IT-Grundschutz-Profil für Hochschulen

Herausgegeben vom Vorstand des ZKI e. V.

Version 2022.0.0

Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Inhalt

Versionshistorie

Version	bisherige Version	Datum	Beschreibung
2019.0.0	0.9	25.11.2019	Veröffentlichung des Rahmendokuments als Community Draft und Vorstellung auf dem Workshop „Informationssicherheit“ der Hochschulrektorenkonferenz
2020.0.0	1.0	08.09.2020	Rahmendokument und Baustein-Kommentierungen auf Grundlage der Edition 2020 des IT-Grundschutz-Kompendiums des BSI veröffentlicht
2022.0.0		04.08.2022	Veröffentlichung des Rahmendokuments aktualisiert auf Stand des Kompendiums 2022; Änderung des Dokumentaufbaus speziell bezüglich der Geschäftsprozesse; Näheres siehe die folgende Tabelle

Änderungen in Version 2022.0.0

Nachfolgend sind die wesentlichen Überlegungen und Änderungen zum Vorgängerdokument zusammengestellt:

Änderung	Hintergrund
Inhaltliche Updates	Die vorliegende Version bezieht sich auf das IT-Grundschutz-Kompendium 2022 des BSI. Gegenüber der Vorgängerversion 2020 bestehen die nachfolgend aufgeführten Bausteinänderungen: Neue Bausteine: APP.1.4 Mobile Anwendungen (Apps) APP.4.4 Kubernetes APP.5.3 Allgemeiner E-Mail-Client und -Server APP.6 Allgemeine Software APP.7 Entwicklung von Individualsoftware CON.10 Entwicklung von Webanwendungen INF.12 Verkabelung INF.13 Technisches Gebäudemanagement INF.14 Gebäudeautomatisierung OPS.1.1.7 Systemmanagement OPS.1.2.6 NTP-Zeitsynchronisation Weggefallene Bausteine: APP.5.1 Allgemeine Groupware INF.3 Elektronische Verkabelung INF.4 IT-Verkabelung CON.4 Auswahl und Einsatz von Standardsoftware CON.5 Einsatz von Individualsoftware
Änderung der Versionierung	Die ersten Versionen wurden noch als Version 0.9 bzw. 1.0 veröffentlicht. Die Versionierung wurde jetzt so angepasst, dass der Bezug auf das jeweilige IT-Grundschutz-Kompendium in der ersten Stelle der Nummer sofort sichtbar wird. Updates werden über die 2. Stelle, kleinere Änderungen über die 3. Stelle markiert.
Ergänzungen in der Landkarte mit Prozessbausteinen	Laut IT-Grundschutz-Kompendium des BSI finden sich nun Bausteine, die von der Nomenklatur her eigentlich Systembausteine sind, bei den Prozessbausteinen, sind also dem „Informationsverbund/übergeordnete Aspekte“ zugeordnet (APP.7, SYS.3.2.2, INF.9). Diese wurden aus Gründen der Übersichtlichkeit, aber auch der Systematik teils bei den Übergeordneten Bausteinen verortet, die aus Sicht der Autorinnen und Autoren ebenfalls für den Informationsverbund zu betrachten sind. Andererseits wurde der Systembaustein APP.6 hier mit aufgenommen, da er aus Sicht der Autorinnen und Autoren ebenfalls übergreifend zu betrachten ist. Näheres dazu findet sich in den Kapiteln 11 bzw. 15. Laut BSI ist der Kontext der Darstellung weniger wichtig als die Betrachtung des jeweiligen Bausteins an sich.
Umstellung der Reihenfolge der Prozesslandkarten	Bereits bisher waren Bausteine, die eigentlich in allen Prozesslandkarten zu modellieren gewesen wären, in die Übergreifenden Anwendungen ausgelagert worden, um sich in den einzelnen Prozesslandkarten der Geschäftsprozesse nicht jeweils wiederholen zu müssen. Die Gruppierung gleicher Bausteine und Zielobjekte ist auch bei der praktischen Umsetzung anzustreben. Dies wurde im aktuellen Profil noch konsequenter umgesetzt (speziell bei Virtualisierung, Containerisierung und Räumen). Um das noch klarer herauszustellen, wurde die Kapitelreihenfolge der Landkarten so umgestellt, dass die Übergreifenden Anwendungen vor die Landkarten der einzelnen Geschäftsprozesse gestellt wurden. Dies betrifft alle Kapitel, in denen auf die Geschäftsprozesse Bezug genommen wird. Diese Reihenfolge gibt damit auch eine sinnvolle Reihenfolge bei der Umsetzung des Grundschutzprofils vor. Die Bausteine erscheinen nun nur dann in mehreren Landkarten, wenn sich abhängig vom jeweiligen Geschäftsprozess unterschiedliche Umsetzungen der Maßnahmen der Bausteine ergeben könnten (z. B. durch unterschiedliche Bereiche/Verantwortlichkeiten in der jeweiligen Hochschule oder durch unterschiedliche Bewertung des Schutzbedarfs in den einzelnen Bereichen).
Veränderte Clusterung der Übergreifenden Anwendungen	Die Clusterung der einzelnen Anwendungen bzw. Bausteine innerhalb der Übergreifenden Anwendungen wurde neben inhaltlichen Updates nochmals geschärft und (soweit möglich) klarer in Server- bzw. Netzwerk- und Clientdienste unterteilt. Dies hat vor allem Darstellungsgründe, vereinfacht aber auch die Umsetzung. Die Autorinnen und Autoren gehen davon aus, dass beide Landkarten der Übergreifenden Anwendungen gleichermaßen zu betrachten sind.
Klarstellung Risikobehandlung	Kapitel 14 stellt klar, dass Risikoakzeptanz bei Basis-Anforderungen nicht möglich ist.
Redaktionelle Änderungen	Klarstellungen und Fehlerbereinigung

1 Vorwort

Das vorliegende IT-Grundschutz-Profil für Hochschulen wurde vom Arbeitskreis Informationssicherheit des Vereins „Zentren für Kommunikationsverarbeitung in Forschung und Lehre e. V. (ZKI)“ im Rahmen seiner Mitgliedschaft in der Allianz für Cybersicherheit 2019 auf Basis mehrerer Workshops unter Leitung des BSI (Bundesamt für Sicherheit in der Informationstechnik) erstellt.

In den Workshops wurden im Rahmen von Expertenrunden von teils bis zu 50 IT-Sicherheitsbeauftragten, IT-Mitarbeitenden sowie Rechenzentrumsleiterinnen und -leitern und dem BSI repräsentative Kernprozesse an Hochschulen herausgearbeitet. Anschließend wurden die für diese Prozesse typischen Applikationen, deren Schutzbedarf sowie die benötigten IT-Systeme und Räumlichkeiten ermittelt. Im letzten Schritt wurden etwa 80 IT-Grundschutz-Bausteine identifiziert, die Anwendbarkeit der Bausteine auf die Hochschullandschaft geprüft und Umsetzungshinweise erarbeitet. Damit ergibt sich ein hochschulspezifisches IT-Grundschutz-Profil, das als Schablone für die eigene Hochschule adaptiert werden und als Basis für ein Informationssicherheitskonzept der eigenen Hochschule dienen kann.

In Hochschulen ergeben sich durch eine große Breite an Aufgabengebieten in Forschung und Lehre sowie durch die sehr dezentrale Organisation viele unterschiedliche Ausprägungen von IT-Landschaften und deren Management. Dieses IT-Grundschutz-Profil erhebt damit nicht den Anspruch auf Vollständigkeit, sondern kann sich nur auf ausgewählte, in allen Hochschulen ähnliche Kernprozesse konzentrieren. Es soll eine Basis liefern, die von den einzelnen Hochschulen entsprechend der eigenen Ausprägung erweitert werden muss. Die Umsetzung der identifizierten Bausteine sichert nicht nur die betrachteten Kernprozesse ab, sondern verbessert entscheidend auch die Sicherheit der restlichen Hochschulprozesse. Gegebenenfalls müssen individuell weitere Bausteine ergänzt werden. Viele der vorhandenen Prozesse greifen bereits auf Übergreifende Anwendungen und damit auf bereits vordefinierte Bausteine zurück, die auch Basis für viele weitere Prozesse an Hochschulen sind (beispielsweise Identity Management IDM). Zudem gibt es Übergeordnete Bausteine (beispielsweise Sensibilisierung und Schulung oder Sicherheitsmanagement), die für den betrachteten Informationsverbund insgesamt gelten.

Das vorliegende IT-Grundschutz-Profil soll Hochschulen damit wirkungsvoll dabei helfen, die Erstellung eines Informationssicherheitskonzepts auf Basis des IT-Grundschutzes handhabbar zu machen. Der weitere eigene Weg bis zum vollständigen Informationssicherheitskonzept der eigenen Hochschule wird durch dieses IT-Grundschutz-Profil erleichtert.

Wir danken den mehr als 60 Expertinnen und Experten aus den ZKI-Mitgliedshochschulen sowie den Mitarbeiterinnen und Mitarbeitern des BSI für ihre wertvollen Beiträge bei der Erstellung dieses IT-Grundschutz-Profils. Ferner danken wir der Frankfurt University of Applied Sciences für die Bereitstellung der gemeinsamen Arbeitsumgebung und die hervorragende Unterstützung.

Die Sprecher des Arbeitskreises Informationssicherheit im ZKI e. V.

Bernhard Brandel
Manfred Paul

2 Einleitung

2.1 Umfeld

Im Rahmen der aktuellen Bedrohungslage erhält die Informationssicherheit auch im Hochschulumfeld eine immer größer werdende Relevanz. Der Forschungsstandort Deutschland ist attraktiv, damit werden auch Hochschulen zunehmend zu Zielen für Angriffe im IT-Bereich. Aufgrund ihrer offenen Struktur sehen sich Hochschulen hier einer besonderen Herausforderung gegenüber.

Hochschulen weisen bezüglich ihrer Standardprozesse in Forschung, Lehre und Weiterbildung allerdings auch große Ähnlichkeiten auf, was sich auch in einem hohen Organisationsgrad im ZKI e. V. zeigt, in dem ein reger Austausch über Strategien der einzelnen Hochschulen erfolgt. Der Arbeitskreis Informationssicherheit des ZKI hat als Partner der Allianz für Cybersicherheit des BSI zusammen mit Informationssicherheitsbeauftragten und Mitarbeitenden der jeweiligen Rechenzentren dieses IT-Grundschutz-Profil erarbeitet.

2.2 Überblick Sicherheitskonzept

Das nachfolgende Bild zeigt, dass eine Sicherheitskonzeption (Summe aller Maßnahmen) einer Hochschule aus Regeln/Dokumenten, einer treibenden/entscheidenden Organisation und unterstützenden (IT-)Prozessen besteht. Ziel des IT-Grundschutz-Profils ist es, den Hochschulen ein Standardvorgehen an die Hand zu geben, das bei der Erstellung der eigenen Sicherheitskonzeption wertvolle Hilfestellung geben kann.

2.3 Einordnung und Vorgehen

Grundsätzlich gibt es mehrere Vorgehensweisen, die zum Aufbau eines soliden Managementsystems für Informationssicherheit (Information Security Management System, ISMS) bzw. zu Sicherheitskonzepten führen, sowie Standards und Normen in diesem Bereich. In Deutschland haben sich vor allem der IT-Grundschutz des BSI und die Norm ISO/IEC 27001 etabliert.

Der IT-Grundschutz des BSI nähert sich der Informationssicherheit von den Geschäftsprozessen und von den Maßnahmen her, und zwar in Form eines Baukastenprinzips. Die Bausteine enthalten sehr detaillierte Anforderungen zur Absicherung konkreter Zielobjekte (Anwendungen, IT-Infrastruktur, Räume und Gebäude) im sogenannten Informationsverbund.

Darüber hinaus formulieren Übergeordnete Bausteine grundlegende, organisatorische oder personelle Anforderungen, die losgelöst von einzelnen Zielobjekten für den gesamten Informationsverbund gelten.
Das Vorgehen nach IT-Grundschutz, wie es in dem vorliegenden IT-Grundschutz-Profil zur Anwendung kommt, erfolgt in zwei Schritten:

1. Ausgehend von ausgewählten Geschäftsprozessen, erfolgt eine relativ grobe Schutzbedarfsfeststellung in drei Klassen „normal“, „hoch“ bzw. „sehr hoch“ hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit.

2. Bei der anschließenden Modellierung des Informationsverbundes werden den vorhandenen Zielobjekten (Anwendungen, IT-Infrastruktur, Räume und Gebäude) Bausteine des IT-Grundschutz-Kompendiums zugeordnet. Hinzu kommen die Übergeordneten Bausteine.

Im Grunde kann die Modellierung und damit die Umsetzung konkreter Maßnahmen aller für den Informationsverbund relevanten Bausteine zur Erhöhung der Sicherheit aber bereits unabhängig von einer Schutzbedarfsfeststellung beginnen, um damit zunächst eine Basis-Absicherung zu erreichen. Der IT-Sicherheitsprozess kann anschließend mit der Umsetzung der Maßnahmen aus der Kategorie Standard-Absicherung fortgesetzt werden. Spätestens dann folgt eine individuelle Schutzbedarfsfeststellung.

Nur dort, wo ein Schutzbedarf „hoch" oder „sehr hoch" vermutet wird, wird eine Risikoanalyse für das entsprechende Zielobjekt durchgeführt. Diese kann unter Umständen zu der Feststellung führen, dass die vorhandenen Maßnahmen ausreichen oder weitere Maßnahmen getroffen werden müssen. Dabei kann auf die in dem Baustein exemplarisch aufgeführten Anforderungen für erhöhten Schutzbedarf zurückgegriffen werden. Welche Maßnahmen für Zielobjekte mit erhöhtem Schutzbedarf („hoch" oder „sehr hoch") im individuellen Fall ausreichen, ist aus der Risikoanalyse abzuleiten.

Am Ende der Umsetzung des IT-Grundschutz-Profils Hochschule könnte eine ISO-27001-Zertifizierung für die Hochschule (gegebenenfalls auch in Teilbereichen) wie folgt erreicht werden:

- direkte Durchführung einer Zertifizierung des bestimmten Informationsverbundes „nach ISO 27001 auf Basis von IT-Grundschutz" durch das BSI

- klassische ISO-27001-Zertifizierung durch direkte Anwendung der Normen DIN EN ISO/IEC 270xx. Diese betrachten Informationssicherheit mit Blick auf alle relevanten Informationswerte (Assets) einer Organisation, die zu inventarisieren und nach Primärwerten (Prozesse, Informationen) und Sekundärwerten (Hard- und Software, Netzwerk, Personal, Gebäude und Organisation) zu klassifizieren sind. Sie werden dann einem in der ISO/IEC 27005 detailliert beschriebenen Risikomanagementprozess zugeführt. ISO/IEC 27001 beschreibt die Anforderungen an eine Sicherheitsorganisation. Im Anhang A der Norm finden sich die 114 sehr abstrakt gehaltenen Controls (Kriterien) zur Erreichung der Sicherheit. Diese müssen vom Anwender für die jeweiligen Gegebenheiten seiner Organisation konkretisiert und angepasst werden. Hier sind allerdings große Synergien zu den dann bereits angewendeten konkreten Maßnahmen gemäß IT-Grundschutz zu erwarten.

Eine Zuordnung von ISO/IEC 27001 und ISO/IEC 27002 zum IT-Grundschutz findet sich auf der Webseite des BSI, zum Stand der Drucklegung unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_IT_Grundschutz.html aufrufbar.

3 Formale Aspekte

Titel:	IT-Grundschutz-Profil für Hochschulen
Autoren:	siehe Kapitel 6 „Liste der Autorinnen und Autoren"
Herausgeber:	Arbeitskreis Informationssicherheit im ZKI e. V. (Zentren für Kommunikationsverarbeitung in Forschung und Lehre) Kontakt: zki.de/goto/gp-piJ19w
Versionsstand:	2022.0.0, veröffentlicht am 04.08.2022 Informationen zu aktuellen Versionsständen unter zki.de/goto/gp-7tJLTw
IT-Grundschutz-Profil:	Dieses IT-Grundschutz-Profil basiert auf dem IT-Grundschutz-Kompendium des BSI in der Edition 2022.
Revisionszyklus:	Es wird nach Freigabe der Version 2022.0.0 eine jährliche Überprüfung angestrebt.
Vertraulichkeit:	Dieses Dokument darf in unveränderter Version weitergegeben werden.

4 Haftungsausschluss

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorinnen und Autoren haben keinen Einfluss auf die Nutzung dieses IT-Grundschutz-Profils durch Anwenderinnen und Anwender und kennen auch nicht die individuellen Anforderungen an deren Sicherheitskonzepte, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

5 Urheberrecht

6 Liste der Autorinnen und Autoren

An der Erarbeitung dieses Dokumentes waren die Teilnehmerinnen und Teilnehmer der Workshop-Reihe „IT-Grundschutz- Profil für Hochschulen“ beteiligt. Die Workshops wurden vom Arbeitskreis Informationssicherheit des ZKI e. V. veranstaltet, die Moderation lag bei Vertretern des BSI. Die Beteiligten an den bisherigen Versionen werden in der nachfolgenden Tabelle in alphabetischer Reihenfolge aufgeführt.

Name, Vorname	Organisation zum Zeitpunkt der Mitarbeit
Becker, Jochen	TU Darmstadt
Blomenkemper, Irmgard	Universität zu Köln
Brandel, Bernhard	Kath. Univ. Eichstätt-Ingolstadt
Dauwe, Julia	Universität Siegen
Eckhofer, Felix	Technische Universität Bergakademie Freiberg
False, Jana	Technische Universität Ilmenau
Fötinger, Christian	Stabsstelle Informationssicherheit bayerischer Hochschulen
Glowatz, Christoph	Hochschule Düsseldorf
Hilgers, Ursula	Heinrich-Heine-Universität Düsseldorf
Keil, Andreas	Deutsche Sporthochschule Köln
Kellermann, Nils	Philipps-Universität Marburg
Kramert, Grit	Frankfurt University of Applied Sciences
Krohnfuß, Thomas	Universität der Bundeswehr Hamburg
Kryzanowski, Arnold	Hochschule München
Kunze, Rüdiger	GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel
Lauer, Hermann	Universität Heidelberg
Leendertse, Jan	Albert-Ludwigs-Universität Freiburg
Leitel, Jana	Friedrich-Schiller-Universität Jena
Mai, Martin	Universität Bamberg
Michels, Andreas	Universität Duisburg-Essen
Molter, Karl	Hochschule Trier
Neidt, Dirk	Christian-Albrechts-Universität zu Kiel
Paul, Manfred	Hochschule München
Paulsen, Christian	HafenCity Universität Hamburg
Plehn, Hartmut	Universität Bamberg
Porombka, Sebastian	Universität Paderborn
Rentzsch, Sylvia	Universität Magdeburg
Rienecker, Steffen	Universität Leipzig
Sander, Jürgen	DFN-CERT
Sander, Klaus	Stiftung Tierärztliche Hochschule Hannover
Schwarz, Stefan	UniBw München
Topp, Florian	Hochschule Düsseldorf
Ulber, Peter	Universität Stuttgart
Weichert, Ralph	Hochschule RheinMain
Winkhardt, Willi	Hochschulservicezentrum Baden-Württemberg
Zeidan, Adham	Goethe-Universität Frankfurt am Main
Zengerling, Helmut	Universität Mainz

7 Management Summary

7.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an Hochschulleitungen, Informationssicherheitsbeauftragte (ISB, CISOs), CIOs, Rechenzentrumsleitungen, Datenschutzbeauftragte und andere Verantwortliche, die sich aufgrund der oft dezentralen IT-Strukturen an Hochschulen mit Informationssicherheit beschäftigen.

7.2 Einordnung und Zielsetzung

Der Aufbau eines soliden Informationssicherheitsmanagements zur Aufrechterhaltung der Informationssicherheit einer Organisation ist grundsätzlich mit Zeitaufwand und entsprechendem Ressourcenbedarf verbunden. Dieses IT-Grundschutz-Profil für Hochschulen leistet hier eine Hilfestellung. Entstanden aus der gemeinsamen Arbeit von Informationssicherheitsbeauftragten und Mitarbeitenden von Rechenzentren aus mehr als 50 Hochschulen bundesweit, liefert es eine Basis und notwendige Vorarbeiten bei der Erstellung eines eigenen hochschulspezifischen Sicherheitskonzepts auf Basis des IT-Grundschutzes des BSI.

Grundsätzlich gibt es mehrere Vorgehensweisen, die zu Sicherheitskonzepten führen, sowie Standards und Normen in diesem Bereich. In Deutschland haben sich vor allem der IT-Grundschutz, die Norm ISO/IEC 27001 und ISIS12 (für den Bereich mittelständischer Industrie, der hier nicht weiter betrachtet wird) etabliert.

Der IT-Grundschutz nähert sich der Informationssicherheit über die Geschäftsprozesse und die daraus folgenden Anforderungen in Form eines Baukastenprinzips. Ein Baustein-Katalog mit sehr detailliert beschriebenen Anforderungen ermöglicht zunächst eine Basis-Absicherung und anschließend eine Standard-Absicherung. Erst dort, wo in einer ersten Schutzbedarfsfeststellung ein hoher Schutzbedarf angenommen wird, wird eine detaillierte Risikobetrachtung durchgeführt, die dann gegebenenfalls zu einer weiteren Erhöhung des Schutzniveaus oder einer Risikoakzeptanz führen kann.

Ausgehend von fünf Geschäftsprozessen wird ein Informationsverbund (bestehend aus Anwendungen sowie IT- und Gebäude-Infrastruktur) in Form sogenannter Prozesslandkarten modelliert, in denen eine konkrete Zuordnung von Bausteinen des IT-Grundschutz-Kompendiums zu den Prozessen erfolgt. Für die Anwendung der einzelnen Bausteine in der Hochschule werden Umsetzungsempfehlungen gegeben, die von Vertreterinnen und Vertretern der Mitgliedseinrichtungen im Arbeitskreis Informationssicherheit des ZKI kontinuierlich weiterentwickelt werden. Dies ermöglicht z. B. Verweise aus dem eigenen Konzept auf dieses IT-Grundschutz-Profil und die darin empfohlenen konkreten Maßnahmen zur Erhöhung der Informationssicherheit.

Am Ende des Prozesses für die einzelne Hochschule nach dem hier beschriebenen Vorgehen kann auch eine ISO-27001- Zertifizierung (auch in Teilbereichen) stehen. Auch bei einem Vorgehen nach ISO werden zunächst alle relevanten Informationswerte (primäre Assets wie Leistungs- und Führungsprozesse) einer Organisation betrachtet und sekundäre Assets (Hardware) erfasst und priorisiert. Sie werden dann einem Risikomanagementprozess zugeführt, auf dessen Basis dann aus eher allgemein gehaltenen Erläuterungen der ISO Controls konkrete Schutzmaßnahmen definiert werden, die wiederum aus den Anforderungen des IT-Grundschutz-Kompendiums bestehen können.

7.3 Geschäftsprozesse

Aufgrund der großen Ähnlichkeit der Geschäftsprozesse in den Bereichen Forschung, Lehre und Weiterbildung an Hochschulen gibt dieses IT-Grundschutz-Profil eine allgemeine Handlungsanweisung zur Umsetzung von Maßnahmen, die einfach auf die individuellen Rahmenbedingungen einer Hochschule übertragen werden kann. Im Fokus dieses IT-Grundschutz-Profils stehen dabei zunächst fünf Geschäftsprozesse:

- Übergreifende Anwendungen
- Bewerbung und Zulassung
- Immatrikulation und Studierendenmanagement
- Prüfungen
- IT-Infrastruktur für Studierende

Um den Handlungsbedarf für eine ganze Hochschule zu bestimmen, müssen alle ihre Geschäftsprozesse entsprechend der Vorgehensweise dieses IT-Grundschutz-Profils betrachtet, Schutzmaßnahmen ausgewählt und diese in ein Informationssicherheitskonzept aufgenommen werden. Die oben genannten Geschäftsprozesse stellen hier zwar einen Einstieg dar, umfassen aber bereits einen Großteil der notwendigen Bausteine bezüglich der vorhandenen Dienste- und Netzwerkinfrastruktur einer Hochschule.

Es wird davon ausgegangen, dass für weitere Geschäftsprozesse z. B. in der Hochschulverwaltung (Finanzwesen etc.) oder in Forschung und Weiterbildung aufgrund vorhandener Überschneidungen zu den hier betrachteten Maßnahmen nur noch sehr wenige zusätzliche Bausteine und Maßnahmen zu betrachten sind. Der ZKI-Arbeitskreis Informationssicherheit hat sich zum Ziel gesetzt, das vorliegende IT-Grundschutz-Profil zukünftig um weitere Geschäftsprozesse in den Bereichen Forschung und Verwaltung zu ergänzen.

7.4 Vorgehen

Der IT-Grundschutz unterscheidet zwischen der Umsetzung von Maßnahmen aus sogenannten Übergeordneten Bausteinen, die vor allem konzeptionelle und organisatorische Maßnahmen beinhalten, sowie aus den im Rahmen der o. g. Geschäftsprozesse definierten Bausteinen und empfiehlt eine entsprechende Reihenfolge (sichtbar in den Prozesslandkarten dieses Profils). Der Einstieg in ein Sicherheitskonzept sollte grundsätzlich mit einigen der Übergeordneten Bausteine wie der Einführung eines ISMS, einiger weiterer Maßnahmen im Bereich Organisation und Personal sowie der Kern-IT-Prozesse beginnen. Erst in zweiter Linie sollten dann die Maßnahmen umgesetzt werden, die sich aus der konkreten Betrachtung der Geschäftsprozesse ergeben.

.

In allen Bausteinen sind Anforderungen zur Basis-Absicherung, zur Standard-Absicherung und für erhöhten Schutzbedarf beschrieben. Die Autorinnen und Autoren empfehlen bei der Umsetzung aller Anforderungen, zuerst mit dem Ziel der Basis-Absicherung zu beginnen und anschließend die Standard-Absicherung und gegebenenfalls den höheren Schutzbedarf abzudecken und so Schritt für Schritt das Sicherheitsniveau zu erhöhen.

Darüber hinaus kann das IT-Grundschutz-Profil Hilfestellung bei der Durchführung einer weiterführenden Schutzbedarfsfeststellung und Risikoanalyse leisten, wenn die Schutzbedarfskategorien „hoch“ bzw. „sehr hoch“ zugrunde gelegt werden sollen. Informationen hierzu sind in Kapitel 13 bzw. 14 zu finden. In Fällen, in denen ein hoher Schutzbedarf besteht, ist eine individuelle Risikobewertung durchzuführen um festzustellen, ob die oben genannten Anforderungen zur Basis- bzw. Standard-Absicherung ausreichen oder ob weitere Anforderungen erforderlich werden. Diese sind ebenfalls – aber nicht normativ – mit angegeben und mit Umsetzungshinweisen für die einzelnen Bausteine versehen.

Im Rahmen des ISMS muss dieses Informationssicherheitskonzept dann regelmäßig überprüft und fortgeschrieben werden.

8 Festlegung des Geltungsbereichs (Scope)

8.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an Hochschulen.

8.2 Schutzbedarf

In diesem IT-Grundschutz-Profil wird der Schutzbedarf der einzelnen Anwendungen in den betrachteten Teilprozessen mit definiert. Details zur Bedeutung der einzelnen Schutzbedarfskategorien finden sich in Kapitel 13. In den meisten Fällen gehen die Autorinnen und Autoren von „normalem“ Schutzbedarf aus. Gleichzeitig empfehlen sie, an einigen ausgewählten Stellen den Schutzbedarf „hoch“ anzusetzen, was nach der IT-Grundschutz-Methode eine individuelle Risikoanalyse notwendig macht. Die Risikoanalyse wird im Rahmen dieses IT-Grundschutz-Profils nicht durchgeführt. Die individuelle Umsetzung des IT-Grundschutz-Profils bringt die Notwendigkeit mit sich, die hier als Empfehlung formulierten Schutzbedarfskategorien individuell zu prüfen und gegebenenfalls anzupassen.

Nachdem die Verarbeitung von Studierendendaten aber das Kerngeschäft einer Hochschule ausmacht und diese entsprechend sensibel zu behandeln sind, wurde teilweise in diesen Prozessen ein hoher Schutzbedarf definiert. Ein Beispiel ist die Einschätzung eines hohen Schutzbedarfs beim Prozess Immatrikulation und Studierendenmanagement bezüglich Vertraulichkeit. Dasselbe gilt beim Prozess Prüfungen bezüglich Vertraulichkeit (hoch) und Integrität (hoch), teilweise auch bezüglich Verfügbarkeit (hoch), zumindest bei der Durchführung elektronischer Prüfungen. Diese Einschätzungen können von Hochschule zu Hochschule abweichen und bedürfen gegebenenfalls einer gesonderten Prüfung. Die getroffenen Maßnahmen sind dann entsprechend anzupassen.

8.3 IT-Grundschutz-Vorgehensweise

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen für Hochschulen und verwenden die Basis- und Standard-Absicherung nach dem BSI-Standard 200-2. Gemäß IT-Grundschutz ist es empfehlenswert, zunächst mit einer Basis-Absicherung zu beginnen und perspektivisch mindestens die Standard-Absicherung gemäß IT-Grundschutz anzustreben und umzusetzen.

8.4 ISO-27001-Kompatibilität

Dieses IT-Grundschutz-Profil empfiehlt Maßnahmen zur Basis- und Standard-Absicherung. Ein mit ISO 27001 konformes Sicherheitsniveau wird bei Prozessen mit Schutzbedarf „normal“ erst mit Anwendung der IT-Grundschutz-Vorgehensweise mit „Standard-Absicherung“ erreicht. Bei (Teil-)Prozessen mit Schutzbedarf „hoch“ wird dieses Niveau erst nach der Durchführung von Risikoanalysen und gegebenenfalls der Anwendung erweiterter Maßnahmen erreicht. Dabei kann auf die in den Bausteinen exemplarisch aufgeführten Anforderungen für erhöhten Schutzbedarf zurückgegriffen werden. Damit ist dann bei Bedarf eine direkte Zertifizierung gemäß ISO 27001 für IT-Grundschutz möglich.

Bei einer klassischen ISO-27001-Zertifizierung durch direkte Anwendung der ISO-27001-Norm ist davon auszugehen, dass nach Etablierung eines Risikomanagementprozesses bei der Definition geeigneter Maßnahmen große Synergien zum bereits durchgeführten IT-Grundschutz vorhanden sind.

9 Abgrenzung des Informationsverbundes

9.1 Bestandteile des Informationsverbundes

Zum Informationsverbund gehören alle Prozesse und Verfahren in einer Hochschule, die für die Abwicklung der Kernaufgaben Forschung, Lehre und Weiterbildung notwendig sind. Das vorliegende IT-Grundschutz-Profil konzentriert sich dabei auf Kernprozesse im Rahmen der Lehre. Im Einzelnen sind dies die folgenden Prozesse und Verfahren:

- Übergreifende Anwendungen (Basisdienste)
- Bewerbung und Zulassung
- Immatrikulation und Studierendenmanagement
- Prüfungen
- IT-Infrastruktur für Studierende

9.2 Nicht berücksichtigte Objekte

Im IT-Grundschutz-Profil für Hochschulen werden über die in Kapitel 9.1. benannten Prozesse hinausgehende Prozesse, die zur Erfüllung weitergehender Aufgaben von Hochschulen erforderlich sind, nicht berücksichtigt. Bezüglich der Auswahl der IT-Grundschutz-Bausteine besteht eine große Überschneidung zu anderen Hochschulprozessen, sodass sich der Ergänzungsaufwand gemäß Einschätzung der Autorinnen und Autoren im Rahmen halten sollte. Diese weiteren Prozesse müssen entsprechend der hier vorgestellten Vorgehensweise noch individuell berücksichtigt werden.

9.3 Verbindung zu anderen IT-Grundschutz-Profilen

Zu diesem Zeitpunkt gibt es keine Verweise auf andere IT-Grundschutz-Profile.

9.4 Weiterführende Arbeiten

Das vorliegende IT-Grundschutz-Profil wurde unter Betrachtung ausgewählter Prozesse bzw. Basisdienste (siehe Kapitel 9.1) entwickelt. Diese decken nicht den vollständigen Bedarf umzusetzender Maßnahmen für die gesamte Hochschule ab. Welche weiteren Maßnahmen überprüft und in einem folgenden ergänzenden IT-Grundschutz-Profil für Hochschulen hinzuzufügen sind, muss in weiteren individuellen Projekten oder zentralen Arbeitssitzungen erhoben werden. Neben der Betrachtung der restlichen Prozesse aus dem Campus Management sind Anforderungen der Zentralverwaltung und der Forschung zu evaluieren.

Da für Zielobjekte des Campus Managements bereits weitgehende Betrachtungen durchgeführt wurden, sind für die weitere Bearbeitung insbesondere die Prozesse zu untersuchen, die neue Zielobjekte (IT-Systeme oder Anwendungen) erfordern. Anforderungen der Zentralverwaltung sind zusätzlich in Hinblick auf behördliche Aufgaben und mögliche Anbindungen an Netze des öffentlichen Dienstes zu betrachten. Spezielle Anforderungen der Forschungsumgebungen variieren mit den dort abgewickelten Projekten und werden nur Musterumgebungen für Forschungsprojekte unterschiedlicher Sensibilität abbilden. Hier werden vor allem Bausteine für die Zusammenarbeit mit Dritten von Bedeutung sein.

Ein detaillierter Überblick über die untersuchten Prozesse und geprüften Bausteine ist in Kapitel 11 zu finden.

Diese sind schrittweise zu erweitern. Durch die Untersuchung von wenigen Prozessen und ausgewählten Basisdiensten konnte mit diesem IT-Grundschutz-Profil die Prüfung und Erarbeitung von Umsetzungsempfehlungen für ca. 75% der vom BSI verfügbaren Bausteine erfolgen.

Daher wird in der Folge der Schwerpunkt auf der Untersuchung weiterer Prozesse und IT-Dienste sowie der Zuordnung zu bereits geprüften Bausteinen liegen und nur zu einem geringeren Teil in der Prüfung neuer Bausteine. Erst der Abschluss dieser Arbeiten wird ein vollständiges IT-Grundschutz-Profil für Hochschulen ergeben. In jedem Fall kann parallel zu den kommenden Arbeiten mit der Umsetzung der hier geprüften Bausteine begonnen werden.

9.5 Ausblick

Die Situation durch Auftreten von COVID-19 verursachte einen starken Wandel an den Hochschulen hin zu deutlich mehr Digitalisierung. Damit treten auch Prozesse in den Vordergrund, die zuvor noch nicht im Fokus standen oder noch nicht in der inzwischen benötigten Tiefe betrachtet wurden.

Allen voran steht das Thema Videoconferencing. Hierzu erschien im zweiten Quartal 2020 das „Kompendium Videokonferenzsysteme“ des BSI (KoViKo 1.0.1). Die Anforderungen an die Sicherheit bei Systemzugängen, bei der Authentifizierung und bei Cloud-Dienstleistungen wurden zudem deutlich erhöht.

Diese neuen Aspekte sollten diskutiert, priorisiert und gegebenenfalls in die Prozesslandkarten aufgenommen und – sobald vorhanden – in den Bausteinen kommentiert werden.

10 Referenzarchitektur

Die Referenzarchitektur (auch „Untersuchungsgegenstand“ genannt) legt fest, auf welche Objekte die Anforderungen des IT-Grundschutzes im Sinne dieses IT-Grundschutz-Profils angewendet werden müssen. Dazu gehören:

- Geschäftsprozesse
- Anwendungen (Software-Programme)
- vorhandene IT-Systeme (u. a. Clients, Server, Netzkopplungselemente, Mobile Devices) sowie eingesetzte Netze, Kommunikationseinrichtungen, externe Schnittstellen
- räumliche Gegebenheiten und Infrastruktur (Liegenschaften, Gebäude, Räume)

10.1 Untersuchungsgegenstand

Im Folgenden werden die in diesem IT-Grundschutz-Profil betrachteten Geschäftsprozesse kurz beschrieben. Diese umfassen im Wesentlichen Prozesse im Zusammenhang mit der Lehre. Zunächst werden alle übergreifenden Dienste und Anwendungen betrachtet, die im Zusammenhang mit den nachfolgenden Prozessen stehen und von Mitarbeitenden der Hochschulen sowie (zumindest teilweise) von Studierenden genutzt werden:

- Übergreifende Anwendungen

Die drei Prozesse
- Bewerbung und Zulassung,
- Immatrikulation und Studierendenmanagement sowie
- Prüfung

werden im Allgemeinen über ein sogenanntes Campus Management System als integrierte Anwendung abgewickelt. In diesem IT-Grundschutz-Profil wird exemplarisch HISinOne betrachtet. Die IT-Grundschutz-Vorgehensweise lässt sich grundsätzlich genauso aber auch für andere an Hochschulen im Einsatz befindliche Systeme übernehmen, wie z. B.:

- HIS POS-GX/QIS
- SAP SLcM
- Campusnet (Datenlotsen)
- CAMPUSonline
- PRIMUSS
- FactScience (im Bereich medizinischer Studiengänge im Einsatz)

Die entsprechenden Unterprozesse sind in den Prozesslandkarten in Kapitel 15 detailliert dargestellt.

10.1.1 Übergreifende Anwendungen

Nachfolgend sind übergreifend verwendete Anwendungen im Rahmen der genannten Prozesse zusammengestellt. Diese sind großteils für die oben genannten Prozesse unabdingbare Voraussetzung (z. B. IDM, virtuelle Serverdienste) oder werden von Mitarbeitenden und Studierenden ebenfalls verwendet (z. B. E-Mail-Plattform):

- Identity Management
- Verzeichnisdienste (AD/LDAP)
- DFN-AAI
- Virtuelle Serverdienste
- Groupware/E-Mail-Plattform/Chat
- Netzwerk-/Internetzugang/LAN
- Kubernetes (Containerisierung)
- Webauftritt der Hochschule
- Telefonie
- Remote-Zugang (WLAN/eduroam, VPN)
- Arbeitsplatz-/Office-PCs für Mitarbeitende im Verwaltungsbereich
- Arbeitsplatz-PCs allgemein
- Endpoint-Security
- Arbeitsplatzbereitstellung
- Mobile Device Management
- IT Servicemanagement

10.1.2 Geschäftsprozess Bewerbung und Zulassung

„Bewerbung“ umfasst die Einrichtung von Bewerbungsverfahren für grundständige und Masterstudiengänge (inklusive verschiedener Studierendengruppen – auch z. B. Hochschulwechsler, Gasthörer, Zweithörer –, Bewerbungszeiträume, Kapazitäten, Bewerbungsvoraussetzungen und rechtlicher Rahmenbedingungen), die Entgegennahme von Bewerbungen in den verschiedenen Ausprägungen sowie deren Überprüfung und gegebenenfalls Bewertung (z. B. zur Notenverbesserung durch außerschulische Leistungen). „Zulassung“ beinhaltet in zulassungsbeschränkten und freien Studiengängen die Zulassung (bzw. Ablehnung) von Bewerberinnen und Bewerbern, gegebenenfalls auch nur für bestimmte Bewerbergruppen, zu Studiengängen in den verschiedenen Varianten (z. B. durch Ranking, Auswahlgespräche) sowie Annahmeverfahren (der Bewerberinnen und Bewerber).

Anwendungen:
- Campus Management System: HISinOne APP (Webserver, Datenbank, Applikationsserver), ggf. andere
- E-Learning-System (teilweise für E-Bewerbungen im Einsatz)
- Office-PC

Schnittstellen zu externen Systemen:
- DOSV-Portal (hochschulstart.de)
- Uni-Assist (extern)

10.1.3 Geschäftsprozess Immatrikulation und Studierendenmanagement

„Immatrikulation“ umfasst die Einschreibung zugelassener Bewerberinnen und Bewerber (die den Studienplatz angenommen haben) und der Bewerberinnen und Bewerber für zulassungsfreie Studiengänge. Dies beinhaltet außerdem die Erzeugung und Bereitstellung bzw. den Versand der zugehörigen Bescheide.„Studierendenmanagement“ umfasst die Verwaltung aller an der Hochschule eingeschriebenen Personen (z. B. Haupt-, Neben-, Gasthörer, Früh- und Seniorenstudierende). Dies umfasst Änderungen von Stammdaten, Studiengang- und Fachwechseln, Vertiefungswahlen, Rückmeldungen, Beurlaubungen, Praxis- und Auslandssemester, Führen von Studienkonten und Ausbildungspartnerdaten bei dualen Studienprogrammen sowie Exmatrikulationen.

Bei dieser Betrachtung ausgeklammert wurde der Bereich „Beiträge und Gebühren“.

Anwendungen:
- Campus Management System: Modul HISinOne STU
- Hochschulportal & IDM (Studierendenlogin)
- Intercard (Hochschulkarte)

10.1.4 Geschäftsprozess Prüfung

Der Hauptprozess „Prüfung“ umfasst, aufbauend auf den Prüfungsordnungen, die Klärung der Zulassungsvoraussetzungen, die Prüfungsplanung pro Semester bzw. Prüfungsphase und deren Veröffentlichung. In diesem Zusammenhang wird der Begriff Prüfung für alle verschiedenen Prüfungsformen verwendet, wie z. B. mündliche Prüfungen, Präsentationen, Hausarbeiten, Klausuren und Abschlussprüfungen (Bachelor-/Master-/Diplomarbeit). Der Hauptprozess beinhaltet außerdem die Anmeldung, Zulassung, ggf. Abmeldung von Studierenden zu Prüfungen sowie die Prüfungsdurchführung. Darüber hinaus schließt er die Ermittlung, Dokumentation, Bescheinigung und Veröffentlichung der Prüfungsergebnisse ein.

Anwendungen:

- Campus Management System: Modul HISinOne EXA
- LPLUS
- Arbeitsumgebung für E-Prüfungen: Citrix, LanDesk etc.
- EvaExam
- Moodle
- Dokumentenmanagementsystem, z. B. Codia

10.1.5 Geschäftsprozess IT-Infrastruktur für Studierende

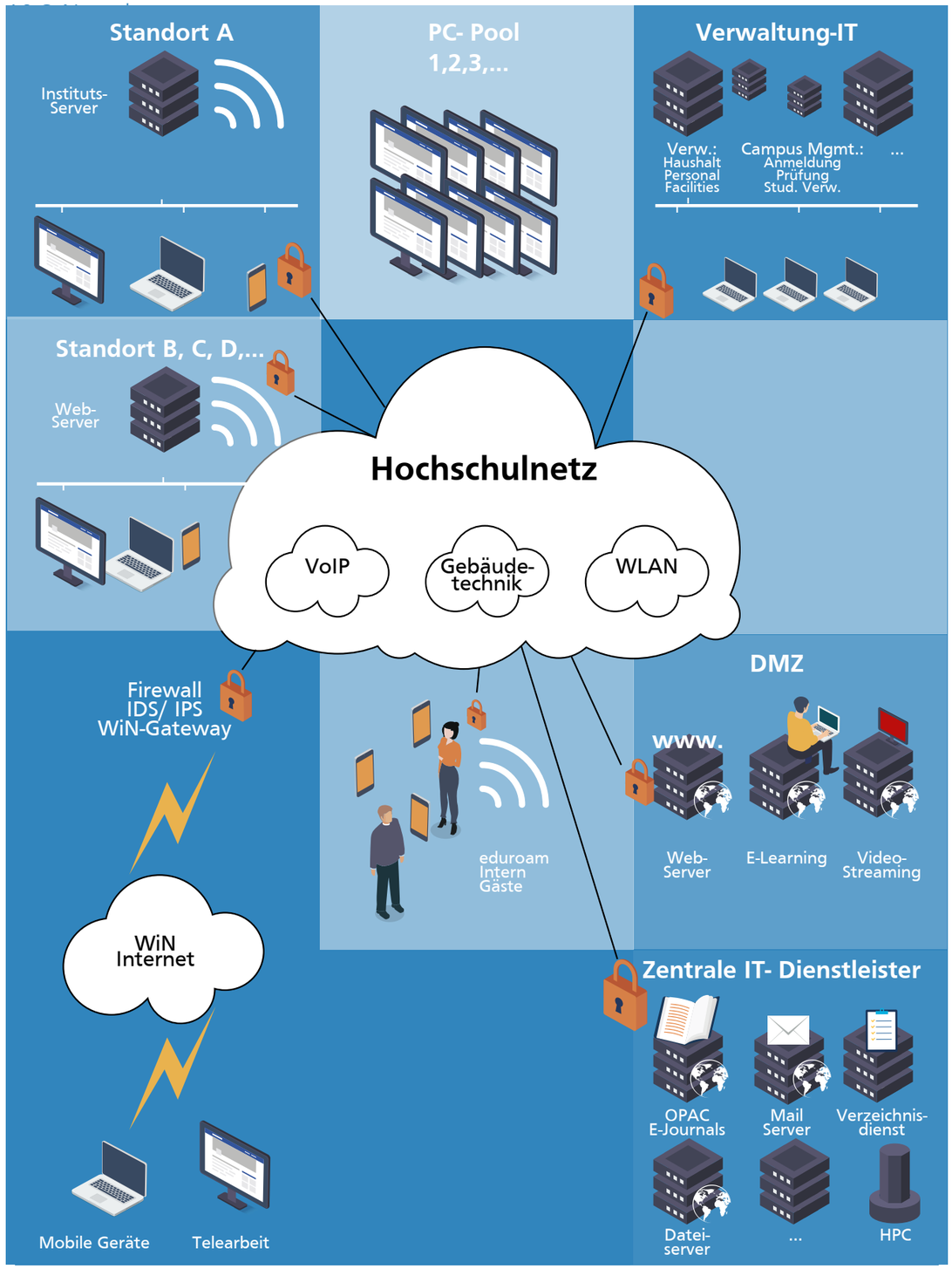
Dieser Prozess beinhaltet die Bereitstellung einer Arbeitsumgebung im Rahmen von Studium und Lehre.

Diese Arbeitsumgebung umfasst die Bereitstellung von zentralen Diensten mit externem Zugang durch eigene Geräte sowie internem Zugang durch zentral bereitgestellte Systeme sowie die darunterliegende Netzwerkinfrastruktur. In diesem IT-Grundschutz-Profil wird davon ausgegangen, dass ein BYOD-Zugang (Bring-Your-Own-Device) seitens der Studierenden auf Hochschuldienste nur über WLAN erfolgt und darüber hinaus PC-Pools mit gewarteten Rechnern in Räumen der Hochschule zur Verfügung gestellt werden. Insofern werden folgende zentrale Dienste zur Verfügung gestellt:

- Bereitstellung von PC-Pools
- Softwareangebote (Download) für Studierende
- E-Learning-Plattform
- Chat-/Messenger-Plattform
- Veranstaltungsaufzeichnung
- zentraler Speicherplatz
- Print-Services
- Nutzersupport

10.2 Umgang mit Abweichungen und Ergänzungen

Von dieser Referenzarchitektur abweichende oder zusätzliche Zielobjekte des zu schützenden Informationsverbundes der jeweiligen Hochschule sind entsprechend der obigen Vorgehensweise zu dokumentieren. Diesen Zielobjekten sind dann geeignete Bausteine zuzuordnen. Diese können durch die Verwendung in anderen Zielobjekten bereits betrachtet worden sein. Gegebenenfalls sind weitere geeignete Bausteine des IT-Grundschutz-Kompendiums, sofern vorhanden, zuzuordnen.



11 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Anhand der Referenzarchitektur lassen sich passende IT-Grundschutz-Bausteine auswählen. Sie enthalten Erläuterungen zu Gefährdungslage und Sicherheitsanforderungen sowie weiterführende Informationen.

Die in diesem IT-Grundschutz-Profil aufgeführten Bausteine aus dem IT-Grundschutz-Kompendium sind für die Erreichung des angestrebten Sicherheitsniveaus im Regelfall ausreichend. Um ein ISO/IEC 27001-konformes Schutzniveau zu erreichen, sind mindestens alle Basis- und Standard-Anforderungen der Bausteine aus Kapitel 11.2 und 11.3 auf geeignete Weise umzusetzen. Vom IT-Grundschutz-Profil abweichende Einsatzumgebungen oder Komponenten erfordern unter Umständen die Anwendung weiterer Bausteine. Daher ist im Rahmen der Anwendung des IT-Grundschutz-Profils eine Überprüfung notwendig.

Zu vielen Bausteinen gibt es zusätzlich Umsetzungshinweise mit detaillierten Beschreibungen passender Sicherheitsmaßnahmen seitens des BSI, die als Grundlage für die Sicherheitskonzeption verwendet werden können. Zudem wurden die in diesem IT-Grundschutz-Profil genannten Bausteine auf Anwendbarkeit im Hochschulumfeld überprüft, gegebenenfalls werden ergänzende Umsetzungshinweise gegeben.

Unterschieden wird zwischen

- übergeordneten, meist organisatorischen Bausteinen (prozessorientierten Bausteinen), die jeweils für die gesamte Hochschule umzusetzen sind, und
- Bausteinen, deren Umsetzung sich aus Betrachtung der einzelnen Geschäftsprozesse ergibt und die in einzelnen Prozesslandkarten dargestellt sind (systemorientierte Bausteine).

Für die Umsetzung der Bausteine empfiehlt das IT-Grundschutz-Kompendium eine Reihenfolge bei der Umsetzung und unterscheidet speziell bei den Übergeordneten Bausteinen zwischen:

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
- R2: Diese Bausteine sollten als Nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

Die empfohlene Reihenfolge der Maßnahmen ist in Kapitel 11.2 dargestellt. Die Bausteine der Prozesslandkarten (systemorientierte Bausteine) sind in der Regel alle mit „R2“ vorgegeben.

Innerhalb der Bausteine wird zwischen Anforderungen und Maßnahmen zur Basis-Absicherung, zur Standard-Absicherung und zur Erfüllung von Anforderungen für erhöhten Schutzbedarf unterschieden.

Empfohlen wird daher ein iterativer Sicherheitsprozess, der mit dem Aufbau eines Information Security Management Systems (ISMS) und den ersten Bausteinen aus den Bereichen Organisation und Personal, Konzepte und Vorgehensweisen sowie Maßnahmen für den Kernbetrieb startet, bevor überhaupt mit der Umsetzung der Bausteine auf den Landkarten der einzelnen Geschäftsprozesse begonnen werden sollte. Zudem wird empfohlen, bei allen Bausteinen zuerst die Umsetzung der Maßnahmen zur Basis-Absicherung sicherzustellen, um dann schrittweise die übrigen Maßnahmen zur Standard- Absicherung oder darüber hinaus nachzuziehen.

11.1 „Landkarten“ der Prozesse

Die wesentlichen Geschäftsprozesse wurden im vorherigen Kapitel beschrieben, sie sind als Prozesslandkarten in Kapitel 15 dargestellt. Die Landkarten zeigen alle wesentlichen Erkenntnisse aus der Strukturanalyse und der Modellierung (Auswahl passender IT-Grundschutz-Bausteine).

Für jeweils einen Geschäftsprozess werden die Referenzarchitektur (Anwendungen, IT-Systeme sowie Räumlichkeiten) und die Zuordnung der IT-Grundschutz-Bausteine dargestellt. Wo keine Zuordnung bestehender Bausteine erfolgen kann, sind eine eigene Risikoanalyse und gegebenenfalls hochschulspezifische Lösungen notwendig.

In Form von Grafiken bieten die Landkarten quasi alles auf einen Blick und eröffnen so einen Einstieg in den individuellen IT-Sicherheitsprozess. Sie können sowohl als Entscheidungsgrundlage für die Hochschulleitung als auch als „Umsetzungs-Fahrplan“ für den IT-Sicherheitsmanagementprozess dienen.

Die Landkarten zu den hier behandelten Geschäftsprozessen, Hinweise zur deren Nutzung und Erklärungen der verwendeten Symbole sind in Kapitel 15 zu finden:

- Übergreifende Anwendungen
- Bewerbung und Zulassung
- Immatrikulation und Studierendenmanagement
- Prüfungen
- IT-Infrastruktur für Studierende

Die Herangehensweise in diesem IT-Grundschutz-Profil sieht vor, dass bei der jeweiligen Anwendung als Mindestmaß die Basis-Anforderungen der jeweiligen Bausteine umgesetzt werden müssen und anschließend die Standard-Anforderungen nachgezogen werden sollten. Teilweise sind aufgrund hohen Schutzbedarfs in Einzelfällen auch die in den Bausteinen genannten erweiterten Anforderungen umzusetzen.

11.2 Übersicht I: Übergeordnete Bausteine

Die in diesem Kapitel dargestellten Bausteine sind nicht in den Landkarten zu finden, da sie sich eher auf den gesamten Informationsverbund beziehen und nicht auf einzelne Zielobjekte. Diese Bausteine sind für ein ganzheitliches Konzept eines Informationssicherheitssystems notwendig. Der Aufwand in der konkreten Ausgestaltung hängt stark von den individuellen Gegebenheiten an den einzelnen Hochschulen ab.

Die Reihenfolge der Umsetzung empfiehlt sich, wie oben bereits beschrieben, gemäß Kennzeichnung R1 bis R3. Neu im IT-Grundschutz-Kompendium 2022 ist die Zuordnung der Bausteine APP.7 (Entwicklung von Individualsoftware), SYS.3.2.2 (Mobile Device Management) und INF.9 (Mobiler Arbeitsplatz) zum gesamten Informationsverbund. Der Baustein APP.7 findet sich daher in der nachfolgend dargestellten Landkarte für die Übergeordneten Bausteine.

Nachdem die Übergreifenden Anwendungen im hier vorliegenden Grundschutzprofil allerdings ebenfalls als Basis für die anderen Geschäftsprozesse dienen, werden die Bausteine SYS.3.2.2 sowie INF.9 neben den anderen SYS- und INF-Bausteinen dort modelliert.

Der Baustein APP.6 (Allgemeine Software) wurde aus Gründen der Übersichtlichkeit in die nachfolgend dargestellte Landkarte für die Übergeordneten Bausteine übernommen, um ihn nicht bei allen APP-Bausteinen der übrigen Prozesslandkarten darstellen zu müssen. Er ist jedoch trotzdem für jede Anwendung separat zu betrachten.

Prio	Sicherheits-management	Organisation und Personal	Konzepte und Vorgehensweisen	Betrieb	Detektion und Reaktion
R1	Sicherheits-management **ISMS.1**	Organisation **ORP.1** Personal **ORP.2** Sensibilisierung und Schulung zur Informationssicherheit **ORP.3** Identitäts- und Berechtigungsma-nagement **ORP.4**	Datensicherungs-konzept **CON. 3** Löschen und Vernichten **CON. 6**	Ordnungsgemäße IT Administration **OPS.1.1.2.** Patch- und Äderungsmanagement **OPS.1.1.3.** Schutz vor Schadprogrammen **OPS.1.1.4.** Protokollierung **OPS.1.1.5** Software-Tests und -Freigaben **OPS.1.1.6**	
R2			Datenschutz_ **CON. 2** Entwicklung von Webanwendungen **CON. 10** Allgemeine Software **APP:6**	Systemmanagement **OPS.1.1.7** NTP-Zeitsynchronisation **OPS.1.2.6** Cloud-Nutzung **OPS. 2.2**	Detektion von sicherheitsrelevanten Ereignissen **DER.1** Behandlung von Sicherheitsvorfällen **DER.2.1**
R3		Compliance Management (Anforderungs-management) **ORP.5**	Kryptokonzept **CON. 1** Informationsicherheit auf Auslandsreisen **CON. 7** Software-Entwicklung **CON. 8** Informations-Austausch **CON.9** Entwicklung von Individualsoftware **APP.7**	Archivierung **OPS.1.2.2** Telearbeit **OPS.1.2.4** Fernwartung **OPS.1.2.5** Outsourcing für Kunden **OPS.2.1** Outsourcing für Dienstleister **OPS.3.1**	Vorsorge für die IT-Forensik **DER.2.2** Bereinigung weit-reichender Sicherheits-vorfälle **DER.2.3** Audits und Revisionen **DER.3.1** Notfallmanagement **DER.4**

11.3 Übersicht II: Bausteine aus den Prozesslandkarten

Die in diesem Kapitel aufgelisteten Bausteine finden sich auch in den Landkarten in Kapitel 15 und sind dort einzelnen Zielobjekten zugeordnet. Auf eine Kennzeichnung der empfohlenen Priorität bei der Umsetzung wurde bei den einzelnen Bausteinen verzichtet, sie liegt bei allen Bausteinen auf Priorität R2. Damit lautet die Empfehlung, bei der Einführung einer Sicherheitskonzeption erst mit den mit R1 priorisierten Übergeordneten Bausteinen zu beginnen und erst danach mit den Bausteinen dieses Kapitels, die ebenfalls in den Prozesslandkarten zu finden sind, fortzufahren. Wie bereits erwähnt, sollte dabei jeweils zunächst die Basis-Absicherung im Vordergrund stehen, um dann die Maßnahmen zur Standard-Absicherung oder gegebenenfalls darüber hinausgehende Maßnahmen nachzuziehen.

11.3.1 APP: Anwendungen

- APP.1.1 Office-Produkte
- APP.1.2 Web-Browser
- APP.1.4 Mobile Anwendungen (Apps)
- APP.2.1 Allgemeiner Verzeichnisd
- APP.2.2 Active Directory
- APP.2.3 OpenLDAP
- APP.3.1 Webanwendungen und Webservices
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.4 Samba*
- APP.3.6 DNS-Server
- APP.4.2 SAP-ERP-System*
- APP.4.3 Relationale Datenbanken
- APP 4.4 Kubernetes
- APP.5.2 Microsoft Exchange und Outlook
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.6 Allgemeine Software**
- APP.7 Entwicklung von Individualsoftware***

* Diese Bausteine sind in Einzelfällen (Vorhandensein entsprechender Installationen in der Hochschule) anzuwenden, wurden im Rahmen der Prozess-Modellierung und in den Kommentierungen des Grundschutzprofils aber nicht näher berücksichtigt.

** Der Baustein APP.6 wurde aus Gründen der Übersichtlichkeit in der Landkarte der Übergeordneten Bausteine in Kapitel 11.2 modelliert, auch wenn er in den einzelnen Geschäftsprozessen zu betrachten ist.

*** Der Baustein APP.7 ist laut IT-Grundschutz-Kompendium 2022 dem Bereich Informationsverbund/übergreifende Aspekte zugeordnet und ebenfalls in Kapitel 11.2 modelliert.

11.3.2 SYS: Systeme

- SYS.1.1 Allgemeiner Server
- SYS.1.2.2 Windows Server 2012
  Für Windows Server 2016 wird empfohlen, den benutzerdefinierten Baustein SYS.bd.1 mit zu betrachten, für Windows Server 2019 den Baustein SYS.1.2.3 Windows Server 2019 (Community Draft).
- SYS.1.3 Server unter Linux und Unix
- SYS.1.5 Virtualisierung

- SYS.1.6 Containerisierung
- SYS.1.8 Speicherlösungen
- SYS.2.1 Allgemeiner Client
- SYS.2.2.3 Clients unter Windows 10 (ältere Versionen werden hier nicht mehr betrachtet)
- SYS.2.3 Clients unter Linux und Unix
- SYS.2.4 Clients unter macOS
- SYS.3.1 Laptops
- SYS.3.2.1 Allgemeine Smartphones und Tablets
- SYS.3.2.2 Mobile Device Management (MDM)*
- SYS.3.2.3 iOS (for Enterprise)
- SYS.3.2.4 Android
- SYS.3.3 Mobiltelefon
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
- SYS.4.4 IoT**
- SYS.4.5 Wechseldatenträger

* Der Baustein SYS.3.2.2 ist laut IT-Grundschutz-Kompendium 2022 dem Bereich Informationsverbund/übergreifende Aspekte zuzuordnen, wurde aber aus Gründen der Übersichtlichkeit in der Prozesslandkarte Übergreifende Anwendungen in Kapitel 15 modelliert.

** Der Baustein SYS.4.4 ist in Einzelfällen (Vorhandensein entsprechender Installationen in der Hochschule) anzuwenden, wurde im Rahmen der Prozess-Modellierung und in den Kommentierungen des Grundschutzprofils aber nicht näher berücksichtigt.

11.3.3 NET: Netze und Kommunikation

- NET.1.1 Netzarchitektur und -design
- NET.1.2 Netzmanagement
- NET.2.1 WLAN-Betrieb
- NET.2.2 WLAN-Nutzung
- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN
- NET.4.1 TK-Anlagen
- NET.4.2 VoIP

11.3.4 INF: Infrastruktur

- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz*
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume
- INF.12 Verkabelung
- INF.13 Technisches Gebäudemanagement
- INF.14 Gebäudeautomation**

* Der Baustein INF.9 ist laut IT-Grundschutz-Kompendium 2022 dem Bereich Informationsverbund/übergreifende Aspekte zuzuordnen, wurde aber aus Gründen der Übersichtlichkeit in der Prozesslandkarte Übergreifende Anwendungen in Kapitel 15 modelliert

** Der Baustein INF.14 ist in Einzelfällen (Vorhandensein entsprechender Installationen in der Hochschule) anzuwenden, wurde im Rahmen der Prozess-Modellierung und in den Kommentierungen des Grundschutzprofils aber nicht näher berücksichtigt.

12 Risikobetrachtung/Risikobehandlung

Die Basis- und Standard-Anforderungen der IT-Grundschutz-Bausteine wurden so festgelegt, dass dazu passende Maßnahmen für normalen Schutzbedarf und für typische Informationsverbünde und Anwendungsszenarien einen angemessenen und ausreichenden Schutz bieten. Hierfür wurde vorab geprüft, welchen Gefährdungen die in den Bausteinen behandelten Sachverhalte üblicherweise ausgesetzt sind und wie den daraus resultierenden Risiken zweckmäßig begegnet werden kann. Anwenderinnen und Anwender des IT-Grundschutz-Profils benötigen daher in der Regel für den weitaus größten Teil des gewählten Informationsverbundes keine aufwendigen Untersuchungen mehr zur Festlegung erforderlicher Sicherheitsmaßnahmen.
Ein zusätzlicher Analysebedarf besteht lediglich in folgenden vier Fällen:

- Ein Zielobjekt hat einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.
- Es gibt für ein Zielobjekt keinen hinreichend passenden Baustein im IT-Grundschutz-Kompendium.
- Es gibt zwar einen geeigneten Baustein, die Einsatzumgebung des Zielobjekts ist allerdings für den IT-Grundschutz untypisch.
- Anforderungen können organisatorisch nicht im Wortlaut des Kompendiums umgesetzt werden (wie das Vier-Augen-Prinzip bei einer kleinen Hochschule).

Hinweise zur Durchführung einer Risikoanalyse sind in Kapitel 14 zu finden.

13 Schutzbedarf

13.1 Informationen zu den Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich der IT-Grundschutz auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit (CIA: confidentiality, integrity, availability) unterteilt wird:

Schutzbedarfskategorien	Beschreibung
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Dabei beschreiben die nachfolgenden Tabellen für die einzelnen Schutzbedarfskategorien mögliche Folgen, die bei einer Einordnung in die Schutzbedarfskategorien „normal“, „hoch“ oder „sehr hoch“ auftreten können, und geben eine Hilfestellung bei der Einordnung. Gegebenenfalls sind die Tabellen dem eigenen Umfeld anzupassen und zu erweitern.

Im Rahmen einer Feststellung des Schutzbedarfs sollte eine Datenklassifikation durchgeführt werden. Diese liefert Vorgaben vor allem unter dem Gesichtspunkt der Vertraulichkeit, teilweise auch der Integrität. Gemäß der folgenden, gegebenenfalls angepassten Tabellen lassen sich hier wiederum Anhaltspunkte für die Einordnung in die Schutzbedarfskategorien finden. So sind vertrauliche Daten wohl üblicherweise einer hohen Schutzbedarfskategorie bezüglich der Vertraulichkeit und vielleicht Integrität zuzuordnen, aber eventuell nur einem normalen Schutzbedarf bezüglich der Verfügbarkeit. Erst aus dieser Einordnung lassen sich die Anforderungen an Anwendungen, IT-Systeme und Infrastruktur ableiten.

Schutzbedarfskategorie „normal“	Erläuterung
1. Verstoß gegen Gesetze/Vorschriften/ Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • geringfügige Vertragsverletzungen mit höchstens geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungs rechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigt werden können.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden..
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten..
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Tabelle 1: Schutzbedarfskategorie „normal“

Schutzbedarfskategorie „hoch“	Erläuterung
1. Verstoß gegen Gesetze/Vorschriften/ Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden können.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen 4 und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist aber nicht existenzbedrohend.

Tabelle 2: Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie „sehr hoch“	Erläuterung
1. Verstoß gegen Gesetze/Vorschriften/ Verträge	• fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungs rechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit der Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als vier Stunden..
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabelle 3: Schutzbedarfskategorie „sehr hoch“

13.2 Vorgehen zur Schutzbedarfsfeststellung

Bei den hier betrachteten Geschäftsprozessen geht dieses IT-Grundschutz-Profil für die meisten Prozesse von einem Schutzbedarf der Kategorie „normal“ aus. Das erleichtert u. a. auch den Einstieg in den Informationssicherheitsprozess. In diesen Fällen wird zunächst, aber auch als absolutes Minimum, die Umsetzung der Anforderungen der Basis-Absicherung vorgeschlagen, erst in zweiter Linie die Umsetzung der Anforderungen zur Standard-Absicherung.

Für manche Zielobjekte wird in diesem IT-Grundschutz-Profil der Schutzbedarf „hoch“ definiert. Hier reichen die Maßnahmen der Basis- und Standard-Absicherung unter Umständen nicht mehr aus. In diesen Fällen muss eine individuelle Risikoanalyse erfolgen, auf deren Basis dann Maßnahmen festgelegt werden müssen. Hinweise zur Durchführung einer Risikoanalyse finden sich in Kapitel 14.

In einzelnen Fällen könnte nach einer Risikobetrachtung gegebenenfalls festgestellt werden, dass Maßnahmen gemäß Standard-Absicherung ausreichend sind, in anderen Fällen werden Maßnahmen für den erhöhten Schutzbedarf umzusetzen sein. Beispiele und Umsetzungshinweise für Maßnahmen einzelner Bausteine bei einem erhöhten Schutzbedarf befinden sich bei den Bausteinbeschreibungen des BSI. Zusätzliche hochschulspezifische Umsetzungshinweise befinden sich in den Baustein-Kommentierungen sowie auf der Austauschplattform des ZKI-Arbeitskreises Informationssicherheit unter https://it-grundschutz.zki.de. Ein Beispiel für die Betrachtung eines Teilprozesses mit hohem Schutzbedarf findet sich in Kapitel 13.3.

Jede Hochschule sollte eine individuelle Schutzbedarfsfeststellung nach der IT-Grundschutz-Methode für alle Zielobjekte durchführen und je nach Einordnung entsprechende Maßnahmen definieren.

Die nachfolgende Tabelle fasst das Vorgehen nochmals in einer Übersicht zusammen.
Die in Klammern angegebenen Referenzen beziehen sich auf das Dokument BSI-Standard 200-2 IT-Grundschutz-Methodik.

<table>
<tr><th colspan="2">Die Schadensauswirkungen sind begrenzt und überschaubar.</th><th>Die Schadensauswirkungen können beträchtlich sein.</th><th>Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.</th></tr>
<tr><td colspan="2">Schutzbedarf normal</td><td>Schutzbedarf hoch</td><td>Schutzbedarf sehr hoch</td></tr>
<tr><td colspan="2">Sicherheitsanforderungen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen. (8.2.9)</td><td rowspan="2">Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen sollten auf Basis einer Risikoanalyse ermittelt werden. (8.2.9)</td><td rowspan="2">Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer Risikoanalyse ermittelt werden. (8.2.9)</td></tr>
<tr><td colspan="2">In der Vorgehensweise nach IT-Grundschutz wird bei der Erstellung der IT- Grundschutz-Bausteine implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. Hierbei werden nur solche Gefährdungen betrachtet. die nach sorgfältiger Analyse eine so hohe Eintrittswahrscheinlichkeit oder so einschneidende Auswirkungen haben, dass Sicherheitsmaßnahmen ergriffen werden Dieser Ansatz hat den Vorteil, dass Anwender des IT-Grundschutzes für einen Großteil des Informationsverbundes keine individuelle Bedrohungs- und Schwachstellenanalyse durchführen müssen, weil diese Bewertung vorab bereits vorgenommen wurde. (8.5)</td></tr>
<tr><td colspan="2">implizite Risiko-Bewertung</td><td colspan="2" rowspan="2">explizite Risiko-Bewertung
Anforderungen bei erhöhtem Schutzbedarf sind eine Auswahl von Vorschlägen für eine weiterführende Absicherung, die bei erhöhten Sicherheitsanforderungen oder unter bestimmten Rahmenbedingungen als Grundlage für die Erarbeitung geeigneter Anforderungen und Maßnahmen berücksichtigt werden können. (8.3.1)</td></tr>
<tr><td>Bei der Umsetzung der Vorgehensweise „Basis-Absicherung“ wird ein Sicherheitsniveau erreicht, das zwar deutlich unter dem der Standard-Absicherung liegt, aber eine gute Grundlage für ISMS-Einsteiger bietet. (1.2)
Basis-Anforderungen müssen vorrangig erfüllt werden, da bei diesen Empfehlungen mit (relativ) geringem Aufwand der größtmögliche Nutzen erzielt werden kann. Es handelt sich um uneingeschränkte Anforderungen. Die Basis-Anforderungen sind ebenfalls die Grundlage für die Vorgehensweise „Basis-Absicherung“. (8.3.1)</td><td>Durch die Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird mit der Vorgehensweise „Standard-Absicherung“ ein Sicherheitsniveau für die betrachteten Geschäftsprozesse erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. (1.2)
Standard-Anforderungen bauen auf den Basis-Anforderungen auf und adressieren den normalen Schutzbedarf. Sie sollten grundsätzlich erfüllt werden, aber nicht vorrangig. Die Ziele der Standard-Anforderungen müssen erreicht werden, um eine Standard-Absicherung zu erzielen. Es können sich aber durch die jeweiligen Rahmenbedingungen der Institution auch Gründe ergeben, warum eine Standard-Anforderung nicht wie beschrieben umgesetzt wird, sondern die Sicherheitsziele auf andere Weise erreicht werden. Wenn eine Standard-Anforderung durch andere Sicherheitsmaßnahmen erfüllt wird, müssen die dadurch entstehenden Auswirkungen sorgfältig abgewogen und geeignet dokumentiert werden. (8.3.1)</td></tr>
<tr><td colspan="2">Die im IT-Grundschutz-Kompendium aufgeführten Basis- und Standard-Anforderungen stellen zusammengenommen den Stand der Technik dar. Diese müssen für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz erfüllt werden. (2.7)</td><td colspan="2"></td></tr>
<tr><td>Anforderungen Basis</td><td>Anforderungen Standard</td><td colspan="2">Anforderungen Erhöht</td></tr>
<tr><td>Maßnahmen müssen umgesetzt werden</td><td>Maßnahmen sollten umgesetzt werden</td><td colspan="2">Maßnahmen sollten umgesetzt werden</td></tr>
</table>

13.3 Untersuchung eines Bausteins mit Anforderung „hoher Schutzbedarf“

Die Bausteine enthalten auch Empfehlungen zur Anwendung und Umsetzung im Hochschulkontext. Hierbei sind die Vorgaben der Bausteine entsprechend zu interpretieren, um die Vorgaben auf die Hochschullandschaft so zu übertragen, dass ein adäquates Sicherheitsniveau erreicht werden kann. So ist oft von Mitarbeitenden die Rede, dieser Begriff ist gegebenenfalls auf andere betroffene Mitglieder einer Hochschule zu übertragen.

Beispiel: Baustein ORP.3 Sensibilisierung und Schulung zur Informationssicherheit:

> **„ORP.3.A9 Spezielle Schulung von exponierten Personen und Institutionen (H)**
> Besonders exponierte Personen SOLLTEN vertiefende Schulungen in Hinblick auf mögliche Gefährdungen sowie geeignete Verhaltensweisen und Vorsichtsmaßnahmen erhalten.“

Die Empfehlung der Autorinnen und Autoren zum hohen Schutzbedarf ist hier: Die Anforderung ORP.3.A9 ist bei hohem Schutzbedarf ebenfalls anzuwenden. Dabei ist der Begriff Mitarbeitende auch auf Studierende auszudehnen, die im Rahmen ihres Studiums, z. B. bei Abschlussarbeiten, in solchen Institutionen oder Organisationsbereichen tätig sind.

14 Hinweise zur Durchführung einer Risikoanalyse

Das grundlegende Verfahren zur Untersuchung von Sicherheitsgefährdungen und deren Auswirkungen ist eine Risikoanalyse. Der BSI-Standard 200-3: Risikomanagement bietet hierfür eine effiziente Methodik. Für das konkrete Vorgehen und eine detaillierte Beschreibung wird an dieser Stelle daher auf den BSI-Standard 200-3 verwiesen. Im Folgenden eine kurze Auflistung der durchzuführenden Schritte einer Risikoanalyse:

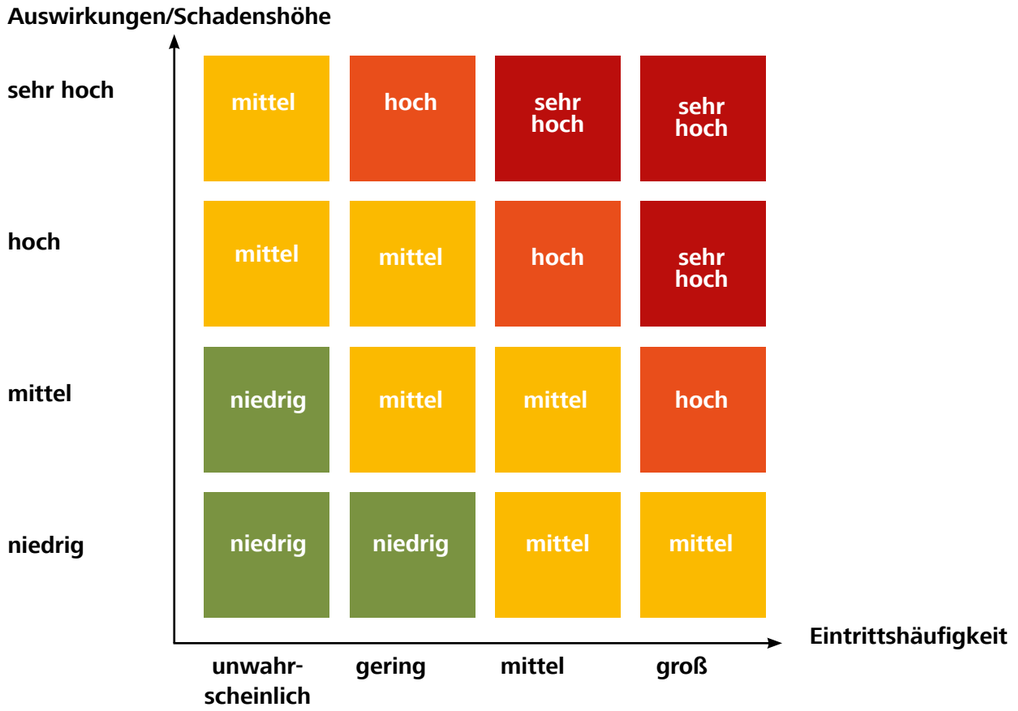
1. **Zielobjekte zusammenstellen**
   Voraussetzung für die Durchführung von Risikoanalysen im Rahmen der Standard-Absicherung ist, dass bei der Strukturanalyse die Zielobjekte des Informationsverbundes zusammengestellt sind, deren Schutzbedarf festgestellt ist, und ihnen bei der Modellierung soweit möglich passende IT-Grundschutz-Bausteine zugeordnet wurden. Eine Risikoanalyse ist für solche Zielobjekte durchzuführen, die einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder für die es keinen passenden IT-Grundschutz-Baustein gibt oder die in Einsatzszenarien betrieben werden, die für den IT-Grundschutz untypisch sind.

2. **Gefährdungsübersicht anlegen**
   Der erste Schritt einer Risikoanalyse ist es, die Risiken zu identifizieren, denen ein Objekt oder ein Sachverhalt ausgesetzt ist. Hierfür ist zunächst zu beschreiben, welchen Gefährdungen das Objekt oder der Sachverhalt unterliegt. Hierzu hat das BSI eine Liste von elementaren Gefährdungen erstellt.

3. **Gefährdungsübersicht ergänzen**
   Auch wenn die Zusammenstellung elementarer Gefährdungen vielfältige Bedrohungen berücksichtigt, denen Informationen und Informationstechnik ausgesetzt sind, so kann dennoch nicht ausgeschlossen werden, dass weitere Gefährdungen zu betrachten sind. Dies gilt insbesondere dann, wenn es für ein Zielobjekt keinen geeigneten Baustein gibt oder es in untypischen Einsatzszenarien betrieben wird. Im Anschluss an den ersten Teilschritt ist daher zu prüfen, ob neben den relevanten elementaren Gefährdungen weitere Gefährdungen zu untersuchen sind.

4. **Häufigkeit und Auswirkungen einschätzen**
   Die Höhe eines Risikos ergibt sich aus der Häufigkeit einer Gefährdung und der drohenden Schadenshöhe. Ein Risiko ist umso größer, je häufiger eine Gefährdung ist, umgekehrt sinkt es, je geringer der mögliche Schaden ist. Grundsätzlich können beide Größen sowohl quantitativ, also mit genauen Zahlenwerten, als auch qualitativ, also mithilfe von Kategorien zur Beschreibung der Größenordnung, bestimmt werden.

5. **Risiken bewerten**
   Nachdem die Eintrittshäufigkeiten und Schadensauswirkungen einer Gefährdung eingeschätzt wurden, lässt sich das aus beiden Faktoren resultierende Risiko bewerten. Es ist auch hierfür zweckmäßig, eine nicht zu große Anzahl an Kategorien zu verwenden – drei bis fünf sind üblich, oft werden auch nur zwei Kategorien verwendet. Der BSI- Standard 200-3 enthält ein Beispiel mit vier Stufen, das sich an die Gegebenheiten und Erfordernisse einer Institution anpassen lässt.



6. **Risiken behandeln**
   In der Regel wird die Gefährdungsbewertung aufzeigen, dass nicht alle Gefährdungen durch das vorhandene Sicherheitskonzept ausreichend abgedeckt sind. In diesem Fall gilt es zu überlegen, wie angemessen mit den verbleibenden Gefährdungen umgegangen werden kann, und eine begründete Entscheidung zu treffen. Risikoakzeptanz, Risikominimierung, Risikotransfer und Risikovermeidung sind die entsprechenden Behandlungsmethoden. Risikoakzeptanz ist jedoch bei Basis-Anforderungen nicht möglich. Das in Kapitel 12 angesprochene „Vier-Augen-Prinzip“ fällt nach „ORP.1.A4 Funktionstrennung zwischen unvereinbaren Aufgaben (B)“ darunter.

7. **Sicherheitskonzeption konsolidieren**
   Als Abschluss der Risikoanalyse sind die zusätzlichen Maßnahmen, deren Umsetzung beschlossen wurde, in das vorhandene Sicherheitskonzept zu integrieren (= Konsolidierung des Sicherheitskonzepts) und darauf aufbauend der Sicherheitsprozess fortzusetzen

15 Prozesslandkarten

Im Folgenden sind die Landkarten zu den hier behandelten Geschäftsprozessen zusammengestellt. Zu den einzelnen Prozessen sind Anwendungen mit dem entsprechenden Schutzbedarf angegeben sowie Systeme, Räume und Gebäude. Die einzelnen Bausteine zu den jeweiligen Komponenten sind angegeben, wobei Bausteine, die gegebenenfalls Maßnahmen für einen erhöhten Schutzbedarf berücksichtigen müssen, im jeweiligen Kontext mit einem „!“ markiert sind. Zu den einzelnen Landkarten ist jeweils dargestellt, aufgrund welcher Voraussetzungen in den Bereichen Vertraulichkeit, Integrität, Verfügbarkeit (CIA) ein erhöhter Schutzbedarf angenommen wurde.

In diesen Fällen muss eine Risikoabschätzung erfolgen. Auf dieser Basis wird festgelegt, ob und wenn ja welche der in den Bausteinen beschriebenen Maßnahmen für erhöhten Schutzbedarf im Einzelfall beim betroffenen Baustein anzuwenden sind bzw. ob weitere, eigene Maßnahmen zu treffen sind.

15.1 Landkarten Übergreifende Anwendungen

Hier werden übergreifend verwendete Anwendungen, die Basisinfrastruktur und Basisdienste eines Hochschulrechenzentrums im Rahmen der genannten und nachfolgend betrachteten Prozesse zusammengestellt. Neben den genannten Basisanwendungen an sich ist die Betrachtung der einzelnen Bausteine auch für die Durchführung der in den Kapiteln 15.2. bis 15.5. genannten einzelnen Geschäftsprozesse erforderlich. Sie werden dort nicht mehr wiederholt, es sei denn, sie sind unter Umständen aufgrund spezieller Anforderungen nochmals separat zu betrachten, z. B. wenn durch den jeweiligen Geschäftsprozess ein erhöhter Schutzbedarf gefordert ist oder wenn davon auszugehen ist, dass die Bewertung der einzelnen Anforderungen der jeweiligen Bausteine im betrachteten Geschäftsprozess gegenüber der Bewertung in den Übergreifenden Anwendungen abweicht.

Aus Gründen der Übersichtlichkeit sind die Prozesse der Übergreifenden Anwendungen auf zwei entsprechenden Landkarten zusammengefasst. Die erste zeigt die Basisdienste sowie die dazugehörige Infrastruktur, auf der zweiten Landkarte ist vor allem der interne und externe Clientzugriff auf die Übergreifenden Anwendungen, aber auch auf Anwendungen der später gezeigten Geschäftsprozesse dargestellt. Der Schutzbedarf für diese Übergreifenden Anwendungen ergibt sich teilweise aus dem Schutzbedarf der im Rahmen der in den Kapiteln 15.2. bis 15.5. dargestellten übrigen Geschäftsprozesse bzw. Unterprozesse.

Die Bausteine SYS.3.2.2 (Mobile Device Management) und INF.7 sind laut IT-Grundschutz-Kompendium 2022 des BSI eigentlich dem Bereich Informationsverbund/übergeordnete Aspekte (Landkarte Kapitel 11) zuzuordnen, obwohl die Namensgebung eigentlich auf Systembausteine schließen lässt. Nachdem die beiden hier dargestellten Landkarten Übergreifende Anwendungen jedoch ebenfalls übergeordnet zu begreifen sind und die Basis für die weiteren Geschäftsprozesse darstellen, wurden die genannten Bausteine aus Gründen der Übersichtlichkeit zusammen mit anderen IT-System- und Raumbausteinen hier modelliert.

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Übergreifende Anwendungen (Basisdienste)	Identity Management/ Authentication Groupware / E-Mail / Chat Fileservice / Sync & Share Orchestrierung Container Webauftritt Virtuelle Serverdienste Print Services Netzwerkinfrastruktur-Dienste/WLAN Telefonie	Identity Management ! **APP. 2.1** **APP. 4.3**	VMWare Virtualisierung ! Virtual Appliance **SYS. 1.1** **SYS. 1.5**	Allgemeines Gebäude **INF.1**
		Active Directory ! (Verzeichnisdienst) **APP. 2.1** **APP. 2.2**	Windows Server 2012 ! **SYS. 1.1** **SYS. 1.2.2**	Rechenzentrum sowie Serverraum ! **INF.2**
		OpenLDAP ! (Verzeichnisdienst) **APP. 2.1** **APP. 2.3**	Linux Server ! **SYS. 1.1** **SYS. 1.3**	Raum sowie Schrank für technische Infrastruktur ! **INF.5**
		Shibboleth (DFN-AAI) !, OpenID-Connect Kerberos, Radius (Authentication) **APP. 2.1**	Containerisierung ! **SYS. 1.6**	Verkabelung **INF.12**
			Speichersystem **SYS. 1.1** **SYS. 1.8**	Technisches Gebäudemanagement **INF.13**
		DNS **APP. 3.6**	Drucker, Kopierer, Multifunktionsgeräte **SYS. 4.1**	
		Kubernetes ! **APP. 4.4**	Firewall **SYS. 1.1** **NET. 3.2**	
		MS Exchange (E-Mail) **APP. 5.2** **APP. 5.3**	Netze ! • LAN • Switches und Router **NET. 1.1** **NET. 1.2** **NET. 3.1**	
		Chat / Messenger		
		Webserver (Webauftritt) **APP. 3.2** **APP. 4.3**	WLAN **NET. 2.1** **NET. 2.2**	
		CMS (Webauftritt) **APP. 3.1** **APP. 3.2** **APP. 4.3**	TK-Anlage, VoIP **NET. 4.1** **NET. 4.2**	
		Fileservice / Sync & Share **APP. 3.1**		
		CUPS (Print Services)		

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Übergreifende Anwendungen (Clientdienste)	Mobiler Zugriff Remotearbeit (VPN, eduroam, WLAN) Statische Arbeitsumgebung Arbeitsplatzbereitstellung Mobile Device Management IT Servicemanagement	IPSec VPN (Checkpoint Mobile Access, Cisco Any-Connect, OpenSwan / StrongSwan,…)	Desktop/Notebook ! **SYS. 2.1** **SYS. 3.1**	Allgemeines Gebäude **INF.1**
		SSL-VPN (OpenVPN, EduVPN)	Windows 10 Client **SYS. 2.1** **SYS. 2.2.3**	Rechenzentrum sowie Serverraum ! **INF.2**
		eduroam (RadsecProxy, SecureW2,…)	MacOS Client **SYS. 2.1** **SYS. 2.4**	Raum sowie Schrank für technische Infrastruktur ! **INF.5**
		Virtueller Remote Desktop, (Citrix (GU), Horizon View, XEN-App,…)	Linux Client **SYS. 2.1** **SYS. 2.3**	Büroarbeitsplatz **INF.7**
		Client mit Office, Browser, E-Mail ! **APP. 1.1** **APP. 1.2**	Wechseldatenträger **SYS. 4.5**	Häuslicher Arbeitsplatz **INF.8**
		Endpoint Security **APP. 3.1** **APP. 3.2** **APP. 4.3**	Tablet und Smartphone **SYS. 3.2.1** **SYS. 3.2.3** **SYS. 3.2.4** **SYS. 3.3**	Mobiler Arbeitsplatz **INF.9**
		Arbeitsplatz bereitstellen (SCCM, Zenworks, Jamf,…) **APP. 1.4**	Mobile Device Management **SYS. 3.2.2**	Besprechungs-, Veranstaltungs- und Schulungsräume **INF.10**
		Ticketsystem: (OTRS, Jira,…) **APP. 3.1** **APP. 3.2** **APP. 4.3**	VPN Gateway **SYS. 1.1**	Verkabelung **INF.12**
			VPN **NET. 3.3**	Technisches Gebäudemanagement **INF.13**

Hintergrund für die Einschätzung des erhöhten Schutzbedarfs (gekennzeichnet durch „!“ in der obigen Darstellung), hier für:

- **Vertraulichkeit, Integrität und Verfügbarkeit für die Netzwerkinfrastruktur, Virtualisierungsumgebung und das Identity Management**
  Die genannten Anwendungen bzw. Systeme werden als Basisinfrastruktur und zentraler Bestandteil für die in den folgenden Kapiteln genannten Prozesse verwendet, für die wiederum hoher Schutzbedarf definiert ist. Daher gilt hier das Maximumprinzip. Für Netzbereiche und abgesetzte Virtualisierungscluster für andere Prozesse, in denen geringere Anforderungen an den Schutzbedarf gelten, können die Anforderungen angepasst werden.

15.2 Landkarte Geschäftsprozess Bewerbung und Zulassung

„Bewerbung“ umfasst die Einrichtung von Bewerbungsverfahren für grundständige und Masterstudiengänge (inklusive verschiedener Studierendengruppen – auch z. B. Hochschulwechsler, Gasthörer, Zweithörer –, Bewerbungszeiträume, Kapazitäten, Bewerbungsvoraussetzungen und rechtlicher Rahmenbedingungen), die Entgegennahme von Bewerbungen in den verschiedenen Ausprägungen sowie deren Überprüfung und gegebenenfalls Bewertung (z. B. zur Notenverbesserung durch außerschulische Leistungen).

„Zulassung“ beinhaltet in zulassungsbeschränkten und freien Studiengängen die Zulassung (bzw. Ablehnung) von Bewerberinnen und Bewerbern, gegebenenfalls auch nur für bestimmte Bewerbergruppen, zu Studiengängen in den verschiedenen Varianten (z. B. durch Ranking, Auswahlgespräche etc.) sowie Annahmeverfahren (der Bewerberinnen und Bewerber).

Der Geschäftsprozess Bewerbung und Zulassung umfasst die folgenden Unterprozesse mit Angabe der Bausteine:

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Bewerbung und Zulassung	Bewerbungsverfahren einrichten Bewerbung entgegennehmen Nicht-EU Bewerbungen prüfen Bewerbungen prüfen Bewerbungen bewerten Vorprüfung durchführen Zulassungsverfahren durchführen Zulassungsangebot annehmen/nicht annehmen Bescheide erstellen/bereitstellen nachgelagerte Zulassung durchführen Bewerberdaten löschen	HISinOne APP ! (Alternativ: SAP SLcM Campusnet CampusOnline Primuss FactScience) **APP. 3.1** **APP. 3.2** **APP. 4.2** **APP. 4.3**	Windows Server 2012 ! **SYS. 1.1** **SYS. 1.2.2**	Allgemeines Gebäude **INF.1**
		DOSV-Portal (extern)	Linux Server ! **SYS. 1.1** **SYS. 1.3**	
		Uni-Assist (extern)		

Hintergrund für die Einschätzung des erhöhten Schutzbedarfs (gekennzeichnet durch „!“ in der obigen Darstellung), hier für:

- **Datenintegrität (n,h,n)**
  Veränderungen/Manipulationen an den Bewerberdaten führen unter Umständen zu falschen Bewerbungen, die vor allem bei zulassungsbeschränkten Verfahren problematisch sind.

Die ebenfalls notwendigen clientseitigen Zugriffe auf das Campus Management System, das Identity Management System und externe Systeme werden beim Prozess Übergreifende Anwendungen (Kapitel 15.1) berücksichtigt. Dasselbe gilt, wenn Server als virtuelle Maschinen oder in sog. Containern laufen. Die Maßnahmen gemäß der genannten Serverbausteine sowie Bausteine INF.1 (Allgemeines Gebäude) sind hier nochmals separat genannt, sie könnten unter Umständen von der Bewertung innerhalb der Übergreifenden Anwendungen (Basisdienste) abweichen.

In obiger Liste der Unterprozesse wird beispielhaft auf die Anwendung HISinOne APP verwiesen. An den Hochschulen sind für diese Prozesse unter Umständen andere Anwendungen im Einsatz, beispielsweise

- HIS ZUL-GX/QIS
- SAP SLcM
- Campusnet (Datenlotsen)
- CAMPUSonline
- PRIMUSS
- FactScience (im Bereich medizinischer Studiengänge im Einsatz)

Für diese Anwendungen gelten die Einschätzungen für den Schutzbedarf sowie die darunterliegenden IT-Systeme entsprechend.

15.3 Landkarte Geschäftsprozess Immatrikulation und Studierendenmanagement

„Immatrikulation“ umfasst die Einschreibung zugelassener Bewerberinnen und Bewerber (die den Studienplatz angenommen haben) und der Bewerberinnen und Bewerber für zulassungsfreie Studiengänge. Sie beinhaltet außerdem die Erzeugung und Bereitstellung bzw. den Versand der zugehörigen Bescheide.
„Studierendenmanagement“ umfasst die Verwaltung aller an der Hochschule eingeschriebenen Personen (z. B. Haupt-, Neben-, Gasthörer, Früh- und Seniorenstudierende). Dies umfasst Änderungen von Stammdaten, Studiengang- und Fachwechsel, Vertiefungswahlen, Rückmeldungen, Beurlaubungen, Praxis- und Auslandssemester, Führen von Studienkonten und Ausbildungspartnerdaten bei dualen Studienprogrammen sowie Exmatrikulationen. Bei dieser Betrachtung ausgeklammert wurde der Bereich „Beiträge und Gebühren“.

Der Geschäftsprozess Immatrikulation und Studierendenmanagement umfasst die folgenden Unterprozesse:

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Immatrikulation und Studierenden-management	Immatrikulation bearbeiten Immatrikulation durchführen Studierendendaten verwalten Studierendenstatus verwalten Studiengang- und Fachwechsel durchführen	HISinOne STU ! (Alternativ: SAP SLcM Campusnet CampusOnline Primuss FactScience) **APP. 3.1** **APP. 3.2** **APP. 4.2** **APP. 4.3**	Windows Server 2012 ! **SYS. 1.1** **SYS. 1.2.2**	Allgemeines Gebäude **INF.1**
		Dakota (SMV) !	Linux Server ! **SYS. 1.1** **SYS. 1.3**	Raum sowie Schrank für technische Infrastruktur ! **INF.5**
			Windows 10 Client ! (Plattform für Dakota) **SYS. 2.1** **SYS. 2.2.3**	Verkabelung **INF.12**

Hintergrund für die Einschätzung des erhöhten Schutzbedarfs (gekennzeichnet durch „!“ in der obigen Darstellung), hier für:

- **Vertraulichkeit (h,n,n) für alle Unterprozesse**
  An einigen Hochschulen werden Gesundheitsdaten mitverarbeitet. Wo dies nicht der Fall ist, kann in der Regel der Schutzbedarf n,n,n zugrunde gelegt werden.

Die ebenfalls notwendigen clientseitigen Zugriffe auf das Campus Management System, das Identity Management System und externe Systeme werden beim Prozess Übergreifende Anwendungen (Kapitel 15.1) berücksichtigt. Dasselbe gilt, wenn Server als virtuelle Maschinen oder in sog. Containern laufen. Die Maßnahmen gemäß der genannten IT-Systembausteine SYS.2.1 bzw. SYS.2.2.3 und Gebäude/Raum-Bausteine INF.5 sowie INF.12 sind hier nochmals separat genannt, sie könnten unter Umständen von der Bewertung innerhalb der Übergreifenden Anwendungen abweichen. Grund hierfür ist die Anwendung Dakota, die auf einem Windows Client als Serverplattform basiert. Hier ist sowohl wegen des ggf. erhöhten Schutzbedarfs wie auch der Verwendung des Client-Betriebssystems als Plattform für die Anwendung eine Risikoanalyse mit einer individuellen Bewertung der einzelnen Maßnahmen innerhalb der genannten Bausteine durchzuführen, ggf. sind zusätzliche Maßnahmen zu definieren. Aufgrund der speziellen Situation sind neben INF.1 auch die Bausteine INF.5 sowie INF.12 hier nochmals aufgeführt, die Bewertung der einzelnen Maßnahmen könnte von denen im Prozess Übergreifende Anwendungen abweichen. In obiger Liste der Unterprozesse wird beispielhaft auf die Anwendung HISinOne STU verwiesen. An den Hochschulen sind für diese Prozesse unter Umständen andere Anwendungen im Einsatz, beispielsweise:

- HIS SOS-GX/QIS
- SAP SLcM
- Campusnet (Datenlotsen)
- CAMPUSonline
- PRIMUSS
- FactScience (im Bereich medizinischer Studiengänge im Einsatz)

Für diese Anwendungen gelten die Einschätzungen für den Schutzbedarf sowie die darunterliegenden IT-Systeme entsprechend.

15.4 Landkarte Geschäftsprozess Prüfungen

Der Hauptprozess „Prüfungen“ umfasst, aufbauend auf den Prüfungsordnungen, die Klärung der Zulassungsvoraussetzungen, die Prüfungsplanung pro Semester bzw. Prüfungsphase und deren Veröffentlichung. In diesem Zusammenhang wird der Begriff Prüfung für alle verschiedenen Prüfungsformen verwendet wie z. B. mündliche Prüfungen, Präsentationen, Hausarbeiten, Klausuren und Abschlussprüfungen (Bachelor-/Master-/Diplomarbeit). Der Hauptprozess beinhaltet außerdem die Anmeldung, Zulassung, ggf. Abmeldung von Studierenden zu Prüfungen sowie die Prüfungsdurchführung. Darüber hinaus schließt er die Ermittlung, Dokumentation, Bescheinigung und Veröffentlichung der Prüfungsergebnisse ein.

Ebenfalls berücksichtigt ist die Durchführung elektronischer Prüfungen, wobei in diesem Prozess die Serverseite und die Prüfungssysteme (inklusive E-Learning-Systeme, die zur Durchführung von Online-Prüfungen geeignet sind) erfasst sind.

Die Client-Seite zum Zugriff auf die E-Prüfungen ist im Prozess „Infrastruktur für Studierende“ in Kapitel 15.5 separat berücksichtigt.

Der Prozess Prüfungen umfasst die folgenden Unterprozesse:

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Prüfungen	Planen Durchführen Bewerten Prüfungsergebnisse bereitstellen / veröffentlichen Archivieren / Auskunft erteilen	HISinOne EXA ! (Alternativ: SAP SLcM Campusnet CampusOnline Primuss FactScience) **APP. 3.1** **APP. 3.2** **APP. 4.3**	Windows Server 2012 ! **SYS. 1.1** **SYS. 1.2.2**	Allgemeines Gebäude **INF.1**
		E-Prüfungs-System ! • LPLUS • EvaExam **APP. 3.1** **APP. 3.2** **APP. 4.3**	Linux Server ! **SYS. 1.1** **SYS. 1.3**	Archiv **INF.6**
		Papierarchiv	Windows 10 Client ! (Plattform für Dakota) **SYS. 2.1** **SYS. 2.2.3**	Büroarbeitsplatz ! **INF.7**
			Drucker, Kopierer, Multifunktionsgeräte ! **SYS. 4.1**	

Hintergrund für die Einschätzung des erhöhten Schutzbedarfs (gekennzeichnet durch „!“ in der obigen Darstellung) hier für:

- **Vertraulichkeit, Integrität, Verfügbarkeit (h,h,h) für die Unterprozesse „Anwesenheitskontrolle“ und „Prüfung durchführen“**
- **Vertraulichkeit und Integrität (h,h,n) für alle übrigen Unterprozesse**

Die Feststellung und Bewertung des Wissensniveaus am Ende von Lehrveranstaltungen ist eine der Kernaufgaben in der Lehre. Es werden die individuellen Leistungen geprüft, die Bearbeitungs- und Prüfungsergebnisse dürfen in der Regel anderen Prüflingen nicht bekannt werden. Diese Ergebnisse führen zu Dokumenten (Zeugnissen), deren Integrität unabdingbar gegeben sein muss, sie dürfen daher während der Prüfung durch Dritte und ansonsten nachträglich grundsätzlich nicht veränderbar sein.

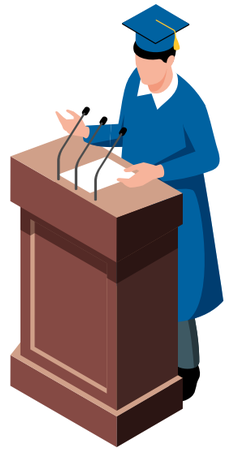
Bei der Durchführung elektronischer Prüfungen muss beginnend mit der Anwesenheitskontrolle zusätzlich eine hohe Verfügbarkeit der IT-Systeme gegeben sein, um Nachteile für einzelne Prüflinge zu vermeiden. Als Alternative kämen sonst in der Regel nur der Abbruch und die Wiederholung der gesamten Prüfung infrage.

Sofern die Server als virtuelle Maschinen oder in Containern laufen, wird dies bei den Übergreifenden Anwendungen betrachtet. Die Client-Seite zur Verwaltung von Prüfungen und deren Ergebnissen sowie die IT-Systeme zum Scannen von Prüfungsantwortbögen sind in den IT-Systembausteinen und mit den Bausteinen für das allgemeine Gebäude sowie den Büroarbeitsplatz INF.7 hier nochmals separat erfasst. Die Bewertung der Maßnahmen könnte von den Bewertungen innerhalb der Übergreifenden Anwendungen abweichen.

In obiger Liste der Unterprozesse wird beispielhaft auf die Anwendung HISinOne EXA verwiesen. An den Hochschulen sind für diese Prozesse unter Umständen andere Anwendungen im Einsatz, beispielsweise:

- HIS POS-GX/QIS
- SAP SLcM
- Campusnet (Datenlotsen)
- CAMPUSonline
- PRIMUSS
- FactScience (im Bereich medizinischer Studiengänge im Einsatz)

Für diese Anwendungen gelten die Einschätzungen für den Schutzbedarf sowie die darunterliegenden IT-Systeme entsprechend.



15.5 Landkarte Geschäftsprozess IT-Infrastruktur für Studierende

Dieser Prozess beinhaltet die Bereitstellung einer Arbeitsumgebung im Rahmen von Studium und Lehre.Diese Arbeitsumgebung umfasst die Bereitstellung von zentralen Diensten mit externem Zugang durch eigene Geräte sowie internem Zugang durch zentral bereitgestellte Systeme sowie die darunterliegende Netzwerkinfrastruktur.

Im Geschäftsprozess „Prüfungen" (siehe Kapitel 15.4) wurde die Durchführung elektronischer Prüfungen für die Serverseite mit definiert. Sofern elektronische Prüfungen durchgeführt werden, gilt damit auch ein erhöhter Schutzbedarf für die Prüfungsdesktops, in der Landkarte gekennzeichnet durch „!".

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Infrastruktur für Studierende	Statische Arbeitsumgebung E-Prüfungen E-Learning	Pool PC (Windows/Linux/MacOS) !	Windows Server 2012 ! **SYS. 1.1** **SYS. 1.2.2**	Allgemeines Gebäude **INF.1**
		Remote Unix Desktop	Linux Server ! **SYS. 1.1** **SYS. 1.3**	Raum sowie Schrank für technische Infrastruktur ! **INF.5**
		Virtueller Remote Desktop, (Citrix, Horizon View, XEN-App) !	Windows 10 Client ! (Plattform für Dakota) **SYS. 2.1** **SYS. 2.2.3**	
		E-Learning-System • Moodle • Ilias • StudIP	MacOS Client ! **SYS. 2.1** **SYS. 2.4**	Büroarbeitsplatz **INF.7**
			Linux Client ! **SYS. 2.1** **SYS. 2.3**	Besprechungs-, Veranstaltungs- und Schulungsräume **INF.10**
			Drucker, Kopierer, Multifunktionsgeräte ! **SYS. 4.1**	
				Verkabelung **INF.12**

Hintergrund für die Einschätzung des erhöhten Schutzbedarfs (gekennzeichnet durch „!" in der obigen Darstellung) hier für:

- **Vertraulichkeit, Integrität und Verfügbarkeit (h,h,h) für den Unterprozess E-Prüfungen**
  Es muss sichergestellt sein, dass Inhalte von Prüfungsantworten nicht bekannt werden und nachträgliche Änderungen nicht möglich sind, damit die Integrität der Prüfungen gewahrt bleibt. Beginnend mit der Anwesenheitskontrolle muss zusätzlich eine hohe Verfügbarkeit der IT-Systeme gegeben sein, um Nachteile für einzelne Prüflinge zu vermeiden. Als Alternative kämen sonst in der Regel nur der Abbruch und die Wiederholung der gesamten Prüfung infrage.

Sofern die Server als virtuelle Maschinen oder in Containern laufen, wird dies bei den Übergreifenden Anwendungen betrachtet. Die Client-Seite zur Durchführung von Prüfungen wird hier in den IT-Systembausteinen (SYS2.1, SYS2.2.3, SYS.2.3, SYS.2.4. und SYS.4.1) und den Bausteinen für Gebäude bzw. Räume (INF.5, INF.7, INF.10, INF.12) separat von den Übergreifenden Anwendungen betrachtet, nachdem hier unter Umständen eigene Schutzmaßnahmen festgelegt werden müssen. Dies gilt insbesondere für den Zugang und die Konfiguration der Arbeitsplätze sowie den Netzwerkzugriff.

16 Baustein-Kommentierungen

Den Autorinnen und Autoren war es ein besonderes Anliegen, den Hochschulen Hilfestellungen zu den Bausteinen mitzugeben. Dazu wurden die verwendeten Bausteine und Umsetzungshinweise (Stand: IT-Grundschutz-Kompendium Edition 2022) aus Hochschulsicht kommentiert. Es handelt sich dabei um ein lebendes Dokument, in das auch zukünftige Erfahrungen der Hochschulen mit einfließen sollen. Daher wird es regelmäßig aktualisiert.
Die aktuelle Version der Baustein-Kommentierungen finden Sie als PDF-Datei hier: zki.de/publikationen bzw. als direkte Links auf die einzelnen Baustein-Kommentierungen in nachfolgender Tabelle.

Baustein	Kommentierung
Sicherheitsmanagement	
ISMS.1 Sicherheitsmanagement	https://zki.de/goto/gp-9XPreg
Organisation und Personal	
ORP.1 Organisation	https://zki.de/goto/gp-53vbSA
ORP.2 Personal	https://zki.de/goto/gp-eeEltw
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	https://zki.de/goto/gp-n8OGlg
ORP.4 Identitäts- und Berechtigungsmanagement	https://zki.de/goto/gp-ghMdYA
ORP.5 Compliance Management (Anforderungsmanagement)	https://zki.de/goto/gp-9tVcUg
Konzepte und Vorgehensweisen	
CON.1 Kryptokonzept	https://zki.de/goto/gp-IZifMg
CON.2 Datenschutz	https://zki.de/goto/gp-NpCKfQ
CON.3 Datensicherungskonzept	https://zki.de/goto/gp-FvyzYQ
CON.6 Löschen und Vernichten	https://zki.de/goto/gp-7W7dOA
CON.7 Informationssicherheit auf Auslandsreisen	https://zki.de/goto/gp-0s4u9g
CON.8 Software-Entwicklung	https://zki.de/goto/gp-hJcafN
CON.9 Informationsaustausch	https://zki.de/goto/gp-I2GDXA
CON.10 Entwicklung von Webanwendungen	https://zki.de/goto/gp-gWaRVC
Betrieb	
OPS.1.1.2 Ordnungsgemäße IT-Administration	https://zki.de/goto/gp-CA4Pbg
OPS.1.1.3 Patch- und Änderungsmanagement	https://zki.de/goto/gp-Eka5JA
OPS.1.1.4 Schutz vor Schadprogrammen	https://zki.de/goto/gp-UiwUmw
OPS.1.1.5 Protokollierung	https://zki.de/goto/gp-fF0JVw
OPS.1.1.6 Software-Tests und -Freigaben	https://zki.de/goto/gp-Ugwm4Q
OPS.1.1.7 Systemmanagement	https://zki.de/goto/gp-n30THD
OPS.1.2.2 Archivierung	https://zki.de/goto/gp-NLxeSQ
OPS.1.2.4 Telearbeit	https://zki.de/goto/gp-xomePw
OPS.1.2.5 Fernwartung	https://zki.de/goto/gp-EqFDcg

Baustein	Kommentierung
OPS.1.2.6 NTP-Zeitsynchronisation	https://zki.de/goto/gp-q7ZrNh
OPS.2.1 Outsourcing für Kunden	https://zki.de/goto/gp-cnbtzg
OPS.2.2 Cloud-Nutzung	https://zki.de/goto/gp-VRty7Q
OPS.3.1 Outsourcing für Dienstleister	https://zki.de/goto/gp-hxKRLQ
Detektion und Reaktion	
DER.1 Detektion von sicherheitsrelevanten Ereignissen	https://zki.de/goto/gp-cMw6hQ
DER.2.1 Behandlung von Sicherheitsvorfällen	https://zki.de/goto/gp-6Qd47w
DER.2.2 Vorsorge für die IT-Forensik	https://zki.de/goto/gp-fDWKBQ
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle	https://zki.de/goto/gp-3lsweQ
DER.3.1 Audits und Revisionen	https://zki.de/goto/gp-aDI2Qg
DER.4 Notfallmanagement	https://zki.de/goto/gp-RmMZ9A
Anwendungen	
APP.1.1 Office-Produkte	https://zki.de/goto/gp-hx786w
APP.1.2 Web-Browser	https://zki.de/goto/gp-KswnfQ
APP.1.4 Mobile Anwendungen (Apps)	https://zki.de/goto/gp-eyqawh
APP.2.1 Allgemeiner Verzeichnisdienst	https://zki.de/goto/gp-hrUEvQ
APP.2.2 Active Directory	https://zki.de/goto/gp-f5GhCg
APP.2.3 OpenLDAP	https://zki.de/goto/gp-5lrjYA
APP.3.1 Webanwendungen und Webservices	https://zki.de/goto/gp-eUFq3w
APP.3.2 Webserver	https://zki.de/goto/gp-Dbur9Q
APP.3.3 Fileserver	https://zki.de/goto/gp-9RANFw
APP.3.6 DNS-Server	https://zki.de/goto/gp-xc6ruw
APP.4.2 SAP-ERP-System	https://zki.de/goto/gp-ubHJgQ
APP.4.3 Relationale Datenbanken	https://zki.de/goto/gp-AEjx7A
APP.4.4 Kubernetes	https://zki.de/goto/gp-rpaVAG
APP.5.2 Microsoft Exchange und Outlook	https://zki.de/goto/gp-Bk0Zxg
APP.5.3 Allgemeiner E-Mail-Client und -Server	https://zki.de/goto/gp-REIm4o
APP.6 Allgemeine Software	https://zki.de/goto/gp-jVb1YB
APP.7 Entwicklung von Individualsoftware	https://zki.de/goto/gp-I1WyYD
IT-Systeme	
SYS.1.1 Allgemeiner Server	https://zki.de/goto/gp-nCIBwA
SYS.1.2.2 Windows Server 2012	https://zki.de/goto/gp-Dnkreg
SYS.bd.1 Windows Server 2016	https://zki.de/goto/gp-QInHTQ
SYS.1.2.3 Windows Server 2019	https://zki.de/goto/gp-NHMGZw
SYS.1.3 Server unter Linux und Unix	https://zki.de/goto/gp-dBmr2A
SYS.1.5 Virtualisierung	https://zki.de/goto/gp-SSAw0w

Baustein	Kommentierung
SYS.1.6 Containerisierung	https://zki.de/goto/gp-1S5yrA
SYS.1.8 Speicherlösungen	https://zki.de/goto/gp-B3nSdw
SYS.2.1 Allgemeiner Client	https://zki.de/goto/gp-kdlHhQ
SYS.2.2.3 Clients unter Windows 10	https://zki.de/goto/gp-uWZLTg
SYS.2.3 Clients unter Linux und Unix	https://zki.de/goto/gp-ddyhjA
SYS.2.4 Clients unter macOS	https://zki.de/goto/gp-ZCCpsQ
SYS.3.1 Laptops	https://zki.de/goto/gp-L0ymIQ
SYS.3.2.1 Allgemeine Smartphones und Tablets	https://zki.de/goto/gp-gheI3g
SYS.3.2.2 Mobile Device Management (MDM)	https://zki.de/goto/gp-rEanaA
SYS.3.2.3 iOS (for Enterprise)	https://zki.de/goto/gp-NhHbqw
SYS.3.2.4 Android	https://zki.de/goto/gp-4VqUpg
SYS.3.3 Mobiltelefon	https://zki.de/goto/gp-epk76A
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	https://zki.de/goto/gp-0gcVAg
SYS.4.5 Wechseldatenträger	https://zki.de/goto/gp-JffVYQ
Netze und Kommunikation	
NET.1.1 Netzarchitektur und -design	https://zki.de/goto/gp-sEzS4g
NET.1.2 Netzmanagement	https://zki.de/goto/gp-dvuV0g
NET.2.1 WLAN-Betrieb	https://zki.de/goto/gp-WKq6ZA
NET.2.2 WLAN-Nutzung	https://zki.de/goto/gp-ZfnKjQ
NET.3.1 Router und Switches	https://zki.de/goto/gp-IWaByw
NET.3.2 Firewall	https://zki.de/goto/gp-sg1NnQ
NET.3.3 VPN	https://zki.de/goto/gp-kCwnwg
NET.4.1 TK-Anlagen	https://zki.de/goto/gp-7kiAfA
NET.4.2 VoIP	https://zki.de/goto/gp-wBmvy
Infrastruktur	
INF.1 Allgemeines Gebäude	https://zki.de/goto/gp-y4N6dg
INF.2 Rechenzentrum sowie Serverraum	https://zki.de/goto/gp-ocqyXg
INF.5 Raum sowie Schrank für technische Infrastruktur	https://zki.de/goto/gp-7PwOhg
INF.6 Datenträgerarchiv	https://zki.de/goto/gp-zRFA2g
INF.7 Büroarbeitsplatz	https://zki.de/goto/gp-ueuB8A
INF.8 Häuslicher Arbeitsplatz	https://zki.de/goto/gp-s20bjQ
INF.9 Mobiler Arbeitsplatz	https://zki.de/goto/gp-nphuVw
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	https://zki.de/goto/gp-6utaFA
INF.12 Verkabelung	https://zki.de/goto/gp-GU0zNt
INF.13 Technisches Gebäudemanagement	https://zki.de/goto/gp-vhF09S

Zentren für
Kommunikation und Informationsverarbeitung
in Lehre und Forschung e.V.

c/o CIO der Freien Universität Berlin
Fabeckstraße 32, 14195 Berlin
Telefon: +49 30 2062262 0
E-Mail: geschaeftsstelle@zki.de
Homepage: http://www.zki.de