASuV Zentrale ausgewählt. Diese Prozesse haben wenig direkte Verflechtungen mit anderen Prozessen und Aufgaben des LASuV und können so separat betrachtet werden. Beide Prozesse führen einen Teil ihrer Aufgaben mithilfe von Fachverfahren aus. Diese werden durch die zentrale IuK betrieben. Somit ergibt sich im weiteren Verlauf die Anwendung des IT-Grundschutzes auf diese Anwendungen und IT-Systeme. Des Weiteren wird nur die Zentrale des LASuV betrachtet. Die Spiegelreferate der Niederlassungen haben ähnliche Aufgaben, werden im Rahmen dieser Arbeit aber nicht einbezogen.

6.1 Ersterfassung

Mithilfe der Ersterfassung soll ein grober Überblick über die Institution gewonnen werden (BSI, 2017b, S. 80). Für das LASuV wurden dazu bereits vorhandene Listen und Aufstellungen gesichtet. Das Organigramm in Abbildung 1 verdeutlicht den strukturellen Zusammenhang der einzelnen Organisationeinheiten und die Weisungsbefugnisse. Im Geschäftsverteilungsplan sind für jede Organisations-einheit die Aufgaben aufgestellt. Eine Prozesslandkarte ist im LASuV nicht vorhanden. Ein Verfahrensverzeichnis listet einen Großteil der eingesetzten Software auf. Insbesondere für die Institution bedeutsame Fachverfahren sind hier enthalten. Das Verfahrensverzeichnis benennt teilweise den Fachverantwortlichen und enthält eine Schutzbedarfseinschätzung. Die Schutzbedarfseinschätzung ist eine Einschätzung der Beauftragten für Informationssicherheit ohne Anwendung einer Schutzbedarfsdefinition. Die Einschätzung kann damit nur als erste Orientierung dienen. Die Tabelle 2 zeigt Ausschnitte des Verfahrensverzeichnisses. Das vorhandene Informationssicherheitskonzept auf Basis BSI 100-2 ist aus dem Jahr 2012. Aufgrund der seitdem bereits stark fortentwickelten IT-Landschaft und der Weiterentwicklung des BSI-Standards konnte dieses nicht als Basis zur Fortschreibung genutzt werden. Aus dem Geschäftsverteilungsplan des LASuV konnte entnommen werden, dass das Referat 11 – Personal grundsätzlich für die

Personalverwaltung zuständig ist. Teil des Referates 14 ist das Sachgebiet Innerer Dienst. Dieses ist Ansprechpartner für die Gebäudeverwaltung. Für den Betrieb der IT-Systeme und Fachanwendungen ist das Sachgebiet IuK des Referates 14 der Zentrale zuständig.

Bezeichnung	unterstützte Verwaltungsaufgabe	bedeutsam	datenschutz relevant	Schutzbedarf Vertraulich-keit	Schutzbedarf Verfügbarkeit	Schutzbedarf Integrität	ressortüber greifend
CSBF	Vergabemeldungen an den Bund	ja	nein	normal	normal	normal	nein
eANV/ZEDAL	Elektronische Nachweisführung für gefährliche und nicht gefährliche Abfälle	ja	nein	normal	normal	normal	nein
Ebble	Entschädigungsbewertung bei Landentzug	nein	ja	hoch	normal	hoch	nein
Elektronisches Grundbuch	Auskunftsystem	ja	ja	hoch	normal	hoch	nein

Tabelle 2: Ausschnitte des Verfahrensverzeichnisses mit Schutzbedarfsabschätzung

6.2 Strukturanalyse der Prozesse

Aus dem Geschäftsverteilungsplan wurden die Teilaufgaben der in Kapitel 6 genannten Organisationseinheiten betrachtet. Idealerweise ist eine Prozesslandkarte vorhanden. Dies ist für das LASuV nicht der Fall, sodass aus den dokumentierten 30 bzw. 20 Aufgaben des Geschäftsverteilungsplanes jeweils ca. 15 Prozesse abgeleitet wurden. Diese fassen ähnliche Aufgaben als Unterprozesse zusammen (BSI, 2017b, S. 80). Orientierung dafür lieferte die personelle Zuständigkeit für mehrere Aufgaben sowie ein ähnlicher vermuteter Schutzbedarf. Die gebildeten Unterprozesse sind fein genug, um unterschiedliche Schutzbedarfe der einzelnen Aufgaben und Objekte abbilden zu können. Sie stellen jedoch keine detaillierten Arbeitsprozesse dar. Eine größere Detailierung ist für ein Informationssicherheitskonzept nicht sinnvoll (BSI, 2017b, S. 80). Als Mittel zur Dokumentation wurden vorerst Tabellen genutzt. Vom BSI gibt es eine beispielhafte Dokumentation eines fiktiven Unternehmens, der RECPLAST GmbH (BSI, 2022c). Deren Tabellen wurden um weitere Spalten erweitert. Tabelle 3 zeigt Teile des Tabellenkopfes und einige Beispieleinträge.

Erkennbar ist die Zuweisung eines eindeutigen Schlüssels an allen Prozessen und Objekten. Dieser dient im weiteren Verlauf der Dokumentation zur Referenzierung der Objekte.

Schlüssel	Referat	Name	Teilprozess von	Beschreibung	Vertraulichkeit	Grund Vertraulichkeit	Verfügbarkei	Grund Verfügbarkeit	Integrität	Grund Integrität
GPZ11-01	11	Referat 11 - Personal		Alle mit der I Personenbez						
GPZ11-02	11	Grundsatzangelegenheiten Personal	GPZ11-01	Umfasst die Personalvert	normal		normal		normal	
GPZ11-03	11	Führung und Registratur Personalakten	GPZ11-01	Personalakte Vorbereitung	hoch	VwV Personalakte	hoch	Fristen	hoch	große Auswirkung

Tabelle 3: Ausschnitt der Strukturanalyse – hier für Prozesse

6.3 Strukturanalyse der IT-Systeme

Dem Vorgehensmodell folgend wurden zuerst die Prozesse analysiert (BSI, 2017b, S. 77–78). Zur Ausführung der fachlichen Aufgaben werden IT-Systeme und verschiedene Software genutzt. Somit ergibt sich eine Abhängigkeit der Prozesse von dem ordnungsgemäßen Betrieb dieser Systeme und Anwendungen. Neben der Aufstellung der Systeme und der Software, wurden auch die direkten Abhängigkeiten wie in Tabelle 4 dokumentiert. Dazu ist für jeden Prozess dargestellt, von welchen weiteren Prozessen, Systemen und Anwendungen dieser abhängig ist. Ein Beispiel: für die Personalverwaltung wird die Software *PVS* genutzt. Diese Clientanwendung kommuniziert mit einem SQL-Datenbankserver. Der Prozess *GPZ11-07 Pflege Personaldatenbank, Regelbeurteilung, Abmahnung* ist somit *direkt* von der Anwendung *APP025 PVS* abhängig. Zum *SQL-Datenbankserver S013* und dessen Server-Betriebssystem besteht hingegen eine *indirekte* Abhängigkeit. Fällt der Server aus, sind auch der Datenbankserver und somit das Fachprogramm nicht mehr nutzbar. Für eine spätere Dokumentation in einem geeigneten Programm ist es zweckmäßig, in der Tabelle nur die direkten Abhängigkeiten in beide Richtungen darzustellen. Um auch die indirekten Abhängigkeiten eines Prozesses oder Objektes feststellen zu können, muss in dieser Tabelle dem Pfad der einzelnen Objekte gefolgt werden.

Diese logischen Verbindungen der einzelnen Assets würden sich auch in einem geeigneten Dokumentationsprogramm ergeben. In solchen Programmen werden die einzelnen Objekte miteinander verknüpft, um Abhängigkeiten aufzuzeigen und die Vererbung des Schutzbedarfs zu realisieren.

Kürzel	Name	Zuordnung	Kürzel	Name
GPZ11-03	**Führung und Registratur Personalakten**			
		nötig für	GPZ11-04	Übermittlung Gehaltsrelevanter Daten an LSF
		nötig für	GPZ11-05	Arbeitszeiterfassung
		nötig für	GPZ11-06	Fortbildung
		nötig für	GPZ11-07	Pflege Personaldatenbank, Regelbeurteilung, Abmahnung
		benötigt	APP003	MS Outlook 2016
		benötigt	APP004	MS EDGE
		benötigt	APP005	Firefox
		benötigt	APP006	Standard-Software-Paket
		benötigt	APP023	Adobe Acrobat 2017
		benötigt	APP026	eVA.SAX SmartClient
		benötigt	WKS001	Client PCs
		benötigt	NB001	Client Notebook
		benötigt	D001	Multifunktionsdrucker
		benötigt	D002	Drucker
		benötigt	DOK001	Personalakten in Papier
GPZ11-04	**Übermittlung Gehaltsrelevanter Daten an LSF**			
		benötigt	GPZ11-01	Personalverwaltung
		benötigt	GPZ11-03	Führung und Registratur Personalakten
		benötigt	APP002	MS Office 2016

Tabelle 4: Ausschnitt der Strukturanalyse – hier die Abhängigkeiten

Eine Übersicht solcher Abhängigkeiten und Zusammenhänge liefert der Netzplan in Abbildung 4. In diesem sind nicht alle Einzelsysteme und -geräte aufgeführt. Analog zur tabellarischen Auflistung wurden Systeme mit ähnlicher Funktion und ähnlichem Typ gruppiert (BSI, 2017b, S. 91).

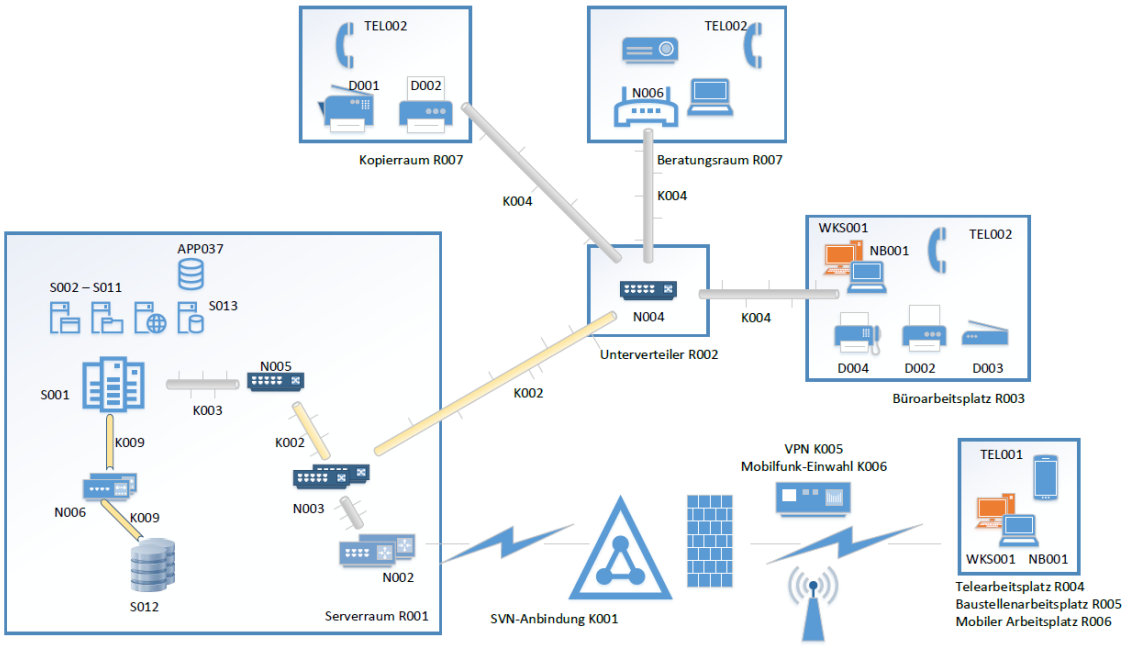

Abbildung 4: vereinfachter Netzplan mit Referenznummern der Objekte

Die Strukturanalyse und der Netzplan zeigen auch den weiteren Aufbau des Informationsverbundes. Client-Systeme *WKS001*, *NB001*, *TAB001* und die Server *S001* bis *S013* sind über die Switche *N004* und *N005* sowie mit den Kommunikationsverbindungen *K003* und *K004* in einer Baumtopologie miteinander verbunden. Dabei befinden sich die Clients in den Räumen *R003 Büroarbeitsplatz*, *R004 Telearbeitsplatz* oder *R006 Mobiler Arbeitsplatz*. Die beiden letztgenannten verfügen entweder über die VPN-Einwahl K005 oder über eine *Mobilfunk-Einwahl K006*.

Alle *Unterverteiler-Switche N004* für den Anschluss von Clients sind in separaten *Unterverteilerräumen R002* untergebracht. Alle Serversysteme befinden sich im *Serverraum R001*. Ein Großteil der Serversysteme sind als virtuelle Maschinen auf dem *Virtualisierungsserver S001* mit seinem *Storage-System S012* ausgeführt. Nahezu alle Server sind damit direkt vom Virtualisierungsserver abhängig.

Für die Modellierung ist es wichtig auch den gesamten *Informationsverbund VBND* als Objekt zu benennen, da hier Prozess-Bausteine modelliert werden, welche keinem genauerem Objekt zugeordnet werden können (BSI, 2022a, S. 25).

6.4 Modellierung

Abweichend vom Vorgehen der Kernabsicherung folgte nach der Strukturanalyse zunächst keine Schutzbedarfsfeststellung. Dies begründet sich in der in Kapitel 5.2 geplanten Vorgehensweise. Da beim IT-Grundschutz-Check die Umsetzungen aller Anforderungen, auch der erhöhten, geprüft werden sollen, ist die Feststellung des Schutzbedarfs zunächst nicht nötig. Zweck der Schutzbedarfsfeststellung ist es unter anderem, bei der Auswahl der Anforderungen die dem Schutzbedarf angemessenen Anforderungen aus den Bausteinen herauszufiltern. Das geplante Vorgehen sieht als Endresultat jedoch eine Übersicht über alle Anforderungen vor. So können bei Erhöhung des Schutzbedarfs in einem weiteren Zyklus direkt die nun geltenden erhöhten Anforderungen eingesehen werden. Es entfällt ein weiteres Interview, welches vorher bereits vorhandene Umsetzungen abfragt.
Ziel der Modellierung ist, den zu betrachtenden Informationsverbund mit den Bausteinen des IT-Grundschutz-Kompendiums nachzubilden (BSI, 2017b, S. 131). Zunächst wurde für jeden Prozessbaustein der Kategorien *ISMS – Sicherheitsmanagement, ORP – Organisation und Personal, CON – Konzepte und Vorgehensweisen, OPS – Betrieb,* und *DER – Detektion und Reaktion* im Abschnitt

Abgrenzung geprüft, ob dieser für den gesamten Informationsverbund anzuwenden ist und diesem zugeordnet. Dies bedeutet nicht, dass die Anforderungen durch jede Organisationseinheit zu erfüllen sind, sondern, dass die Institution als Ganzes entsprechende Prozesse, Konzepte und Maßnahmen etablieren muss, sodass die Umsetzungen in jeder Organisationseinheit wirken (BSI, 2017b, S. 146, 2022a, S. 25). Zur Erarbeitung der geforderten Umsetzungen werden die zuständigen Organisationseinheiten beauftragt.

Danach wurde jedem Asset ein oder mehrere Bausteine zugeordnet. Die *Abgrenzung* der Bausteine enthält auch Verweise auf weitere Bausteine, welche dem Objekt zuzuordnen sind. In Tabelle 5 sind Ausschnitte der Modellierung aufgeführt.

Schlüssel	Referat	Name	Vertraulichkeit	Grund Vertraulichkeit	Verfügbarkeit	Grund Verfügbarkeit	Integrität	Grund Integrität	Bausteine	Baustein Beschreibung
S002		Domänen-Controller	normal	Passwort-Verschl.	normal	Verteilung	hoch	Maximal-P	SYS.1.1	Allgemeiner Server
									SYS.1.2	Windows Server 2012
									APP.3.6	DNS-Server
S003		Dateiserver	hoch	Maximal-P	normal		hoch	Maximal-P	SYS.1.1	Allgemeiner Server
									SYS.1.2	Windows Server 2012
									APP.3.3	Fileserver
S004		Druckserver	normal		normal		normal		SYS.1.1	Allgemeiner Server
									SYS.1.2	Windows Server 2012
S005		OCR-Scan-Server	normal		normal		normal		SYS.1.1	Allgemeiner Server
									SYS.1.2	Windows Server 2019 (Draft)

Tabelle 5: Ausschnitt der Strukturanalyse – hier für Systeme mit zugewiesenen Bausteinen

Einer dieser Prozessbausteine ist *ORP.2 Personal.* Dieser beschreibt „…welche „personellen“ Sicherheitsmaßnahmen die Personalabteilung oder Vorgesetzten ergreifen müssen, damit die Mitarbeiterinnen und Mitarbeiter verantwortungsbewusst mit den Informationen der Institution umgehen und sich so gemäß den Vorgaben verhalten.“ (BSI, 2022a, S. 111). Grundsätzlich zuständig hierfür ist die Personalverwaltung.

7 Untersuchung der Assets

Durch die Modellierung, wie in Kapitel 6.4 beschrieben, ist der Informationsverbund auf Bausteine abgebildet. Diese Abbildung dient nun als Soll-Konzept und setzt sich aus den Anforderungen der Bausteine zusammen, welche auf dem zugeordneten Objekt umzusetzen sind. Der IT-Grundschutz-Check ist ein Soll-Ist-Vergleich und prüft ab, welche Anforderungen des Soll-Konzeptes vollständig, teilweise oder nicht umgesetzt sind. (BSI, 2017b, S. 145)

Zur Erhebung des Ist-Standes wurden Interviews durchgeführt. Im Rahmen dieser Arbeit wurde die zuständige Personalverwaltung zum Baustein *ORP.2 Personal* befragt. Die Gebäudeverwaltung erteilte Auskünfte zur Umsetzung des Bausteins *INF.1 Allgemeines Gebäude* für die Gebäude der Zentrale. Im weiteren Verlauf wurde der IT-Grundschutz-Check in Zusammenarbeit mit der IuK für die Bausteine *SYS.1.1 Allgemeiner Server* und *SYS.1.2.2 Windows Server 2012* durchgeführt. Die beiden letztgenannten Bausteine haben bei entsprechenden Umsetzungen eine große Wirkbreite auf viele Server des LASuV.

Die Schutzbedarfsfeststellung vor der Modellierung wurde zunächst ausgelassen. Laut gewählter Vorgehensweise sollen auch die Anforderungen für eine hohen Schutzbedarf im Interview abgefragt werden.

7.1 Interviewvorbereitung

Die Durchführung der Interviews bedurfte einiger Vorarbeiten. Aus den modellierten Bausteinen wurden alle Anforderungen tabellarisch wie in Tabelle 6 aufgeführt. Wie im Aufbau des BSI Standards in Kapitel 5.1.4 *IT-Grundschutzkompendium* beschrieben, werden die Anforderungen mit den Modalverben *MUSS* und *SOLLTE* definiert. Die Befürchtung war, dass bei IT-fremden Interview-Partnern der Eindruck der Be- oder Abwertung der eigenen bisherigen Arbeitsweise aufkommen könnte. Insbesondere die lange Aneinanderreihung von „MUSS-Anforderungen“ und „SOLLTE-Anforderungen“ könnte eine negative Grundstimmung verursachen. Um die empfohlene entspannte Gesprächsatmosphäre nicht zu gefährden, wurden aus den Anforderungen vor allem offene „W-Fragen“ abgeleitet (BSI, 2022b). Es wurden Termine vereinbart. Der jeweils erste für den Soll-Ist-Vergleich und eine Schutzbedarfsfeststellung, ein

zweiter Termin diente der Risikoanalyse. Die Interviewpartner wurden aus den Bausteinen und dem Organigramm ermittelt. Vorab erhielten diese eine erläuternde E-Mail, die den Zweck und Ablauf des IT-Grundschutz-Checks erklärt sowie die aufgestellten Fragen.

Anforderung	Titel / Fragen	Typ	Entbehrlich	umgesetzt: Ja	umgesetzt: Teilweise	umgesetzt: Nein
ORP.2.A1	**Geregelte Einarbeitung neuer Mitarbeiter**	Basis		X		
	Wie erfolgt die Einarbeitung neuer MA?					
	Wie werden neue MA über Regelungen, Verfahren, Handlungsanweisungen unterrichtet?					
	Gibt es eine Checkliste oder Hinweisetexte für neue MA?					
	Wird ein direkter Ansprechpartner für die Einarbeitung benannt?					
ORP.2.A2	**Geregelte Verfahrensweise beim Weggang von Mitarbeitern**	Basis			X	
	Wie wird der Nachfolger in die Tätigkeit des ausscheidenden MA eingearbeitet?					
	Wie werden ausgehändigte Unterlagen, Schlüssel, Geräte und Ausweise eingezogen?					
	Wird auf die Verschwiegenheitsverpflichtung vor Weggang hingewiesen?					
	Gibt es ein Verbot von Konkurrenzangeboten bzw. eine Übergangszeit?					
	Wie werden andere OE über den Weggang von MA informiert?					
	Wer ist der feste Ansprechpartner der Personalverwaltung für ausscheidende MA?					
ORP.2.A3	**Festlegung von Vertretungsregelungen**	Basis		X		
	Wie wird die Regelung der Vetretung verbindlich sichergestellt?					
	Wie wird sichergestellt, dass der Vertreter über die nötige Qualifikation verfügt?					
	Wie wird der Aufgabenumfang im Vertretungsfall klar definiert?					

Tabelle 6: Ausschnitt der Interviewfragen für den IT-Grundschutz-Check

7.2 IT-Grundschutz-Checks

Für die Interviews brachte die Referatsleiterin *Personal* einen Fachverantwortlichen mit. Dieser ist unter anderem für die Personalverwaltungsdatenbank zuständig. Beim ersten Termin wurden die ausgedruckten Fragen sowie ein Ausdruck des Bausteins *OPS.2 Personal* genutzt. Das Interview wurde durch den Autor geführt, die Beauftragte für Informationssicherheit begleitete die Durchführung. Einleitend wurde noch einmal der Zweck der Befragung des IT-Grundschutzes erläutert, dass aus dem Ergebnis keine arbeitsrechtlichen Konsequenzen entstehen und, dass bei Start eines Informationssicherheitsprozesses mit einem geringen Umsetzungsstand gerechnet werden kann.

Es wurde jeweils eine Frage gestellt und beiden Interviewpartnern Zeit für die Beantwortung eingeräumt. Bereits getätigte Umsetzungsmaßnahmen für einzelne Fragen wurden notiert. Die meisten Anforderungen aus dem Baustein bestehen aus mehreren MUSS- und SOLL-Anforderungen. Entsprechend wurden alle zu dieser Anforderung gehörigen Fragen und Antworten zu einer Gesamteinschätzung des Umsetzungstandes herangezogen. Hierzu wurde die Anforderung aus dem Baustein vorgetragen, um gemeinsam mit den Interviewpartnern den Umsetzungsstand mit *Ja, Nein* oder *Teilweise* festzuhalten. Für eine *Teilweise* Umsetzung bedurfte es einer

Umsetzung von mindestens 50 Prozent. Darüber hinaus wurde darauf geachtet, dass nicht zu positiv interpretiert wurde.

Das Interview mit dem Sachgebietsleiter *Innerer Dienst,* zuständig für die Gebäudeverwaltung, wurde auf gleiche Weise vorbereitet. Geführt wurde das Interview als Videokonferenz. Resultat war hier ein bereits sehr guter Umsetzungstand. Dies begründet sich darin, dass eine in Sachsen gültige Bau-Richtlinie – *RL Bau* – bereits detailliert nahezu all jene Aspekte berücksichtigt, welche auch der BSI-Baustein *INF.1 – Allgemeines Gebäude* aufführt. Zudem wurde das Gebäude vor 10 Jahren kernsaniert und erweitert.
Das Interview mit dem Sachgebiet *IuK* wurde für die Bausteine *SYS.1.1 Allgemeiner Server* und *SYS.1.2.2 Windows Server 2012* mit dem zuständigen Administrator geführt. Hierbei wurde auf die Umwandlung der Bausteinanforderungen in W-Fragen verzichtet. Der Umgang mit Anforderungen ist im IT-Bereich bekannt und wird nicht als Abwertung angesehen. Im Interview wurden konkret getätigte Konfigurationen hinsichtlich der Umsetzung der Anforderungen erläutert.

7.3 Schutzbedarfsfeststellung

Nach der Aufnahme des Ist-Standes aller Anforderungen, wurde im selben Termin eine Schutzbedarfsfeststellung durchgeführt. Diese wurde für die in Kapitel 6.2 erarbeiteten Unterprozesse der Personalverwaltung durchgeführt. Für die Gebäudeverwaltung konnte aus terminlichen Gründen keine Schutzbedarfs-feststellung durchgeführt werden. Diese muss im Rahmen der kontinuierlichen Verbesserung erfolgen.
Der Schutzbedarf im IT-Grundschutz bezieht sich auf die Ziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit (BSI, 2017b, S. 104)*:

Schutzziel	**Beschreibung**
Vertraulichkeit	Schutz vor unautorisiertem Erlangen von Informationen
Integrität	Schutz vor unautorisierter Veränderung oder Erkennung einer unautorisierten Manipulation
Verfügbarkeit	Schutz der Gewährleistung der berechtigten Nutzbarkeit

Tabelle 7: Definition der BSI-Schutzziele nach Eckert (2018, S. 9–12)

Damit ein festgestellter Schutzbedarf verlässlich mit wiederholbarem Ergebnis durchgeführt werden kann, muss zuvor eine Definition für die qualitative

Einschätzung der Schutzbedarfskategorien erzeugt werden. Diese definiert sowohl die Schutzbedarfskategorien als auch die qualitativen Dimensionen, für den diese stehen. (BSI, 2017b, S. 104) Diese Aufgabe übernimmt im Freistaat Sachsen der Beschluss zur *Richtlinie Definition der Schutzbedarfskategorien* vom 07.07.2020. Diese entspricht weitestgehend in ihren Definitionen dem Vorschlag des BSI-Standard 200-2, wurde jedoch um Aspekte der öffentlichen Verwaltung ergänzt. Außerdem wurden Szenarien für Ausfallzeiten und dem Schutz von Dokumenten hinzugefügt.
Mit Hilfe von „Was wäre, wenn“ Fragen wurden gemeinsam mit den Interviewpartnern Szenarien besprochen, um den Schutzbedarf einzelner Unterprozesse festzustellen (BSI, 2017b, S. 110). Im Anhang des BSI 200-2 sind hierfür beispielhafte Fragestellungen aufgeführt, diese dienten als Orientierung, um die Fragen in Tabelle 8 abzuleiten (2017b, S. 173–178). Insbesondere bei Fragestellungen zu rechtlichen Konsequenzen sind die Kenntnisse der Interviewpartner zu den gesetzlichen Grundlagen des betrachteten Fachbereichs notwendig.

Frage	**Schutzziel**
Gibt es Vorschriften, die die Vertraulichkeit vorschreiben?	Vertraulichkeit
Was würde passieren, wenn Informationen unrechtmäßig in Umlauf geraten?	
Ist eine Manipulation von Daten erkennbar?	Integrität
Können ggfs. manipulierte Daten aus anderen Quellen bezogen werden?	
Können verlorene Daten aus anderer Quelle wiederhergestellt werden?	Verfügbarkeit
Wie groß sind die Auswirkungen von Ausfällen?	
Sind Fristen durch Ausfälle in Gefahr?	

Tabelle 8: "Was wäre, wenn" Fragestellungen zur Schutzbedarfsfeststellung

Bei der Auswertung der Schutzbedarfsfeststellung kristallisierten sich bei der Personalverwaltung zwei Prozesse heraus, welche bei mindestens einem der Schutzziele einen hohen Schutzbedarf aufweisen. Zum einen ist die Arbeit mit

papiergebundenen *Personalakten DOK001* mit hohem Schutzbedarf festgestellt worden, als auch alle Tätigkeiten mithilfe des Personalverwaltungsprogrammes *APP025 PVS*. Zur Reduzierung des Aufwandes sollen nach BSI-Standard 200-3 in der Risikoanalyse Prozesse und Anwendungen sinnvoll gruppiert werden (2017c, S. 9). Hierfür wurden zwei „virtuelle“ Prozesse erzeugt:

- *GPZ11-15 Umgang und Verwaltung Personalakten in Papier*
- *GPZ11-16 Verarbeitung elektronischer Personaldaten*

In der Strukturanalyse wurden diese „virtuellen“ Prozesse ergänzt und deren Abhängigkeit zu den Papierakten bzw. der Anwendung hinzugefügt. Dies ist im weiteren Verlauf für die Vererbung des Schutzbedarfs auf diese Assets relevant.

Aus der Strukturanalyse ist erkennbar, von welchen Anwendungen und IT-Systemen bestimmte Prozesse abhängig sind. Diese erben den Schutzbedarf der von ihnen abhängigen Prozesse. Dabei wird das *Maximum-Prinzip* angewandt: Sind mehrere Prozesse mit unterschiedlichem Schutzbedarf von einer Anwendung oder einem IT-System abhängig, gilt der höchste Schutzbedarf der Prozesse auch für diese Anwendung bzw. IT-Systeme. Für den untersuchten virtuellen Prozess *GPZ11-16 Verarbeitung elektronischer Personaldaten* ist die Abhängigkeit zur Anwendung *APP025 PVS* erkennbar. Die Anwendung erbt den hohen Schutzbedarf für die Vertraulichkeit vom Prozess und gibt diesen an den Datenbankserver *S013 SQL-Datenbankserver* der Anwendung weiter. (BSI, 2017b, S. 108)

Auch die andere Richtung muss betrachtet werden. Haben die einzelnen Prozesse einen *normalen* Schutzbedarf, würde die dafür notwendige Anwendung ebenfalls den Schutzbedarf *normal* erben. Fällt die Anwendung selbst aus, sind davon alle von ihr abhängigen Prozesse betroffen. Dieses Szenario verursacht möglicherweise einen hohen Schaden, da sich durch viele kleine Schäden oder Ausfälle der betroffenen Prozesse die Auswirkungen aufaddieren. Dieser Kumulationseffekt tritt bei Ausfall des Servers *S013 SQL-Datenbankserver* und der Anwendung *APP025 PVS* jedoch nicht auf. Die betroffenen kleineren Anwendungen wurden in dieser ersten Iteration als nicht prozesskritisch angesehen. (BSI, 2017b, S. 109)

7.4 Risikoanalyse

Die in der Schutzbedarfsfeststellung festgestellten Assets mit hohem Schutzbedarf, wurden einer Risikoanalyse nach BSI-Standard 200-3, wie in Kapitel 5.1.3 dargestellt, unterzogen. Analysiert wurden die Assets:

- *GPZ11-15 Umgang und Verwaltung Personalakten in Papier*
- *GPZ11-16 Verarbeitung elektronischer Personaldaten*
- *S013 SQL-Datenbankserver*

Im jeweils zweiten Interview wurden gemeinsam alle Gefährdungen aus dem IT-Grundschutzkompendium diskutiert. Für die Interviewvorbereitung wurde bereits vorab eine Betrachtung der Relevanz als Vorschlag durchgeführt. Dabei und im Interview wurden einige elementare Gefährdungen als nicht relevant festgestellt, wenn diese keine weiteren Aspekte gegenüber anderen Gefährdungen aufwiesen oder keinen direkten Einfluss auf das betrachtete Objekt erkennen ließen (BSI, 2017c, S. 16–17). So weist beispielsweise die Gefährdung *G 0.7 Großereignisse im Umfeld* keinen erkennbaren direkten Einfluss auf Geschäftsprozesse einer Behörde auf. Für den untersuchten Server beinhaltet die Gefährdung *G 0.1 Feuer* gegenüber den Auswirkungen unter anderem aus *G 0.25 Ausfall von Geräten oder Systemen* und *G 0.45 Datenverlust* keine weiteren Aspekte auf. Tabelle 9 zeigt ausschnittsweise die Ergebnisse der Risikoanalyse. Für die Bewertung des Risikos wurde die Matrix aus Abbildung 2 des BSI 200-3 herangezogen.

Zielobjekt	Gefährdung	Eintrittshäufigkeit	Auswirkung	Risiko	Risikobehandlung	Erläuterung zur Risikobehandlung / Grund für Irrelevant / Maßnahmen
GPZ11-15 Umgang mit Papier-Personalakten	G 0.1 Feuer	mittel	kritisch	hoch	Risikovermeidung	Kopierer aus Aktenraum entfernen
GPZ11-15 Umgang mit Papier-Personalakten	G 0.2 Ungünstige klimatische Bedingungen	selten	vernachlässigbar	gering	Risikoakzeptanz	
GPZ11-15 Umgang mit Papier-Personalakten	G 0.3 Wasser	mittel	begrenzt	gering	Risikoakzeptanz	
GPZ11-15 Umgang mit Papier-Personalakten	G 0.4 Verschmutzung, Staub, Korrosion	mittel	begrenzt	gering	Risikoakzeptanz	
GPZ11-15 Umgang mit Papier-Personalakten	G 0.5 Naturkatastrophen	irrelevant	vernachlässigbar	gering		Keine neuen Aspekte zu G 0.1 Feuer und G 0.3 Wasser (Tornado)

Tabelle 9: Ausschnitt der Risikoanalyse – hier für einen Prozess der Personalverwaltung

Während der gemeinsamen Risikoanalyse mit dem Personalreferat, konnte bereits das Sicherheitsbewusstsein für zwei sehr konkrete Gefährdungen gesteigert werden. Der Kopierer im Aktenraum für die Personalakten stellt ein erhebliches Feuer-Risiko dar. Eine entsprechende Änderung wurde angeregt. Des Weiteren

kommt es während der Arbeit mit Personalakten häufiger vor, dass diese am Ende des Tages im eigenen Arbeitsplatzbüro verbleiben, statt in den dafür vorgesehene Aktenraum verbracht zu werden. Auch hier konnte das Bewusstsein für das eigene sicherheitsrelevante Handeln verbessert werden. In einer Revision sollte die Dauerhaftigkeit dieser Sensibilisierung überprüft werden.

8 Umsetzungsplan

Die bisher erarbeiteten Teile Strukturanalyse, Schutzbedarfsfeststellung, IT-Grundschutz-Check und Risikoanalyse sind Teile eines Informationssicherheits-konzeptes, auch Sicherheitskonzept. Für eine Umsetzung der Anforderungen müssen aus dem IT-Grundschutz-Check alle fehlenden oder zu ergänzenden Maßnahmen zusammengefasst werden. Anschließend müssen konkrete Umsetzungen der Anforderungen erarbeitet werden. Diese müssen den organisatorischen und technischen Gegebenheiten der Institution angepasst werden. Ergänzend zu den Bausteinen existieren Umsetzungshinweise, welche konkrete Maßnahmen vorschlagen. Sowohl die Anforderungen der Bausteine als auch die Umsetzungshinweise enthalten jedoch keine detaillierten Handlungsanweisungen. Diese muss eine Institution für sich erstellen. Grundsätzlich verantwortlich dafür sind die in den Bausteinen benannten zuständigen Stellen. Je nach Organisationsaufbau der Institution sind weitere Stellen hinzuzuziehen. Die Erarbeitung von wirksamen Maßnahmen kann ein langwieriger Prozess sein und ist daher nicht Teil dieser Arbeit. Im Rahmen dieser Arbeit wurde jedoch eine Umsetzungsplanung aufgestellt, welche die Priorisierung der Umsetzungen aufzeigt. (BSI, 2017b, S. 158)

8.1 Priorisierung

Zur Festlegung einer Reihenfolge wurden verschiedene Faktoren herangezogen. Die Bausteine enthalten eine grobe Reihenfolge von 1 bis 3. Dabei sind übergreifende Bausteine, welche meist auf den gesamten Informationsverbund anzuwenden sind, zuerst umzusetzen (BSI, 2017b, S. 137–138). Außerdem wurde Basisanforderungen Vorrang vor Standardanforderungen eingeräumt. Anforderungen für einen hohen Schutzbedarf sollen laut BSI 200-2 nachrangig umgesetzt werden (2017b, S. 160). Außerdem spielt die Wirkbreite eine wichtige Rolle. Insbesondere zentral getätigte Konfigurationen von IT-Systemen wirken auf alle Systeme und erhöhen damit die Sicherheit eines großen Bereichs des Informationsverbundes (2017b, S. 161). Ebenfalls wurde die Organisationsstruktur beachtet. Bausteine, welche zum Beispiel durch die Personalverwaltung umgesetzt werden müssen, behindern meist nicht die Umsetzungsarbeiten der IT-Administratoren. Voraussetzung für eine parallele Umsetzung sind Grundlagen wie das Bekenntnis der Institutionsleitung

zur Informationssicherheit, vorhandene Ressourcen und eine bekanntgegebene Informationssicherheitsleitlinie.

In Tabelle 10 sind Ausschnitte des Sicherheitskonzeptes sowie die Priorität der Umsetzung dargestellt. Gleiche Prioritäten bedeuten eine mögliche parallele Umsetzung. Da ein Sicherheitskonzept stets vertraulich zu behandeln ist, wurde auf die vollständige Veröffentlichung verzichtet. Die gezeigten Ausschnitte sind allgemeiner Natur und wurden teilweise verfälscht. Enthalten sind:

- Anforderungen aus den modellierten Bausteinen
- Ergebnisse des IT-Grundschutz-Checks
- Verantwortlichkeiten
- grob definierte Maßnahmen
- Umsetzungspriorität

				Entbehr-		umgesetzt				
Anforderung	Anforderung	Typ	Betroffene Assets	lich	Ja	Teilweise	Nein	Bemerkungen / Begründung für Nicht-Umsetzung / Maßnahmen	Baust Reihe	Umsetzungs-Priorität
ORP.2.A2	Geregelte Verfahrensweise beim Weggang von Mitarbeitern	Basis	VBND; GPZ11-01			X		Änderungsmeldung; Laufzettel soll Hinweis zur Verschwiegenheitspflicht erhalten	R1	A
ORP.2.A15	Qualifikation des Personals	Basis	VBND; GPZ11-01			X		DV Fortbildung; VwV Dienstordnung Abs. 14d; Personalentwicklungskonzept vorantreiben	R1	C
ORP.2.A7	Überprüfung der Vertrauenswürdigkeit von Mitarbeitern	Standard	VBND; GPZ11-01			X		regelm. Plausibilitätsprüfung d. Lebenslauf	R1	B
aus R-Analyse		Hoch	R009				X	Kopierer aus Personalaktenraum entfernen	R1	A
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs	Standard	S001 - S013				X	Betriebshandbücher erstellen, ggfs. zusammen mit Konfigurations- und Sicherheits-	R2	D
SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betrieb	Standard	S001 - S013				X	Prüfung auf Kapselungsverfahren; Einbindung in Konfigurationsko	R2	C
SYS.1.1.A27	Hostbasierte Angriffserkennung	Hoch	S001; S003; S008; S010; S013				X	Beschaffung IDS-System bei Notwendigkeit oder Honey-Sensor	R2	G
SYS.1.1.A28	Steigerung der Verfügbarkeit durch Redundanz	Hoch	S001; S003; S008; S010; S013			X		Redundanz einzelner virtueller Server prüfen / konfigurieren	R2	E
SYS.1.1.A30	Ein Dienst pro Server	Hoch	S001; S003; S008; S010; S013				X	bei hohem Schutzbedarf in Planung berücksichtigen	R2	E
SYS.1.1.A31	Einsatz von Ausführungskontrolle	Hoch	S001; S003; S008; S010; S013				X	bei hohem Schutzbedarf Applocker-Einsatz	R2	F

Tabelle 10: Ausschnitt des Sicherheitskonzeptes mit Umsetzungspriorität

Das Sicherheitskonzept bzw. dessen Umsetzungsplan setzt sich aus diesen Spalten zusammen:

Spalte	Inhalt
A	Verweis auf die Anforderung des Bausteins
E	Betroffene Assets, an denen die Umsetzung erfolgt
J	Maßnahme
K	Bausteinreihenfolge
L	Umsetzungspriorität für das LASuV

Tabelle 11: Spalten aus denen sich der Umsetzungsplan zusammensetzt

Der Verweis auf die Anforderungen aus dem jeweiligen BSI-Baustein stellt sicher, dass zum Zeitpunkt der Umsetzung stets mit aktuellen Bausteintexten gearbeitet

wird. Aus den Anforderungen und ggfs. vorhandenen Umsetzungshinweisen leiten sich die Maßnahmen ab. Zudem wurde eine erste Aufwandseinschätzung in Arbeitstagen durchgeführt. Insgesamt konnten 56 *nicht* oder *teilweise* umgesetzte Anforderungen gefunden werden. Davon allein 18 der Kategorie *Basis-Anforderung.*

8.2 Weitere Schritte

Um das aufgestellte Sicherheitskonzept in die Umsetzung zu bringen, muss die Leitungsebene die Verantwortung über die Informationssicherheit übernehmen. Nur auf diese Weise können verbindlich Ressourcen für die Erarbeitung und Umsetzung von Maßnahmen bei den unterschiedlichen Verantwortlichen vergeben werden (BSI, 2017b, S. 20). Wie eingangs in Kapitel 4.2 dargestellt hat die Übernahme der Verantwortung bisher nicht stattgefunden. Der Sicherheitsprozess muss zunächst initiiert werden. Der BSI-Standard 200-1 und BSI-Standard 200-2 bieten hierfür konkrete Hilfestellung. Die Behördenleitung des LASuV muss für das Thema sensibilisiert werden. Gesetzliche Regelungen und die Verantwortung für die Informationssicherheit müssen im Rahmen einer Besprechung durch die Beauftragte für Informationssicherheit und ihrem Team dargestellt werden. Über mögliche Risiken und Konsequenzen muss aufgeklärt werden (BSI, 2017b, S. 20). Die Initiierung und der Aufbau eines Informationssicherheitsprozesses, dessen Steuerung und Aufrechterhaltung müssen durch die Präsidentin des LASuV angeordnet werden. Untergebende Stellen müssen ausführlich darüber unterrichtet, der Rückhalt durch die Leitungsebene zugesichert werden. Auf diese Weise können teils unbequeme Sicherheitsmaßnahmen durchgesetzt werden.

Als Argumentationshilfe kann das im Rahmen dieser Arbeit angefertigte Sicherheitskonzept herangezogen werden. Es enthält trotz eng abgestecktem Geltungsbereich bereits viele nicht umgesetzte Anforderungen.

8.3 Erkenntnisse für weitere Iterationen

Bereits bei der Strukturanalyse eines derart begrenzten Informationsverbundes zeigte sich die hohe Komplexität und Abhängigkeiten der einzelnen Assets. Die genutzte tabellarische Darstellung ist für weitere Arbeiten ungeeignet. Schnellstmöglich muss ein geeignetes Dokumentationswerkzeug beschafft werden.

Die Erstellung von W-Fragen zu den Anforderungen der Bausteine ermöglichte eine offene und wertungsfreie Diskussionsatmosphäre und sollte bei Zusammenarbeiten mit Nicht-IT-Kollegeninnen und -Kollegen fortgeführt werden.

Für einen freien Gedankenaustausch sorgte auch die Arbeit mit ausgedrucktem Papier. Sie ermöglichte eine direkte Zuwendung zum Interviewpartner ohne die sonst nötige Zentrierung um einen Bildschirm.

Der Abbau von Ängsten vor Be- oder Abwertung der Arbeit des Interviewpartners ist wichtig. Eine entsprechende einleitende E-Mail mit den vorab versandten Interviewfragen und ein nochmaliges Erklären, dass fehlende Umsetzungen erstmal normal sind, kann hier helfen. Dies darf jedoch nicht dazu führen, dass der bisherige Zustand der Informationssicherheit weiter hingenommen wird. Aufforderungen zu Umsetzungen muss Folge geleistet werden.

8.4 Kontinuierliche Verbesserung

Informationssicherheit ist kein unveränderbarer Zustand. Das erreichte Sicherheitsniveau muss dauerhaft aufrechterhalten und verbessert werden (BSI, 2017a, S. 17). Veränderungen innerhalb der Institution, neue Aufgaben aber auch Rahmenbedingungen wie neue Gesetze oder neue Technologien führen immer wieder zu notwendigen Anpassungen der Informationssicherheit. Dazu ist ein aktives Steuern der Informationssicherheit notwendig. Durch regelmäßige Überprüfungen muss sichergestellt werden, dass das Sicherheitskonzept und dessen Maßnahmen der aktuellen Technologie und neuen Angriffsformen gewachsen ist. Das Informationssicherheitsmanagement überprüft als permanenter Prozess die Wirksamkeit, Angemessenheit und tatsächliche Anwendung aller Maßnahmen (BSI, 2017a, S. 17). Als Querschnittsprozess muss die Informationssicherheit außerdem bei allen größeren Änderungen mitgeplant werden. Daraus ergeben sich weitere Anpassungen. Dies führt zur Betrachtung des

Lebenszyklus der Informationssicherheit. Die sich ständig wiederholenden PDCA-Phasen lauten:

1. **P**lan – Anpassung des Sicherheitskonzeptes, Planung weiterer Maßnahmen
2. **D**o – Umsetzung der Maßnahmen
3. **C**heck – Erfolgskontrolle, Überwachung der Zielerreichung
4. **A**ct – Optimierung und Verbesserung (BSI, 2017b, S. 17)

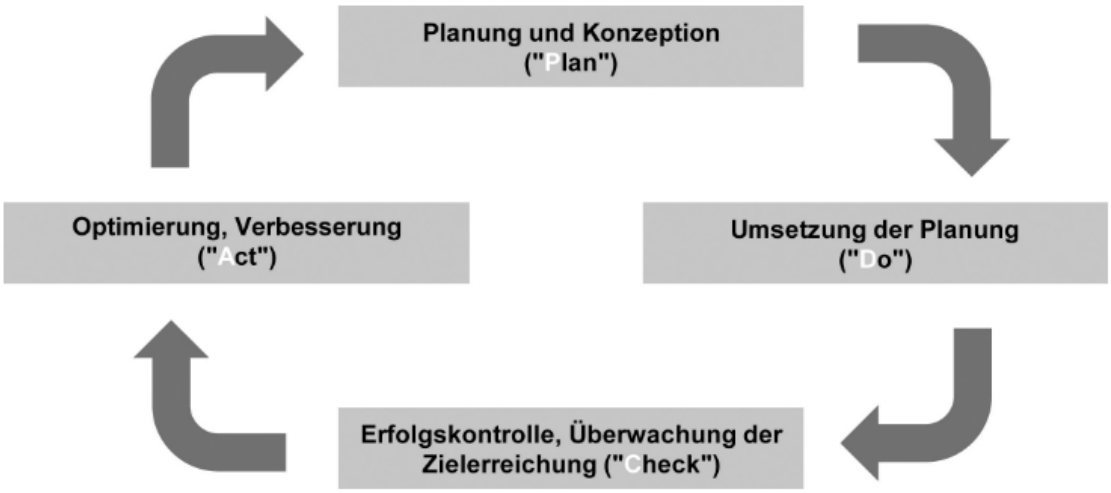

Abbildung 5: PDCA-Zyklus zur Verbesserung der Informationssicherheit nach Deming

Maßnahmen werden geplant, umgesetzt und auf Wirksamkeit überprüft. Werden dabei Mängel festgestellt, werden diese behoben. Sind dazu weiteren Maßnahmen notwendig, müssen diese geplant werden. Der Kreislauf beginnt somit von neuem.

Neben der Informationssicherheit selbst unterliegt auch der Managementprozess der Informationssicherheit diesem in Abbildung 5 dargestellten *PDCA-Zyklus*.
Dabei wird unter anderem überprüft, ob organisatorische Maßnahmen, Abläufe und Dokumentationen wirksam und effizient sind. (BSI, 2017b, S. 164)

9 Fazit

Das LASuV ist gesetzlich verpflichtet, einen Informationssicherheitsprozess nach BSI IT-Grundschutz zu etablieren. Die nötigen Voraussetzungen wie die Verantwortungsübernahme der Leitungseben oder die Erstellung eines Sicherheitskonzeptes nach BSI 200-2 fanden bisher nicht statt. Ziel dieser Arbeit war es, dennoch einen methodischen Einstieg in den IT-Grundschutz zu erarbeiten. Die IT-Grundschutzmethodik bietet dafür 3 Varianten, die Basisabsicherung, die Kernabsicherung und die Standardabsicherung. Zur Vermeidung von Doppelarbeit und zur Reduzierung der Komplexität wurde die Vorgehensweise der Kernabsicherung gewählt. Die erforderlichen Einzelschritte Strukturanalyse, Modellierung, IT-Grundschutz-Check, Schutzbedarfsfeststellung und Risikoanalyse wurden anhand der BSI-Standards 200 methodisch durchgeführt. Untersucht wurden die Personalverwaltung, die Gebäudeverwaltung und die IT-Systeme. Aus den BSI-Bausteinen ergaben sich Anforderungen an die jeweiligen Assets des Informationsverbundes. Mehrere interviewgestützte IT-Grundschutz-Checks zeigten fehlende Umsetzungen der Anforderungen auf. Anhand der durchgeführten Risikoanalysen konnten erste weitere Maßnahmen definiert werden. Das zu erstellende Sicherheitskonzept setzt sich unter anderem aus der Strukturanalyse, der Modellierung und den noch offenen Umsetzungen zusammen. Deren Auflistung wurde in einen priorisierten Umsetzungsplan überführt.
Die weiteren Aufgaben zur Erhöhung der Informationssicherheit umfassen, neben der Etablierung eines Informationssicherheitsprozesses und der Einbindung der Leitungsebene, die Konkretisierung von Maßnahmen und Umsetzungen sowie eine kontinuierliche Verbesserung der Informationssicherheit im LASuV.

Gewonnene Erkenntnisse und Erfahrungen in der Arbeit beziehen sich vor allem auf die praktische Umsetzung der IT-Grundschutz-Methodik. Diese ermöglichen ein dauerhaftes Vorantreiben der Informationssicherheit. Die intensive Vorbereitung der geführten Interviews für den IT-Grundschutz-Check ermöglichten eine konstruktive Zusammenarbeit mit den zuständigen Kolleginnen und Kollegen.

Die IT-Grundschutz-Methodik konnte in geeigneter Weise angewandt werden, um für einen eng abgegrenzten Informationsverbund ein Sicherheitskonzept nach BSI 200-2 zu erstellen.

Literaturverzeichnis

Allianz ACGS (Hrsg.). (2022). *Allianz Risk Barometer 2022: Cyber weltweites Top-Risiko für Unternehmen; Sorge vor Naturgefahren und Klimawandel in Deutschland* [Pressemitteilung | 18. Januar 2022]. https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html

BSI (2017a). BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS).

BSI (2017b). BSI-Standard 200-2: IT-Grundschutz-Methodik.

BSI (2017c). BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz.

BSI. (2020). *Informationssicherheit mit System Der IT-Grundschutz des BSI*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Informationssicherheit_mit_System.html

BSI (2021a). BSI-Standard 200-4: Business Continuity Management (Community Draft).

BSI (2021b). Die Lage der IT-Sicherheit in Deutschland 2021.

BSI. (2021c, 26. Januar). *Glossar der Cyber-Sicherheit*. https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Glossar-der-Cyber-Sicherheit/Functions/glossar.html

BSI. (2021d, 10. August). *IT-Grundschutz*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

BSI. (2021e, 10. August). *IT-Grundschutz*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

BSI. (2022a). *IT-Grundschutz-Kompendium* (5. Aufl.). Bundesanzeiger Verlag GmbH. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

BSI. (2022b, 14. März). *Lerneinheit 6.2: Vorbereitung und Durchführung*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-

Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_6_IT-Grundschutz-Check/Lektion_6_02/Lektion_6_02_node.html

BSI. (2022c, 16. März). *Recplast*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/recplast_node.html

Eckert, C. (2018). *IT-Sicherheit: Konzepte - Verfahren – Protokolle*. *Praxishandbuch*. De Gruyter Oldenbourg.

Grünendahl, R.-T., Steinbacher, A. F. & Will, P. H. (2017). *Das IT-Gesetz: Compliance in der IT-Sicherheit: Leitfaden für ein Regelwerk zur IT-Sicherheit im Unternehmen* (3. Aufl.). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-18205-2

Hanschke, I. (2020). *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-28699-6

ISO (2009). *ISO/IEC Guide: Risk management – Vocabulary*.

Kersten, H. & Klett, G. (2015). *Der IT Security Manager*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-09974-9

Kersten, H., Klett, G., Reuter, J. & Schröder, K.-W. (2020). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-27692-8

Königs, H.-P. (2017). *IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken* (5. Aufl.). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-12004-7

LASuV. (2020). *Über uns - Landesamt für Straßenbau und Verkehr - sachsen.de*. https://www.lasuv.sachsen.de/ueber-uns-4001.html

LISt GmbH. (2017). *Aufgaben - LISt Gesellschaft für Verkehrswesen und ingenieurtechnische Dienstleistungen mbH - sachsen.de*. https://www.list.sachsen.de/aufgaben-4045.html

Sächsische Staatskanzlei (2019). Masterplan "Digitale Verwaltung Sachsen": Überblick. https://www.egovernment.sachsen.de/download/masterplan-digitalisierung.pdf

Schmidt, J. (2021). *Schutz vor schwerwiegender Log4j-Lücke - was jetzt hilft und was nicht.* Heise Medien. https://www.heise.de/ratgeber/Schutz-vor-schwerwiegender-Log4j-Luecke-was-jetzt-hilft-und-was-nicht-6292961.html

SID. (2018). *IT-Infrastruktur & Betrieb - Staatsbetrieb Sächsische Informatik Dienste - sachsen.de*. https://www.sid.sachsen.de/infrastruktur.html

SMJ (2014). Strategie für IT und E-Government des Freistaates Sachsen. https://www.egovernment.sachsen.de/download/Strategie_ITundEGovernment_desFreistaatesSachsen.pdf

Witt, B. C. (2010). *Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung* (2. Aufl.). *Studium*. Vieweg + Teubner.

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization für Standardization
IuK	Information und Kommunikation
LASuV	Landesamt für Straßenbau und Verkehr
SMWA	Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr
VwV	Verwaltungsvorschrift

Tabellenverzeichnis

Abbildungsverzeichnis

Anhangsverzeichnis