Zentren für
Kommunikation und
Informationsverarbeitung e.V.

IT-Grundschutz-Profil für Hochschulen

Version 1.0

08.09.2020

Inhaltsverzeichnis

Versionshistorie

Version	Datum	Beschreibung
0.9	25.11.2019	Veröffentlichung des Rahmendokuments als Community Draft und Vorstellung auf dem Workshop Informationssicherheit der Hochschulrektorenkonferenz.
1.0	08.09.2020	Rahmendokument und Baustein-Kommentierungen auf Grundlage der Edition 2020 des IT-Grundschutz-Kompendiums veröffentlicht.

1 Vorwort

Das vorliegende IT-Grundschutz-Profil für Hochschulen wurde vom Arbeitskreis Informationssicherheit der „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ im Rahmen seiner Mitgliedschaft in der Allianz für Cybersicherheit in 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 fünfzig IT-Sicherheitsbeauftragten, IT-Mitarbeitern und Rechenzentrumsleitern und dem BSI repräsentative Kernprozesse an Hochschulen herausgearbeitet. Anschließend wurden die für diese Prozesse typischen Applikationen, deren Schutzbedarf und die benötigten IT-Systeme und Räumlichkeiten ermittelt. Im letzten Schritt wurden etwa achtzig 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 und 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 deshalb 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 Hochschul-Prozesse. 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 Prozessbausteine (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 der 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.

2 Einleitung

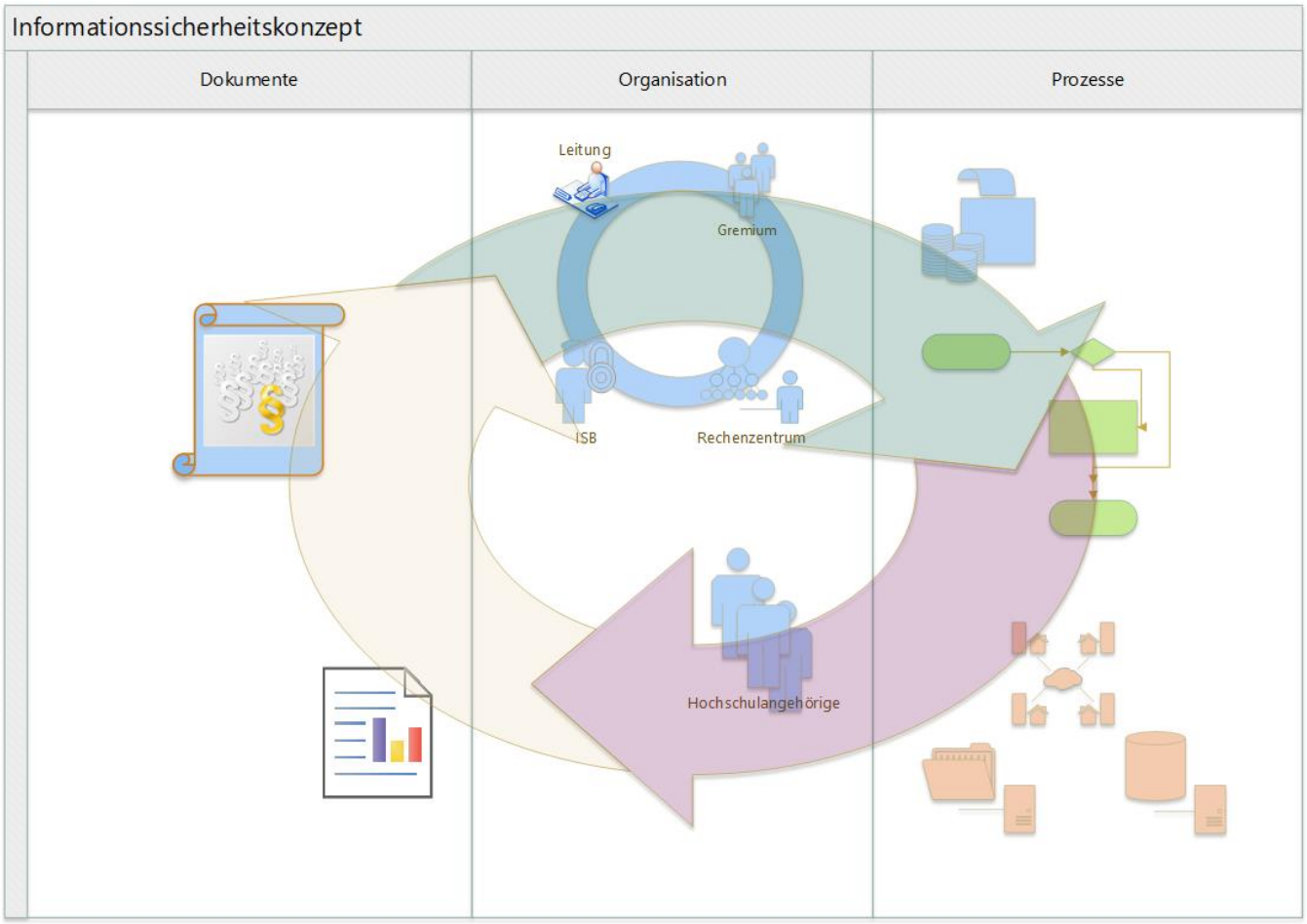
2.1 Umfeld

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. (Zentren für Kommunikationsverarbeitung in Forschung und Lehre) zeigt, in denen 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 Mitarbeitern der jeweiligen Rechenzentren dieses IT-Grundschutz-Profil erarbeitet.

2.2 Überblick Sicherheitskonzept

Nachfolgendes 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 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 (ISMS) bzw. zu Sicherheitskonzepten führen, sowie Standards und Normen in diesem Bereich. In Deutschland haben sich vor allem der BSI Grundschutz und ISO 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 so genannten Informationsverbund, darüber hinaus formulieren übergeordnete Bausteine grundlegende, organisatorische oder personelle Anforderungen.

Das Vorgehen nach IT-Grundschutz, wie es in dem vorliegenden IT-Grundschutz-Profil zur Anwendung kam, nutzt folgenden Zweischritt:

1. Ausgehend von ausgewählten Geschäftsprozessen wird eine relativ grobe Schutzbedarfsfeststellung in drei Klassen „normal“, „hoch“ bzw. „sehr hoch“ hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit durchgeführt.
2. Bei der anschließende Modellierung des Informationsverbunds 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 zur 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 erhöhten 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 DIN EN ISO/IEC 270xx Normen. 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 ISO/IEC 27005 detailliert beschriebenen Risikomanagementprozess zugeführt. ISO 27001 beschreibt die Anforderungen an eine Sicherheitsorganisation. Im Anhang 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 zwischen ISO/IEC 27001 sowie ISO/IEC 27002 zum IT-Grundschutz findet sich unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_modernisierter_IT_Grundschutz.pdf (letzter Zugriff 02.09.2020).

3 Formale Aspekte

Titel:	IT-Grundschutz-Profil für Hochschulen
Autorenschaft:	Siehe Punkt 6 „Liste der Autorinnen und Autoren“
Herausgeberschaft:	Arbeitskreis Informationssicherheit im ZKI e. V. (Zentren für Kommunikationsverarbeitung in Forschung und Lehre). Informationen zu Kontaktmöglichkeiten unter zki.de/goto/gp-piJ19w
Versionsstand:	1.0, veröffentlicht am 08.09.2020 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 2020
Revisionszyklus:	Es wird nach Freigabe der Version 1.0 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 ihre 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-Profile für Hochschulen“ beteiligt. Die Workshops wurden vom Arbeitskreis Informationssicherheit des ZKI e.V (Zentren für Kommunikationsverarbeitung in Forschung und Lehre) veranstaltet, die Moderation lag bei Vertretern des BSI. Die Beteiligten werden in der nachfolgenden Tabelle in alphabetischer Reihenfolge aufgeführt.

Name, Vorname	Organisation
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
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 Heimholtzzentrum 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
Neidt, Dirk	Christian-Albrechts-Universität zu Kiel
Paul, Manfred	Hochschule München
Paulsen, Christian	HafenCity Universität Hamburg
Plehn, Hartmut	Universität Bamberg
Rentzsch, Sylvia	Universität Magdeburg
Rienecker, Steffen	Universität Leizig
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, Informationsicherheitsbeauftragte (ISB, CISO), CIOs, Rechenzentrumsleitungen 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 Hochschule leistet hier eine Hilfestellung. Entstanden aus der gemeinsamen Arbeit von Informationssicherheitsbeauftragten und Rechenzentrumsmitarbeitern 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, ISO 27001 und ISIS12 (für den Bereich mittelständischer Industrie, hier nicht weiter betrachtet) 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 Schutzbedarfsfestellung 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 und IT- und Gebäude-Infrastruktur) in Form sogenannter Prozesslandkarten mit konkreter Zuordnung von Bausteinen des IT-Grundschutz-Kompendiums modelliert. Für die Anwendung der einzelnen Bausteine in der Hochschule werden Umsetzungsempfehlungen gegeben, die von Vertretern der Mitgliedseinrichtungen im Arbeitskreis Informationssicherheit des ZKI kontinuierlich weiterentwickelt werden. Dies ermöglicht zum Beispiel 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 beschrieben 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 Basis dessen 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:

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

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 vorhanden Dienste- und Netzwerkinfrastruktur einer Hochschule.

Es wird davon ausgegangen, dass für weitere Geschäftsprozesse z. B. im Bereich der Hochschulverwaltung (Finanzwesen etc.) oder 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 sog. übergeordneten Bausteinen, die vor allem organisatorische Maßnahmen beinhalten, sowie der im Rahmen der o.g. Geschäftsprozesse definierten Bausteine 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 Information Security Management Systems (ISMS), einiger weiterer Maßnahmen im Bereich Organisation und Personal und 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 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 im Abschnitt 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 (Information Security Management Systems) 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 die Autorinnen und Autoren 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 Prozessen ein hoher Schutzbedarf definiert. Ein Beispiel ist die Einschätzung eines hohen Schutzbedarfs beim Prozess Immatrikulation und Studierendenmanagement bezüglich Vertraulichkeit oder beim Prozess Prüfungen bezüglich Vertraulichkeit und Integrität (teilweise auch Verfügbarkeit, zumindest bei Durchführung elektronischer Prüfungen). Diese Einschätzung kann von Hochschule zu Hochschule abweichen und bedarf 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 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 Durchführung von Risikoanalysen und gegebenenfalls 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 Informationsverbunds

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:

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

9.2 Nicht berücksichtigte Objekte

Im IT-Grundschutz-Profil für Hochschulen werden über die im 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, so dass sich der Ergänzungsaufwand gemäß Einschätzung der Autoren und Autorinnen 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 Punkt 9.1) entwickelt. Diese decken nicht den vollständigen Bedarf umzusetzender Maßnahmen für die gesamte Hochschule ab. Welche weiteren Maßnahmen überprüft und in einem folgendem 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 Campusmanagement sind Anforderungen der Zentralverwaltung und der Forschung zu evaluieren.

Da für Zielobjekte des Campusmanagements 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.

Einen detaillierten Überblick über die untersuchten Prozesse und geprüften Bausteine sind im Kapitel 11 zu finden. Diese sind schrittweise zu erweitern.

Durch 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 der Hochschulen 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.
Ganz voran das Thema Videoconferencing. Hierzu erschien in Q2 2020 das Kompendium Videokonferenzsysteme des BSI (KoViKo 1.0.1). Die Anforderungen an die Sicherheit bei Systemzugängen, bei Authentifizierung und bei Clouddienstleistungen 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. Die entsprechenden Unterprozesse sind in den Prozesslandkarten im Anhang detailliert dargestellt. Darüber hinaus werden einzelne übergreifende Dienste und Anwendungen betrachtet, die sowohl im Zusammenhang mit den nachfolgenden Prozessen stehen und von Mitarbeiterinnen und Mitarbeitern der Hochschulen sowie (zumindest teilweise) auch von Studierenden genutzt werden.

Die drei Prozesse

- Bewerbung und Zulassung,
- Immatrikulation und Studierendenmanagement und
- 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, wie z. B.

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

übernehmen.

10.1.1 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, gegebenenfalls auch nur für bestimmte Bewerbergruppen, zu Studiengängen in den verschiedenen Varianten (z. B. durch Ranking, Auswahlgespräche etc.) sowie Annahmeverfahren (der BewerberInnen).

Anwendungen:

- Campus Management System: HISinOne APP (Webserver, Datenbank, Applikationsserver), ggf. andere,
- eLearning System (teilweise für eBewerbungen im Einsatz),
- Office PC.

Schnittstellen zu externen Systemen:

- DOSV-Portal (hochschulstart.de) und
- Uni-Assist (extern).

10.1.2 Immatrikulation und Studierendenmanagement

„Immatrikulation“ umfasst die Einschreibung zugelassener BewerberInnen (die den Studienplatz angenommen haben) und der BewerberInnen für zulassungsfreie Studiengänge. Er 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“.

Anwendungen:

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

10.1.3 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 ePrüfungen: Citrix, LanDesk etc.,
- EvaExam,
- Moodle,
- Dokumentenmanagementsystem, z. B. Codia.

10.1.4 IT-Infrastruktur für Studierende

Dieser Prozess umfasst 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 internen 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,
- eLearning Plattform,
- Chat/Messenger Plattform,
- Veranstaltungsaufzeichnung,
- Zentraler Speicherplatz,
- Print-Services,
- Nutzersupport.

10.1.5 Übergreifende Anwendungen

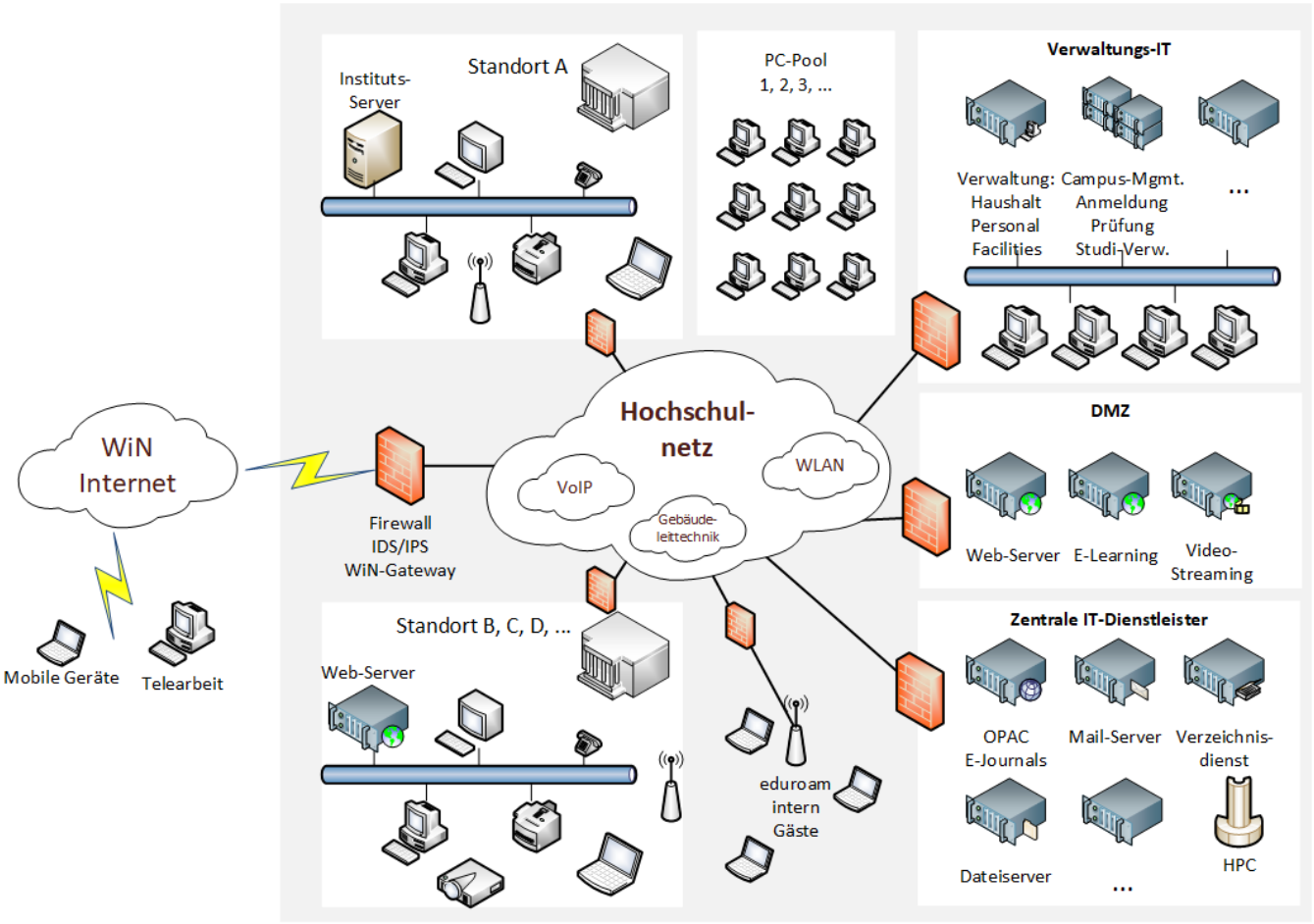
Nachfolgend sind übergreifend verwendete Anwendungen im Rahmen der genannten Prozesse zusammengestellt. Diese werden von Mitarbeitenden der Hochschulen verwendet, sind teilweise jedoch für die oben genannten Prozesse unabdingbare Voraussetzung (z. B. IDM, Backup) oder werden von Mitarbeitenden und Studierenden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

- Remote-Zugang (WLAN/eduroam, VPN),
- Webauftritt der Hochschule,
- Identity Management,
- DFN-AAI,
- Verzeichnisdienste (AD/LDAP),
- Backup, z. B. TSM-Tivoli,
- E-Mail-Plattform,
- Netzwerk-/Internetzugang LAN,
- Arbeitsplatz (Office)-PCs für Mitarbeitende im Verwaltungsbereich,
- Arbeitsplatz-PCs allgemein,
- Browser,
- Endpoint-Security.

10.2 Umgang mit Abweichungen und Ergänzungen

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

10.3 Netzplan



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 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 Bausteine), die für die einzelnen Hochschulen 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 übergeordneten 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 Kern-Betrieb 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 fünf wesentlichen Geschäftsprozesse und übergreifenden Anwendungen wurden im vorherigen Kapitel beschrieben, sie sind als Prozesslandkarten im 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 Nutzung dieser und Erklärungen der verwendeten Symbole sind im Anhang zu finden:

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

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 perspektivisch die Standard-Anforderungen umgesetzt 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 vom individuellen Fall ab.

Die Reihenfolge der Umsetzung empfiehlt sich, wie oben bereits beschrieben, gemäß Kennzeichnung R1 bis R3.

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 ORP.3 Identitäts und Berechtigungs-management ORP.4	Datensicherungs-konzept CON.3 Löschen und Vernichten CON.6	Ordnungsgemäße IT Administration OPS.1.1.2 Patch und Änderungsmanagement 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 Auswahl und Einsatz von Standardsoftware CON.4	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 Entwicklung und Einsatz von Individualsoftware CON.5 Informations-sicherheit bei Auslandsreisen CON.7 Informations-austausch CON.9	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 weitreichender Sicherheitsvorfälle DER.2.3 Audits und Revisionen DER.3.1 Notfall-management DER.4

11.3 Übersicht II: Bausteine aus der Landkarte

Die in diesem Kapitel aufgelisteten Bausteine finden sich auch in den Landkarten in Kapitel 15 und sind dort einzelnen Zielobjekten zugeordnet. Auf 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 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 hinaus 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 Verzeichnisdienst
- APP.2.2 Active Directory
- APP.2.3 OpenLDAP

- APP.3.1 Webanwendungen
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.6 DNS-Server
- APP.4.2 SAP-ERP-System
- APP.4.3 Relationale Datenbanksysteme
- APP.4.6 SAP ABAP-Programmierung
- APP.5.1 Allgemeine Groupware
- APP.5.2 Microsoft Exchange und Outlook

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 Container
- 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.4.5 Wechseldatenträger

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.3 Elektronische Verkabelung
- INF.4 IT-Verkabelung
- 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 Schulungsraum

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 aufwändigen 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 Abschnitt 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	
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell 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 daher 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“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. • Geringfügige Vertragsverletzungen mit höchstens geringen Konventionalstrafen.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• 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“

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 vier 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 jedoch nicht existenzbedrohend.

Tabelle 2: Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze. • Vertragsverletzungen, deren Haftungsschäden ruinös sind.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• 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 unter anderem 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“.

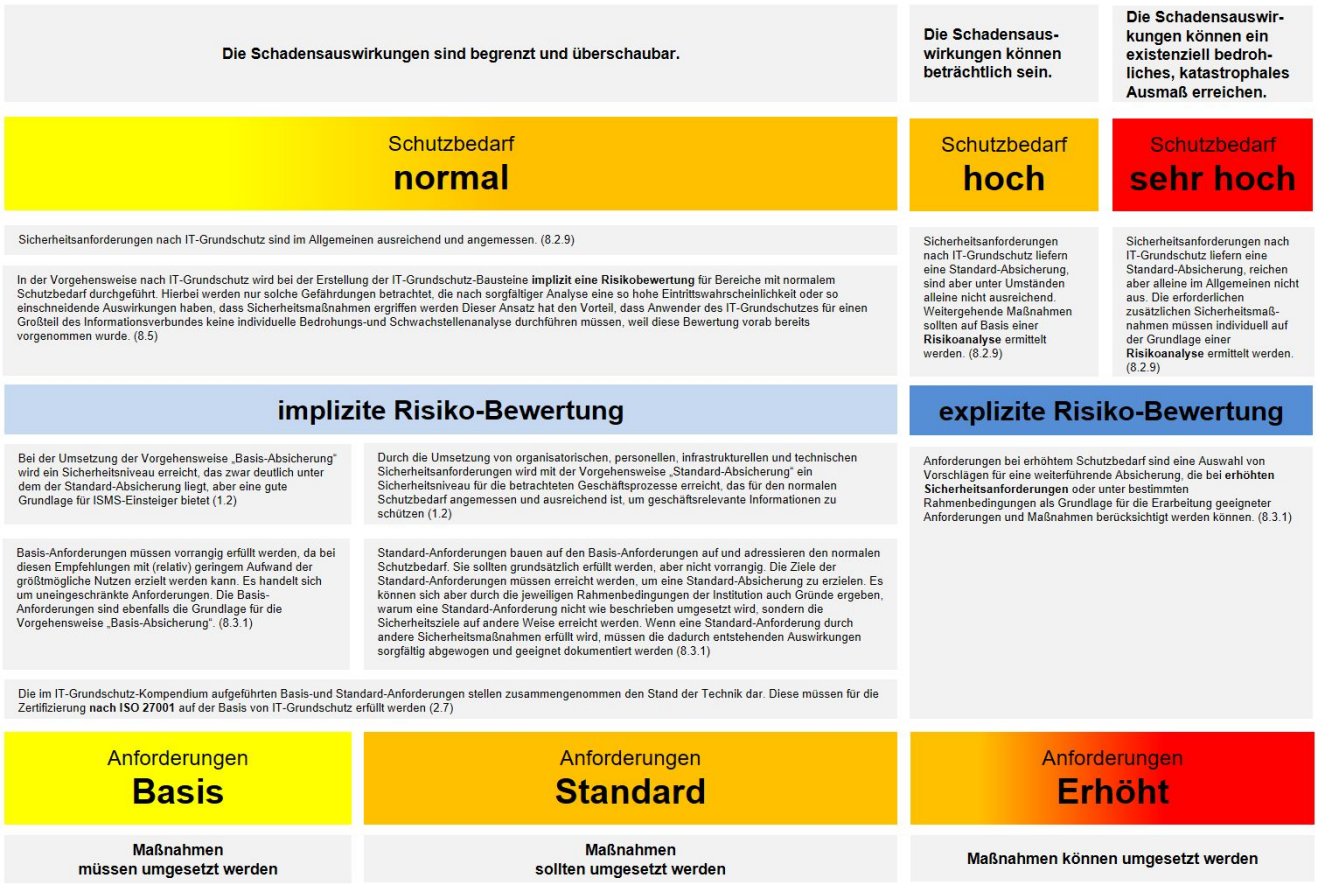
Für manche Zielobjekte wird in diesem IT-Grundschutz-Profil der Schutzbedarf „hoch“ definiert. Hier reichen die Maßnahmen der Basis- und Standard-Absicherung unter Umständen nicht mehr aus. In diesen Fällen muss eine

individuelle Risikoanalyse erfolgen, auf Basis derer dann Maßnahmen festgelegt werden müssen. Hinweise zur Durchführung einer Risikoanalyse finden sich in Kapitel 14. Hinweise zur Durchführung einer Risikoanalyse.

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 für Maßnahmen für einen erhöhten Schutzbedarf einzelner Bausteine befinden sich bei den Bausteinbeschreibungen, Umsetzungshinweise zu den Maßnahmen für die einzelnen Bausteine sind im nichtöffentlichen Teil des Anhangs zusammengestellt. Ein Beispiel für die Betrachtung eines Teilprozesses mit hohem Schutzbedarf findet sich im nächsten 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.

Das nachfolgende Schaubild fasst das Vorgehen nochmal in einer Übersicht zusammen.



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 geeignet zu übertragen.

Beispiel: Baustein ORP.3 Sensibilisierung und Schulung:

„ORP.3.A9 Spezielle Schulung von exponierten Personen und Institutionen (CIA)

Besonders exponierte Personen wie Funktionsträger sowie die Mitarbeiter in besonders exponierten Institutionen oder Organisationsbereichen 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:

- 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.

- 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.

- Gefährdungsübersicht ergänzen

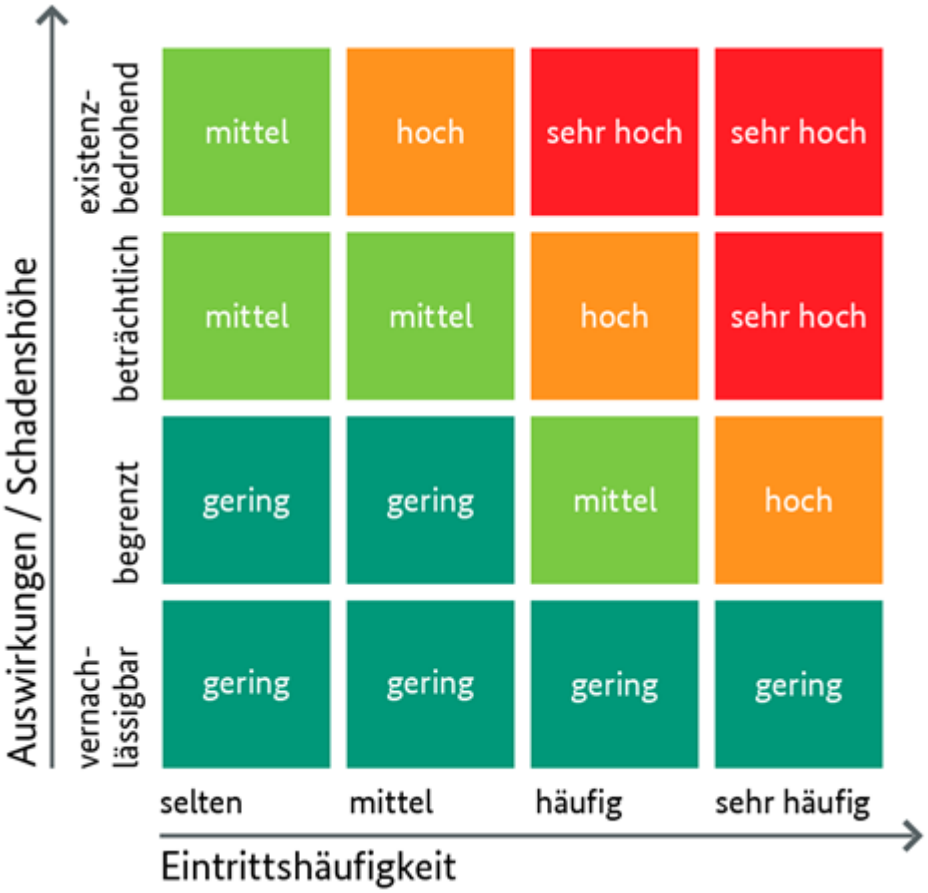
  Auch wenn die Zusammenstellung elementarer Gefährdungen vielfältige Bedrohungen berücksichtigt, denen Informationen und Informationstechnik ausgesetzt sind, so kann dennoch nicht ausgeschlossen werden, dass weitere Gefährdungen zu betrachten sind. Dies gilt insbesondere dann, wenn es für ein Zielobjekt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

- 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 mit Hilfe von Kategorien zur Beschreibung der Größenordnung, bestimmt werden.

- Risiken bewerten

  Nachdem Sie die Eintrittshäufigkeiten und Schadensauswirkungen einer Gefährdung eingeschätzt haben, können Sie 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 Sie an die Gegebenheiten und Erfordernisse Ihrer Institution anpassen können.



- Risiken behandeln

In der Regel wird die Gefährdungsbewertung aufzeigen, dass nicht alle Gefährdungen durch das vorhandene Sicherheitskonzept ausreichend abgedeckt sind. In diesem Fall müssen Sie überlegen, wie angemessen mit den verbleibenden Gefährdungen umgegangen werden kann, und eine begründete Entscheidung hierzu treffen.

- 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. Landkarte Geschäftsprozess Bewerbung und Zulassung

„Bewerbung“ umfasst die Einrichtung von Bewerbungsverfahren für grundständige und Masterstudiengänge (inklusive verschiedener Studierendengruppen – auch z.B. Hochschulwechsler, Gasthörer, Zweithörer – Bewerbungszeiträumen, 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, gegebenenfalls auch nur für bestimmte Bewerbergruppen, zu Studiengängen in den verschiedenen Varianten (z. B. durch Ranking, Auswahlgespräche etc.) sowie Annahmeverfahren (der BewerberInnen).

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 SCLM, Campusnet CampusOnline Primuss FactScience) APP.3.1 APP.3.2 APP.4.3	VMWare Virtualisierung ! SYS.1.1 SYS.1.5	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10
			Windows Server 2012 ! SYS.1.1 SYS.1.2.2	
			Linux Server ! SYS.1.1 SYS.1.3	Serverraum ! INF.2 Technikraum ! INF.5
		DOSV-Portal OPS.2.2	Container ! SYS.1.6	
		Uni-Assist (extern)	Zentrales Storage System ! SYS.1.1 SYS.1.8	

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 Campusmanagementsystem, das Identity Management System und externe Systeme werden beim Prozess "Übergreifende Anwendungen" (Kapitel 15.5) berücksichtigt. Sofern Server als virtuelle Maschinen laufen, ist das IT-System VMware-Virtualisierung (mit Bausteinen SYS.1.1 und SYS.1.5) zusätzlich zu berücksichtigen.

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 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.

15.2 Landkarte Immatrikulation und Studierendenmanagement

„Immatrikulation“ umfasst die Einschreibung zugelassener BewerberInnen (die den Studienplatz angenommen haben) und der BewerberInnen 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 SCLM, Campusnet CampusOnline Primuss FactScience) APP.3.1 APP.3.2 APP.4.3	VMWare Virtualisierung ! SYS.1.1 SYS.1.5 Windows Server 2012 ! SYS.1.1 SYS.1.2.2 Linux Server ! SYS.1.1 SYS.1.3 Container ! SYS.1.6 Zentrales Storage System ! SYS.1.1 SYS.1.8	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10 Serverraum ! INF.2 Technikraum ! INF.5

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 mit verarbeitet. 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 Campusmanagementsystem, das Identity Management System und externe Systeme werden beim Prozess "Übergreifende Anwendungen" (Kapitel 15.5) berücksichtigt. Sofern Server als virtuelle Maschinen laufen, ist das IT-System VMware-Virtualisierung (mit Bausteinen SYS.1.1 und SYS.1.5) zusätzlich zu berücksichtigen.

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 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.

15.3 Landkarte 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 eLearning-Systeme, die zur Durchführung von Online Prüfungen geeignet sind) erfasst sind. Die Clientseite zum Zugriff auf diese ePrüfungen ist im Prozess „Infrastruktur für Studierende“ im Kapitel 15.4 separat berücksichtigt. Die Clientseite zur Verwaltung von Prüfungen und deren Ergebnissen sowie die IT Systeme zum Scannen von Prüfungsantwortbögen sind hier mit erfasst.

Der Prozess Prüfungen umfasst die folgenden Unterprozesse:

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Prüfungen	Planen, Durchführung: • Prüfungsfragen erstellen • Durchführung der Prüfung • Prüfungsbögen erstellen • Anwesenheits-kontrolle Bewerten: • Prüfungen bewerten • Noten im Campus Management System speichern Prüfungsergebnisse bereitstellen / veröffentlichen Archivieren & Auskunft: • Backup erstellen, • Archiv erstellen, • Papierarchiv erstellen, • Verifikation der Auskunft, • Ausheben der Prüfungsdaten /-Zeugnisse, • Prüfungsdaten /-Zeugnisse übertragen / bekannt geben	HISinOne EXA ! (Alternativ: SAP SCLM, Campusnet CampusOnline Primuss FactScience) APP.3.1 APP.3.2 APP.4.3	VMWare Virtualisierung ! SYS.1.1 SYS.1.5	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10
			Windows Server 2012 ! SYS.1.1 SYS.1.2.2	
			Linux Server ! SYS.1.1 SYS.1.3	Serverraum ! INF.2 Technikraum ! INF.5
		ePrüfungs-System ! • LPLUS • EvaExam APP.3.1 APP.3.2 APP.4.3	Container ! SYS.1.6	Büroraum ! INF.7
			Zentrales Storage ! System SYS.1.1 SYS.1.8	Archiv INF.6
		eLearning System ! • Moodle • Ilias • StudIP APP.3.1 APP.3.2 APP.4.3	Windows 10 Client ! SYS.2.1 SYS.2.2.3	
			Drucker, Kopierer, Multifunktionsgeräte ! SYS.4.1	
		Papierarchiv		

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 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 käme sonst in der Regel nur der Abbruch und Wiederholung der gesamten Prüfung in Frage.

Sofern Server als virtuelle Maschinen laufen ist das IT-System VMware-Virtualisierung (mit Bausteinen SYS.1.1 und SYS.1.5) zusätzlich zu berücksichtigen.

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).

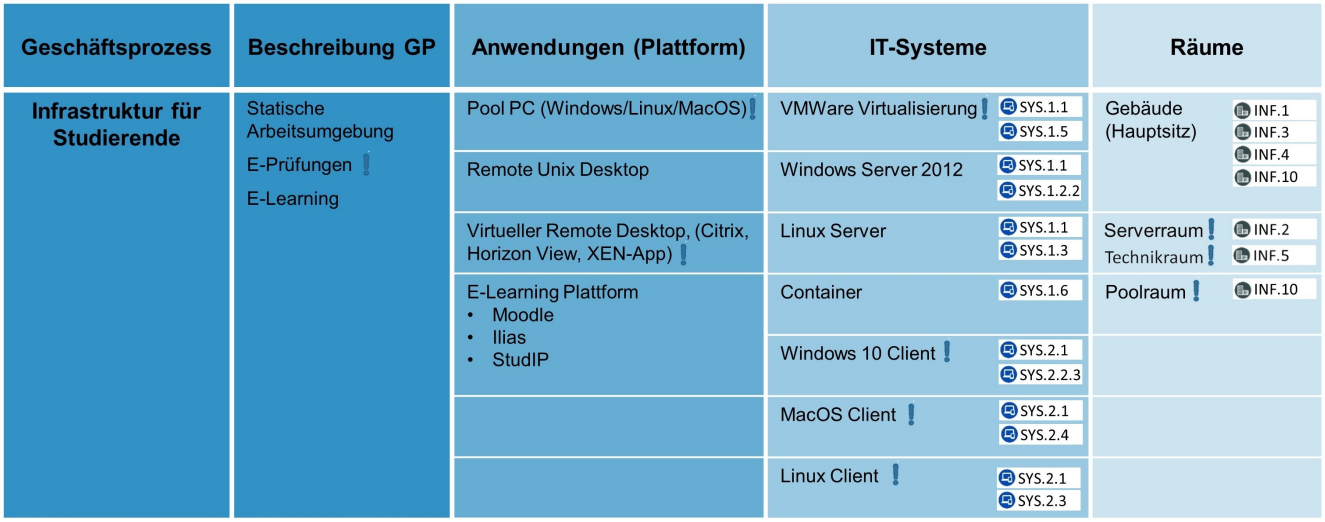
Für diese Anwendungen gelten die Einschätzungen für den Schutzbedarf sowie die darunterliegenden IT-Systeme entsprechend.

15.4 Landkarte IT-Infrastruktur für Studierende

Bereitstellung einer Arbeitsumgebung im Rahmen von Studium und Lehre.

Diese Arbeitsumgebung umfasst die Bereitstellung von zentralen Diensten mit externem Zugang durch eigene Geräte sowie internen Zugang durch zentral bereitgestellte Systeme.

Im Geschäftsprozess „Prüfung“ (siehe Kapitel 15.3) 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 „!“.



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 käme sonst in der Regel nur der Abbruch und die Wiederholung der gesamten Prüfung in Frage.

15.5. Landkarte Übergreifende Anwendungen

Hier werden übergreifend verwendete Anwendungen, die Basisinfrastruktur und Basisdienste eines Hochschulrechenzentrums im Rahmen der genannten Prozesse, zusammengestellt, die vor allem auch für die Durchführung der oben genannten Prozesse erforderlich sind

Diese werden aus Gründen der Übersichtlichkeit als Prozesse der "Übergreifenden Anwendungen" auf zwei entsprechenden Landkarten zusammengefasst. Der Schutzbedarf für diese Anwendungen ergibt sich teilweise aus dem Schutzbedarf der oben bereits zusammengestellten einzelnen Unterprozesse.

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Übergreifende Anwendungen 1	Mobiler Zugriff, Remotearbeit (VPN, eduroam, WLAN) Statische Arbeitsumgebung Netzwerkinfrastruktur-Dienste/WLAN	IPSec VPN (Checkpoint Mobile Access, Cisco AnyConnect)	VMWare Virtualisierung ! Virtual Appliance SYS.1.1 SYS.1.5	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10
		IPsec-VPN (OpenSwan/StrongSwan)	Windows Server 2012 SYS.1.1 SYS.1.2.2	
		OpenVPN (SSL-VPN)	Linux Server SYS.1.1 SYS.1.3	Serverraum ! INF.2 Technikraum ! INF.5
		RadsecProxy, SecureW2 (eduroam)	Windows 10 Client SYS.2.1 SYS.2.2.3	Büroraum INF.7
		Virtueller Remote Desktop, (Citrix (GU), Horizon View, XEN-App)	MacOS Client SYS.2.1 SYS.2.4	Home Office INF.8
		Windows 10 Arbeitsplatz	VPN Gateway/Firewall SYS.1.1	Mobiler Arbeitsplatz INF.9
		Client mit Office, ! Browser,E-Mail APP.1.1 APP.1.2	Desktop/Notebook ! SYS.2.1 SYS.3.1	
		Arbeitsplatz bereitstellen (SCCM, Zenworks, Jamf) APP.1.4	Speichersystem SYS.1.1 SYS.1.8	
		DNS APP.3.6	Netze ! NET.1.1 NET.1.2 NET.3.1 NET.3.2 NET.4.2 • LAN, Switches, • Router, Firewall, • VoIP	
		TK-Anlage NET.4.1 NET.4.2		
			WLAN, VPN NET.3.3 NET.2.1 NET.2.2	
			Tablet und Smartphone, Mobiltelefon SYS.3.2.1 SYS.3.2.2 SYS.3.2.3 SYS.3.2.4 SYS.3.3	
			Wechseldatenträger SYS.4.5	

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Übergreifende Anwendungen 2	Zentrale Dienste: Identity Management/Authentication Groupware/eMail/Chat Fileservice/SyncShare Print Services Webauftritt Virtuelle Serverdienste Ticketsystem	Verzeichnisdienst (Active Directory)! APP.2.2	VMWare Virtualisierung! SYS.1.1, SYS.1.5	Gebäude (Hauptsitz) INF.1, INF.3, INF.4, INF.10
		LDAP, Kerberos, Radius (Verzeichnisdienst/Authentication)! APP.2.3	Windows Server 2012! SYS.1.1, SYS.1.2.2	
		Shibboleth (DFN-AAI)! APP.2.1	Linux Server! SYS.1.1, SYS.1.3	Serverraum! INF.2 Technikraum! INF.5
		Identity Management! APP.2.1, APP.4.3	Container! SYS.1.6	
		MS Exchange (E-Mail) APP.5.2	Windows 10 Client SYS.2.1, SYS.2.2.3	
		Chat /Messenger APP.5.1	MacOS Client SYS.2.1, SYS.2.4	
		Fileservice/Sync&Share APP.3.3, APP.5.2	Linux Client SYS.2.1, SYS.2.3	
		Sophos (Endpoint Security) APP.4.3, APP.3.1, APP.3.2	Drucker, Kopierer, Multifunktionsgeräte SYS.4.1	
		CUPS (Print Services)		
		Ticketsystem: OTRS, Jira ServiceDesk APP.4.3, APP.3.1, APP.3.2		
		Webserver (Webauftritt) APP.3.2, APP.4.3		
		CMS (Webauftritt) APP.4.3, APP.3.1, APP.3.2		

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 vorherigen 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.

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 2020) 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 Bausteinkommentierungen in nachfolgender Liste:

ISMS.1 Sicherheitsmanagement: zki.de/goto/gp-9XPreg

ORP.1 Organisation zki.de/goto/gp-53vbSA
ORP.2 Personal zki.de/goto/gp-eeEltw
ORP.3: Sensibilisierung und Schulung zki.de/goto/gp-n8OGIg
ORP.4 Identitäts- und Berechtigungsmanagement: zki.de/goto/gp-ghMdYA
ORP.5 Compliance Management (Anforderungsmanagement): zki.de/goto/gp-9tVcUg

CON.1 Kryptokonzept: zki.de/goto/gp-IZifMg
CON.2 Datenschutz: zki.de/goto/gp-NpCKfQ
CON.3 Datensicherungskonzept: zki.de/goto/gp-FvyzYQ
CON.4 Auswahl und Einsatz von Standardsoftware: zki.de/goto/gp-sbaCDg
CON.5 Einsatz von Individualsoftware: zki.de/goto/gp-Hc-hzg
CON.6 Löschen und Vernichten: zki.de/goto/gp-7W7dOA
CON.7 Informationssicherheit auf Auslandsreisen: zki.de/goto/gp-0s4u9g
CON.9 Informationsaustausch: zki.de/goto/gp-l2GDXA

OPS.1.1.2 Ordnungsgemäße IT-Administration: zki.de/goto/gp-CA4Pbg
OPS.1.1.3 Patch- und Änderungsmanagement: zki.de/goto/gp-Eka5JA
OPS.1.1.4 Schutz vor Schadprogrammen: zki.de/goto/gp-UiwUmw
OPS.1.1.5 Protokollierung: zki.de/goto/gp-fF0JVw
OPS.1.1.6 Software-Tests und -Freigaben: zki.de/goto/gp-Ugwm4Q
OPS.1.2.2 Archivierung: zki.de/goto/gp-NLxeSQ
OPS.1.2.4 Telearbeit: zki.de/goto/gp-xomePw
OPS.1.2.5 Fernwartung: zki.de/goto/gp-EqFDcg
OPS.2.1 Outsourcing für Kunden: zki.de/goto/gp-cnbtzg
OPS.2.2 Cloud-Nutzung: zki.de/goto/gp-VRty7Q
OPS.3.1 Outsourcing für Dienstleister: zki.de/goto/gp-hxKRLQ

DER.1 Detektion von sicherheitsrelevanten Ereignissen: zki.de/goto/gp-cMw6hQ
DER.2.1 Behandlung von Sicherheitsvorfällen: zki.de/goto/gp-6Qd47w
DER.2.2 Vorsorge für die IT-Forensik: zki.de/goto/gp-fDWKBQ
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle: zki.de/goto/gp-3lsweQ
DER.3.1 Audits und Revisionen: zki.de/goto/gp-aDI2Qg
DER.4 Notfallmanagement: zki.de/goto/gp-RmMZ9A

APP.1.1 Office Produkte: zki.de/goto/gp-hx786w
APP.1.2 Web-Browser: zki.de/goto/gp-KswnfQ
APP.2.1 Allgemeiner Verzeichnisdienst: zki.de/goto/gp-hrUEvQ
APP.2.2 Active Directory: zki.de/goto/gp-f5GhCg

APP.2.3 OpenLDAP: zki.de/goto/gp-5lrjYA
APP.3.1 Webanwendungen: zki.de/goto/gp-eUFq3w
APP.3.2 Webserver: zki.de/goto/gp-Dbur9Q
APP.3.3 Fileserver: zki.de/goto/gp-9RANFw
APP.3.6 DNS-Server: zki.de/goto/gp-xc6ruw
APP.4.2 SAP-ERP-System: zki.de/goto/gp-ubHJgQ
APP.4.3 Relationale Datenbanksysteme: zki.de/goto/gp-AEjx7A
APP.4.6 ABAP-Programmierung: zki.de/goto/gp-7rmakw
APP.5.1 Allgemeine Groupware: zki.de/goto/gp-KJXDGQ
APP.5.2 Microsoft Exchange und Outlook: zki.de/goto/gp-Bk0Zxg

SYS.1.1 Allgemeiner Server: zki.de/goto/gp-nCIBwA
SYS.1.2.2 Windows Server 2012: zki.de/goto/gp-Dnkreg
SYS.bd.1 Windows Server 2016: zki.de/goto/gp-QInHTQ
SYS.1.2.3 Windows Server 2019: zki.de/goto/gp-NHMGZw
SYS.1.3 Server unter Linux und Unix: zki.de/goto/gp-dBmr2A
SYS.1.5 Virtualisierung: zki.de/goto/gp-SSAw0w
SYS.1.6 Container: zki.de/goto/gp-1S5yrA
SYS.1.8 Speicherlösungen: zki.de/goto/gp-B3nSdw
SYS.2.1 Allgemeiner Client: zki.de/goto/gp-kdlHhQ
SYS.2.2.3 Clients unter Windows 10: zki.de/goto/gp-uWZLTg
SYS.2.3 Clients unter Linux und Unix: zki.de/goto/gp-ddyhjA
SYS.2.4 Clients unter macOS: zki.de/goto/gp-ZCCpsQ
SYS.3.1 Laptops: zki.de/goto/gp-L0ymIQ
SYS.3.2.1 Allgemeine Smartphones und Tablets: zki.de/goto/gp-gheI3g
SYS.3.2.2 Mobile Device Management (MDM): zki.de/goto/gp-rEanaA
SYS.3.2.3 iOS (for Enterprise): zki.de/goto/gp-NhHbqw
SYS.3.2.4 Android: zki.de/goto/gp-4VqUpg
SYS.3.3 Mobiltelefon: zki.de/goto/gp-epk76A
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte: zki.de/goto/gp-0gcVAg
SYS.4.5 Wechseldatenträger: zki.de/goto/gp-JffVYQ

NET.1.1 Netzarchitektur und -design: zki.de/goto/gp-sEzS4g
NET.1.2 Netzmanagement: zki.de/goto/gp-dvuV0g
NET.2.1 WLAN-Betrieb: zki.de/goto/gp-WKq6ZA
NET.2.2 WLAN-Nutzung: zki.de/goto/gp-ZfnKjQ
NET.3.1 Router und Switches: zki.de/goto/gp-IWaByw
NET.3.2 Firewall: zki.de/goto/gp-sg1NnQ
NET.3.3 VPN: zki.de/goto/gp-kCwnwg
NET.4.1 TK-Anlagen: zki.de/goto/gp-7kiAfA
NET.4.2 VoIP: zki.de/goto/gp-wBmvyg

INF.1 Allgemeines Gebäude: zki.de/goto/gp-y4N6dg
INF.2 Rechenzentrum sowie Serverraum: zki.de/goto/gp-ocqyXg
INF.3 Elektronische Verkabelung: zki.de/goto/gp-iegsQg
INF.4 IT-Verkabelung: zki.de/goto/gp-qVOjLA
INF.5 Raum sowie Schrank für technische Infrastruktur: zki.de/goto/gp-7PwOhg
INF.6 Datenträgerarchiv: zki.de/goto/gp-zRFA2g
INF.7 Büroarbeitsplatz: zki.de/goto/gp-ueuB8A
INF.8 Häuslicher Arbeitsplatz: zki.de/goto/gp-s20bjQ

INF.9 Mobiler Arbeitsplatz: zki.de/goto/gp-nphuVw
INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum: zki.de/goto/gp-6utaFA