Zentren für
Kommunikation und
Informationsverarbeitung e.V.

IT-Grundschutz-Profil für Hochschulen

Version 0.9, 25.11.2019

Community Draft

Inhaltsverzeichnis

1 Vorwort

Das vorliegende IT-Grundschutzprofil 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 Profil, das als Schablone für die eigene Hochschule adaptiert werden und als Basis für ein Informationssicherheitskonzept der eigenen Hochschule dienen kann.

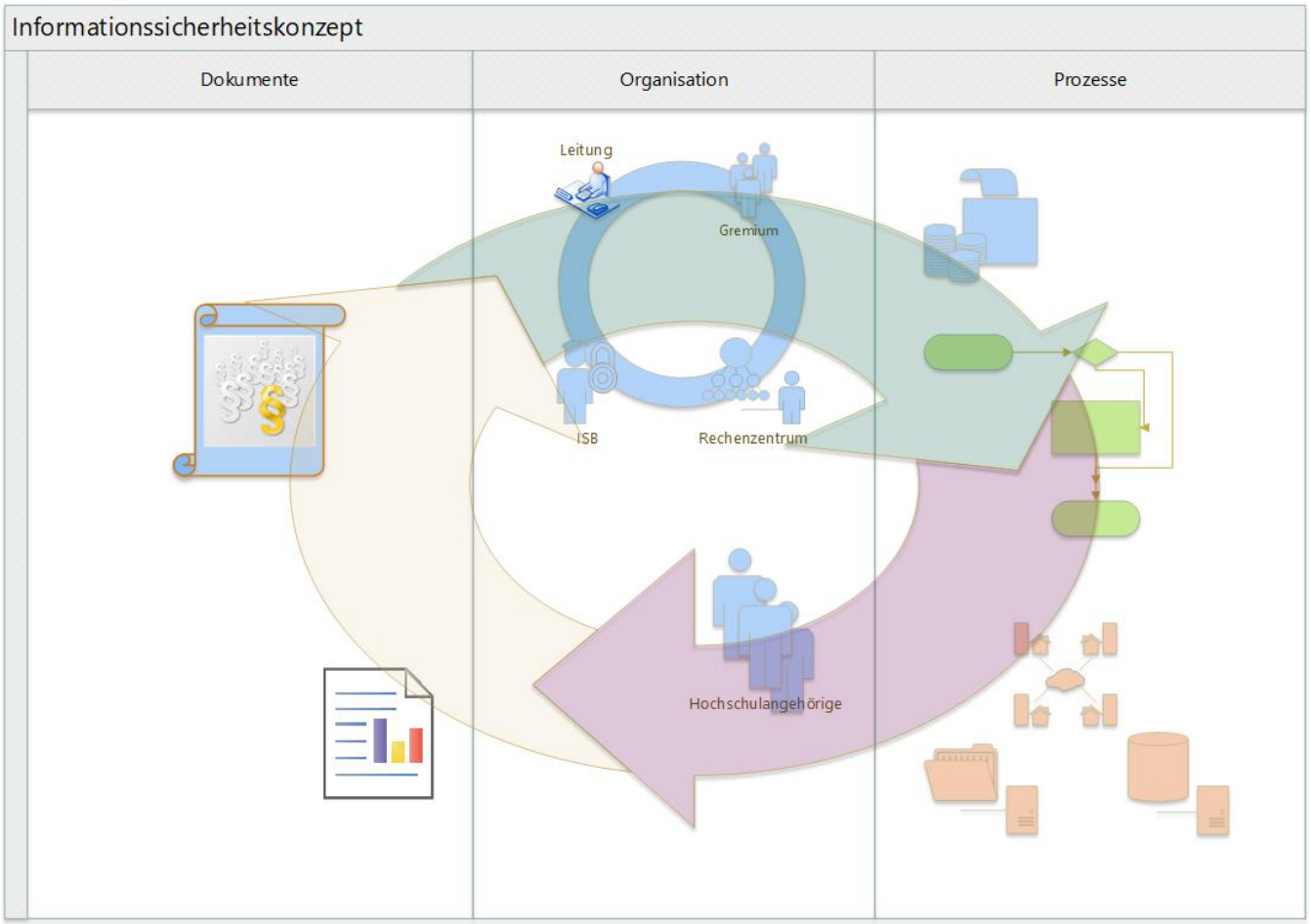
In Hochschulen ergeben sich durch eine große Breite an Aufgabengebieten in Forschung und Lehre und durch die sehr dezentrale Organisation viele unterschiedliche Ausprägungen von IT-Landschaften und deren Management. Dieses Profil erhebt damit nicht den Anspruch auf Vollständigkeit, sondern kann sich 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 übergeordnete 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 generell für den ganzen Informationsverbund gelten.
Das vorliegende IT-Grundschutz-Profil soll Hochschulen damit wirkungsvoll dabei helfen, die Erstellung eines Informationssicherheitskonzepts auf Basis der BSI-Grundschutz-Vorgehensweise handhabbar zu machen. Der restliche Weg bis zum vollständigen Informationssicherheitskonzept der eigenen Hochschule wird somit realistisch.
Wir danken den Experten und Expertinnen aus den Mitgliedshochschulen und den Mitarbeiterinnen und Mitarbeitern des BSI für Ihren Einsatz bei der der Erstellung dieses IT-Grundschutz-Profils.
Die Sprecher des Arbeitskreises Informationssicherheit im ZKI e.V.

2 Einleitung

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 Grundschutzprofil erarbeitet.

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 Profils ist es, den Hochschulen ein Standardvorgehen an die Hand zu geben, das bei Erstellung der eigenen Sicherheitskonzeption wertvolle Hilfestellung geben kann.



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)
Registrierungsnummer:	Wird nach erfolgreichem Durchlaufen des Registrierungsverfahrens vom BSI vergeben
Versionsstand:	0.9
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, so dass 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
False, Jana	Technische Universität Ilmenau
Glowatz, Christoph	Hochschule Düsseldorf
Keil, Andreas	Deutsche Sporthochschule Köln
Kramert, Grit	Frankfurt University of Applied Sciences
Kryzanowski, Arnold	Hochschule München
Kunze, Rüdiger	GEOMAR Helmholtzzentrum für Ozeanforschung Kiel
Lauer, Hermann	Universität Heidelberg
Leendertse, Jan	Albert-Ludwigs-Universität Freiburg
Leitel, Jana	Friedrich-Schiller-Universität Jena
Mai, Martin	Universität Bamberg
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 Leipzig
Sander, Jürgen	DFN-CERT
Schwarz, Stefan	UniBw München
Ulber, Peter	Universität Stuttgart
Weichert, Ralph	Hochschule RheinMain
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, IT-Sicherheitsbeauftragte, CIOs bzw. Rechenzentrumsleiter und andere Verantwortliche an Hochschulen, die die Informationssicherheit in ihrer Hochschule sicherstellen müssen und bei denen die Zuständigkeit für Umsetzung und Aufrechterhaltung der Informationssicherheit liegt.

7.2 Zielsetzung

Ziel dieses IT-Grundschutzprofils ist ein einfacherer Einstieg in die Schaffung von Informationssicherheit an Hochschulen durch Beschreibung einer Vorgehensweise, die einfach auf die individuellen Rahmenbedingungen einer Hochschule übertragen werden kann. Aufgrund der großen Ähnlichkeit der Geschäftsprozesse an Hochschulen in den Bereichen Forschung, Lehre und Weiterbildung gibt dieses IT-Grundschutzprofil eine allgemeine Handlungsanweisung zur Umsetzung von Maßnahmen. Im Fokus stehen drei Geschäftsprozesse im Bereich der Lehre, ein Prozess zur Bereitstellung von IT-Infrastruktur für Studierende sowie ein unterstützender Prozess für übergreifende Anwendungen.

Die fünf betrachteten Geschäftsprozesse sind:

- **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-Grundschutzprofils 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 nur noch sehr wenige zusätzliche Bausteine zu betrachten sind.

7.3 Vorgehen

Dieses IT-Grundschutzprofil zeigt ein modulares Vorgehen zur Definition und Umsetzung von Maßnahmen aus vordefinierten Bausteinen zur Erhöhung der Informationssicherheit an einer Hochschule auf. Es empfiehlt die Umsetzung von Maßnahmen aus sog. übergeordneten Bausteinen, die vor allem organisatorische Maßnahmen beinhalten, sowie der im Rahmen der o.g. Geschäftsprozesse definierten Bausteine. 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 Maßnahmen zur Basisabsicherung, der Standardabsicherung und für erhöhten Schutzbedarf beschrieben. Wir empfehlen bei Umsetzung aller Maßnahmen, zuerst mit dem Ziel der Basisabsicherung zu beginnen und

anschließend die Standardabsicherung und ggf. 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 zu finden. In Fällen, in denen ein hoher Schutzbedarf besteht, ist eine individuelle Risikobewertung durchzuführen, um festzustellen, ob die o.g. Maßnahmen zur Basis bzw. Standardabsicherung ausreichen oder ob weitere Maßnahmen 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. In den meisten Fällen gehen die Autoren von “normalem” Schutzbedarf aus. Gleichzeitig empfehlen die 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 Profils nicht durchgeführt. Die individuelle Umsetzung des Profils bringt die Notwendigkeit mit sich, die hier als Empfehlung formulierten Schutzbedarfskategorien individuell zu prüfen und ggf. anzupassen.

Nachdem die Verarbeitung von Studierendendaten aber das Kerngeschäft einer Hochschule ausmachen und 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 allerdings von Hochschule zu Hochschule abweichen und bedarf ggf. 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 ISO27001 konformes Sicherheitsniveau wird bei Prozessen mit Schutzbedarf "normal" erst mit Anwendung der IT-Grundschutz-Vorgehensweise mit „Standard-Absicherung" erreicht, bei Prozessen mit Schutzbedarf "hoch" erst durch Anwendung erweiterter Absicherung auf Basis von Risikoanalysen bzw. der in den Bausteinen bereits definierten Umsetzungshinweise.

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. Die Autoren und Autorinnen sehen bezüglich der Auswahl der Grundschutzbausteine aber eine große Überschneidung zu anderen Hochschulprozessen, so dass sich der Ergänzungsaufwand gemäß Einschätzung der Autoren im Rahmen hält. 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-Grundschutzprofil 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-Grundschutzprofil 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 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 finden Sie im Kapitel 11. Diese sind schrittweise zu erweitern.

Durch Untersuchung von wenigen Prozessen und ausgewählten Basisdiensten konnte mit diesem 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-Grundschutzprofil für Hochschulen ergeben. In jedem Fall kann parallel zu den kommenden Arbeiten mit der Umsetzung der hier geprüften Bausteine begonnen 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 / Infrastruktur (Liegenschaften, Gebäude, Räume).

10.1 Untersuchungsgegenstand

Im folgenden werden die in diesem IT-Grundschutzprofil 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. Darüberhinaus werden einzelne übergreifende Dienste und Anwendungen betrachtet, die sowohl im Zusammenhang mit den nachfolgenden Prozessen stehen und von Mitarbeitern der Hochschulen sowie (zumindest teilweise) auch von Studierenden genutzt werden.

Die drei Prozesse

- Bewerbung und Zulassung
- Immatrikulation und Studierenden Management
- Prüfung

werden i.A. über ein sog. 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 (inkl. verschiedener Studierendengruppen – auch z.B. Hochschulwechsler, Gasthörer, Zweithörer – Bewerbungszeiträumen, Kapazitäten, Bewerbungsvoraussetzungen, rechtlichen Rahmenbedingungen etc.), die Entgegennahme von Bewerbungen in den verschiedenen Ausprägungen sowie deren Überprüfung und ggf. Bewertung (z.B. zur Notenverbesserung durch außerschulische Leistungen).

"Zulassung" beinhaltet in zulassungsbeschränkten und (ggf.) freien Studiengängen die Zulassung (bzw. Ablehnung) von BewerberInnen, ggf. auch nur für bestimmte Bewerbergruppen, zu Studiengängen in den verschiedenen Varianten (z.B. durch Ranking, Auswahlgespräche etc.) sowie Annahmeverfahren (der BewerberInnen).

Anwendungen:

- Campus-Managementsystem: HISinOne APP (Webserver, Datenbank, Applikationsserver), ggf. andere

- eLearning Systeme (teilweise für eBewerbungen im Einsatz)
- Office PC

Schnittstellen zu externen Systemen:

- DOSV-Portal (hochschulstart)
- Uni-Assist (extern)

10.1.2 Immatrikulation und Studierenden-Management

"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 der Betrachtung innerhalb dieses IT-Grundschutzprofils 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, BA-/MA-/Diplomarbeit (Abschlussprüfungen). 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.

- Campus Management System: Modul HISinOne EXA
- LPLUS
- Citrix / LanDesk etc. (Arbeitsumgebung für ePrüfungen)
- EvaExam
- Moodle
- Dokumentenmanagement-System 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 und internen Zugang durch zentral bereitgestellte Systeme sowie die darunterliegende Netzwerkinfrastruktur. In diesem IT-Grundschutzprofil wird davon ausgegangen, dass ein BYOD-Zugang (Bring-Your-Own-Device) seitens der Studierenden auf Hochschuldienste nur über WLAN erfolgt, und darüber hinaus sog. 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
- Software Angebote (Download) für Studierende
- eLearning Plattform
- Chat/Messenger Plattform
- Veranstaltungsaufzeichnung
- Zentraler Speicherplatz
- Print Services
- Nutzersupport

10.1.5 Übergeordnete Anwendungen

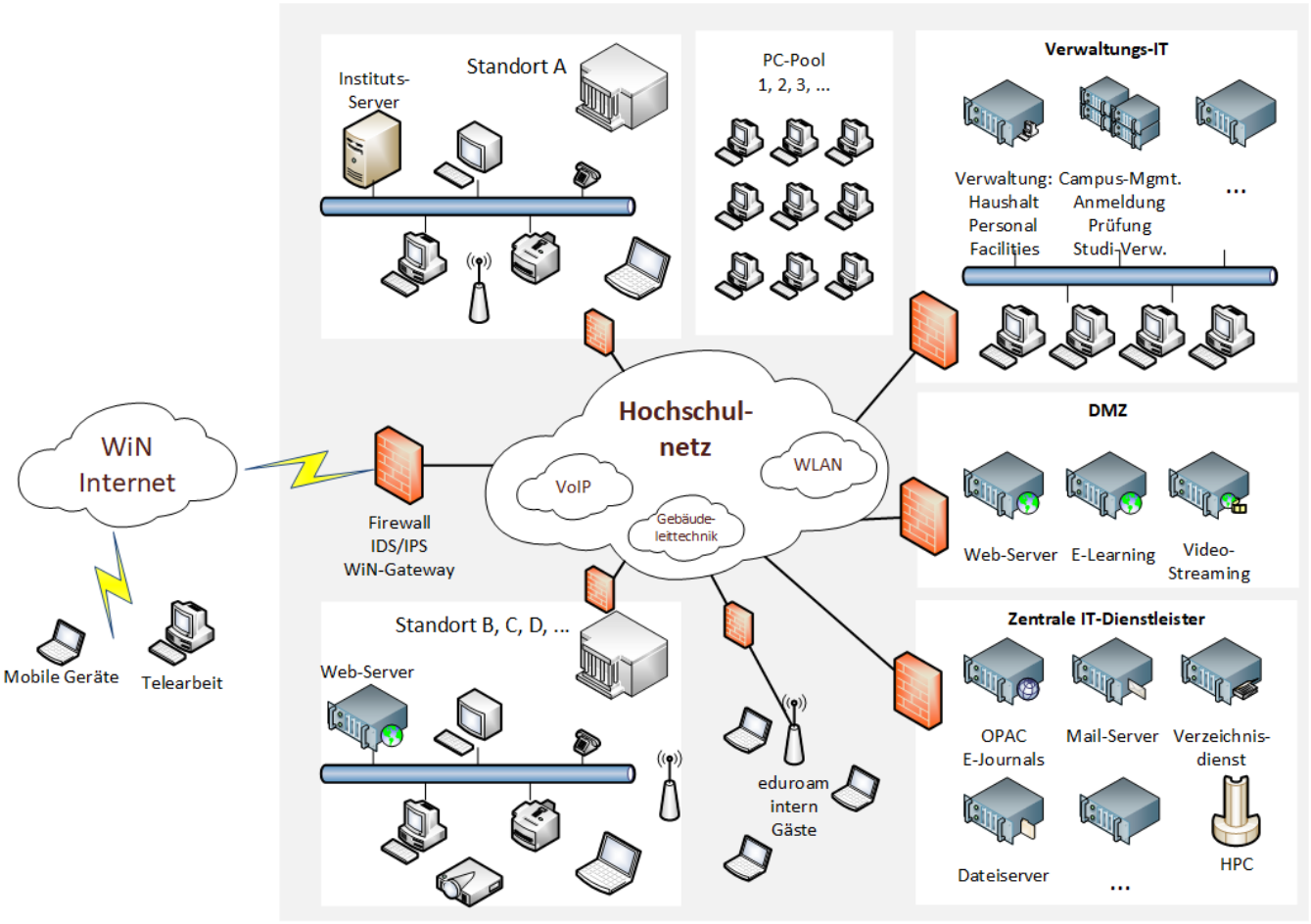
Nachfolgend sind übergeordnete und übergreifend verwendete Anwendungen im Rahmen der genannten Prozesse zusammengestellt. Diese werden von Mitarbeitern der Hochschulen verwendet, sind teilweise jedoch für die oben genannten Prozesse unabdingbare Voraussetzung (z.B. IdM, Backup) oder werden von Mitarbeitern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

- Remote Zugang (WLAN/eduroam, VPN)
- Web Auftritt der Hochschule
- Identity Management
- DFN AAI
- Verzeichnisdienste (AD/LDAP)
- Backup z.B. TSM-Tivoli
- eMail Plattform
- Netzwerk-/Internetzugang LAN
- Arbeitsplatz (Office)-PCs für Mitarbeiter 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, ggf. 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. Alle Basis- und Standard-Anforderungen der Bausteine aus Kapitel 11.2 und 11.3 sind auf geeignete Weise umzusetzen. Vom IT-Grundschutz-Profil abweichende Einsatzumgebungen oder Komponenten erfordern u. U. 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, die als Grundlage für die Sicherheitskonzeption verwendet werden können.

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 in einzelnen Prozesslandkarten dargestellt sind (systemorientierte Bausteine).

Für die Umsetzung der Bausteine empfiehlt das 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 Bausteine der Prozesslandkarten (systemorientierte Bausteine) sind in der Regel alle mit "R2" vorgegeben.

Damit startet der Sicherheitsprozess mit dem Aufbau eines Information Security Management Systems ISMS, und den ersten Bausteinen aus dem Bereichen aus den Bereichen Organisation und Personal, Konzepte und Vorgehensweisen sowie Maßnahmen für den Kern-Betrieb, bevor überhaupt mit Umsetzung der Bausteine auf den Landkarten der einzelnen Geschäftsprozessen begonnen werden sollte. Die empfohlene Reihenfolge der Übergeordneten Maßnahmen ist in Kapitel 11.2 dargestellt.

11.1 „Landkarten“ der Prozesse

Die fünf wesentlichen Geschäftsprozesse und übergeordneten 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 ggf. 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 Mitarbeiter im IT Sicherheitsmanagement Prozess dienen.

Die Landkarten zu den hier behandelten Geschäftsprozessen, ebenso wie die 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	Archivierung OPS.1.2.2	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 allgemeinen Anwendungen überprüfen CON.4 Informations-sicherheit bei Auslandsreisen CON.7	Telearbeit OPS.1.2.4 Informations- und Datenträgeraustausch OPS.1.2.3 Outsourcing für Kunden OPS.2.1 Cloud Nutzung OPS.2.2 Fernwartung OPS.2.4 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.

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.4.3 Relationale Datenbanksysteme
- 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
- SYS.1.3 Server unter Unix
- SYS.1.5 Virtualisierung
- 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 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.3.4 Mobile Datenträger

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.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 drei 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.

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 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 ggf. zu erweitern.

Im Rahmen einer Feststellung des Schutzbedarfs sollte eine Datenklassifikation durchgeführt werden. Diese liefert Vorgaben vor allem unter dem Gesichtspunkt Vertraulichkeit, teilweise auch der Integrität. Gemäß der folgenden ggf. angepassten Tabellen lassen sich hier wiederum Anhaltspunkte für die Einordnung in die Schutzbedarfskategorien finden. So sind vertrauliche Daten wohl üblicherweise einer hohen Schutzbedarfskategorie bezüglich Vertraulichkeit und vielleicht Integrität zuzuordnen, aber evtl. nur einem normalen Schutzbedarf bezüglich 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 maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann
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 der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
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 des 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

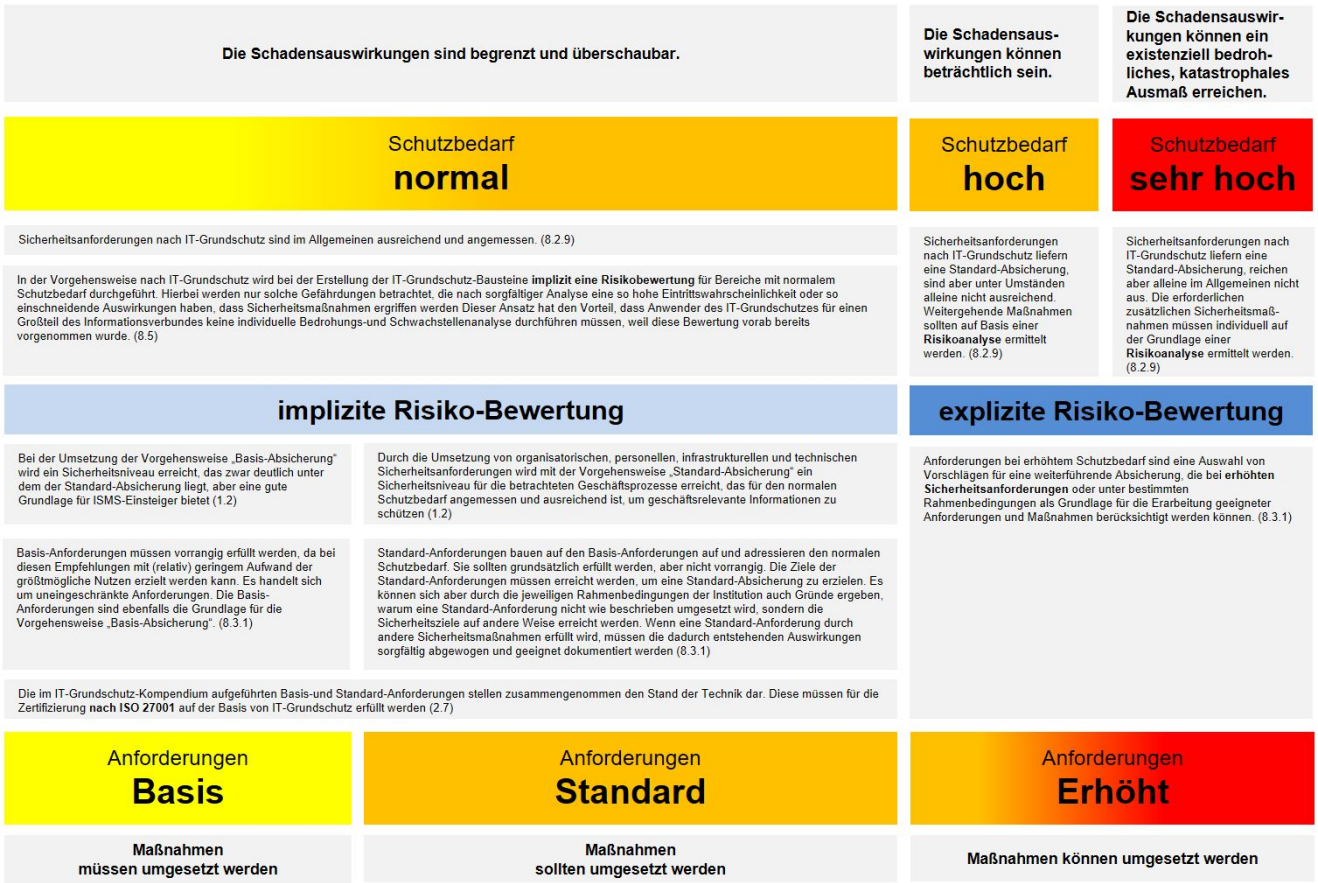
Bei den hier betrachteten Geschäftsprozessen geht dieses IT-Grundschutz-Profil für die meisten Prozesse von einem Schutzbedarf der Kategorie "normal" aus. Das erleichtert u.A. auch den Einstieg in den Informationssicherheitsprozess. In diesen Fällen wird zunächst, aber auch als absolutes Minimum, die 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-Grundschutzprofil 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 13. Hinweise zur Durchführung einer Risikoanalyse.

In einzelnen Fällen könnte nach einer Risikobetrachtung ggf. 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 Grundschutzmethode wird 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 übertragen, dass ein adäquates Sicherheitsniveau erreicht werden kann. So ist oft von Mitarbeitern die Rede, dieser Begriff ist ggf. auf andere betroffenen 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 Autoren zum hohen Schutzbedarf ist hier: Die Anforderung ORP.3.A9 ist bei hohem Schutzbedarf ebenfalls anzuwenden. Dabei ist der Begriff Mitarbeiter auch auf Studenten 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 ggf. 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) ggf. ein erhöhter Schutzbedarf angenommen wurde

In diesen Fällen muss eine Risikoabschätzung erfolgen. Auf dieser Basis festgelegt werden, 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 (inkl. verschiedener Studierendengruppen – auch z.B. Hochschulwechsler, Gasthörer, Zweithörer – Bewerbungszeiträumen, Kapazitäten, Bewerbungsvoraussetzungen, rechtlichen Rahmenbedingungen etc.), die Entgegennahme von Bewerbungen in den verschiedenen Ausprägungen sowie deren Überprüfung und ggf. Bewertung (z.B. zur Notenverbesserung durch außerschulische Leistungen).

"Zulassung" beinhaltet in zulassungsbeschränkten und (ggf.) freien Studiengängen die Zulassung (bzw. Ablehnung) von Bewerber*innen, ggf. 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
		DOSV-Portal OPS.2.2	Zentrales Storage ! System SYS.1.1 SYS.1.8	
		Uni-Assist (extern)		

Hintergrund für die Einschätzung des erhöhten Schutzbedarfs (hier für die Datenintegrität (n,h,n), gekennzeichnet durch "!" in der obigen Darstellung): Veränderungen/Manipulationen an den Bewerberdaten führen u. U. 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 werden bei den übergreifenden Prozessen (Kapitel 15.5) berücksichtigt. Sofern Server als Virtuelle Maschinen laufen ist das IT-System VMWare-Virtualisierung (mit Bausteinen SYS1.1 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 u.U. andere Anwendungen im Einsatz, beispielsweise

- HIS ...
- SAP SLCM,
- Campusnet (Datenlotsen),
- CAMPUSonline,
- PRIMUSS,
- FactScience (Medizinische Studiengänge)

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

15.2 Landkarte Immatrikulation und Studierenden-Management

"Immatrikulation" umfasst die Einschreibung zugelassener Bewerber*innen (die den Studienplatz angenommen haben) und der Bewerber*innen für zulassungsfreie Studiengänge. Er beinhaltet außerdem die Erzeugung und Bereitstellung bzw. den Versand der zugehörigen Bescheide.

"Studierenden-Management" 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 Studierenden-Management 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 Zentrales Speicher System ! SYS.1.1 SYS.1.8	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10 Serverraum ! INF.2

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 bei den übergreifenden Prozessen (Kapitel 15.5) berücksichtigt. Sofern Server als Virtuelle Maschinen laufen ist das IT-System VMWare-Virtualisierung (mit Bausteinen SYS1.1 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 u.U. andere Anwendungen im Einsatz, beispielsweise

- HIS SOS-GX/QIS,
- SAP SLCM,
- Campusnet (Datenlotsen),
- CAMPUSonline,
- PRIMUSS,
- FactScience (Medizinische Studiengänge)

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

15.3 Landkarte 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, BA-/MA-/Diplomarbeit (Abschlussprüfungen). 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 (inkl. 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 Ergebnisse sowie die IT Systeme zum Scannen von Prüfungsantwortbögen sind hier mit erfasst.

Der Prozess Prüfung 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
		ePrüfungs-System ! APP.3.1 APP.3.2 APP.4.3 • LPLUS • EvaExam	Zentrales Storage System ! SYS.1.1 SYS.1.8	Büroraum ! INF.7
			Windows 10 Client ! SYS.2.1 SYS.2.2.3	Archiv INF.6
		eLearning System ! APP.3.1 APP.3.2 APP.4.3 • Moodle • Ilias • StudIP	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, 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 SYS1.1 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 u.U. andere Anwendungen im Einsatz, beispielsweise

- HIS SOS-GX/QIS,
- SAP SLCM,
- Campusnet (Datenlotsen),
- CAMPUSonline,
- PRIMUSS,
- FactScience (Medizinische Studiengänge)

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 und 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 "!".

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Infrastruktur für Studierende	Statische Arbeitsumgebung E-Prüfungen ! E-Learning	Pool PC (Windows/Linux/MacOS) !	VMWare Virtualisierung ! SYS.1.1 SYS.1.5	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10
		Remote Unix Desktop	Windows Server 2012 SYS.1.1 SYS.1.2.2	
		Virtueller Remote Desktop, (Citrix, Horizon View, XEN-App) !	Linux Server SYS.1.1 SYS.1.3	Serverraum INF.2
		E-Learning Plattform • Moodle • Ilias • StudIP	Windows 10 Client ! SYS.2.1 SYS.2.2.3	Poolraum ! INF.10
			MacOS Client ! SYS.2.1 SYS.2.4	
			Linux Client ! SYS.2.1 SYS.2.3	

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, Änderungen nicht durchführbar sind und 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 Wiederholung der gesamten Prüfung in Frage.

15.5. Landkarte Übergreifende Prozesse

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 Darstellung als eigener übergreifender Prozess 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 Aspekte 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
		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	
			Mobile Datenträger SYS.3.4	

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