HRK-Workshop:
Informationssicherheit als strategische Aufgabe der Hochschulleitung
Berlin, 25./26.11.2019

Allianz für Cybersicherheit und IT-Grundschutz des BSI: Erarbeitung eines IT-Grundschutz-Profils für Hochschulen

Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI)
Prof. Dr. Manfred Paul (Hochschule München), **Bernhard Brandel**
(Kath. Univ. Eichstätt-Ingolstadt), **Hartmut Hotzel** (Bauhaus-Universität Weimar)

Bundesamt für Sicherheit in der Informationstechnik (BSI),
Birger Klein, **Johannes Oppelt**

Allianz für Cyber-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik

ZKI Zentren für Kommunikation und Informationsverarbeitung e.V.

Im ZKI - Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. - sind die IT-Zentren deutscher Universitäten und Fachhochschulen sowie Einrichtungen der Großforschung und der Forschungsförderung organisiert. Die Mitgliedshochschulen bilden knapp 90% der Studierenden an deutschen Hochschulen aus.

Der ZKI e.V. unterstützt seine Mitglieder durch:

- Organisation des Meinungs- und Erfahrungsaustausches
- Anregung der Kooperation zwischen den ZKI-Mitgliedseinrichtungen
- Beratung und Zusammenarbeit mit bildungs- und wissenschaftsfördernden Einrichtungen im In- und Ausland.

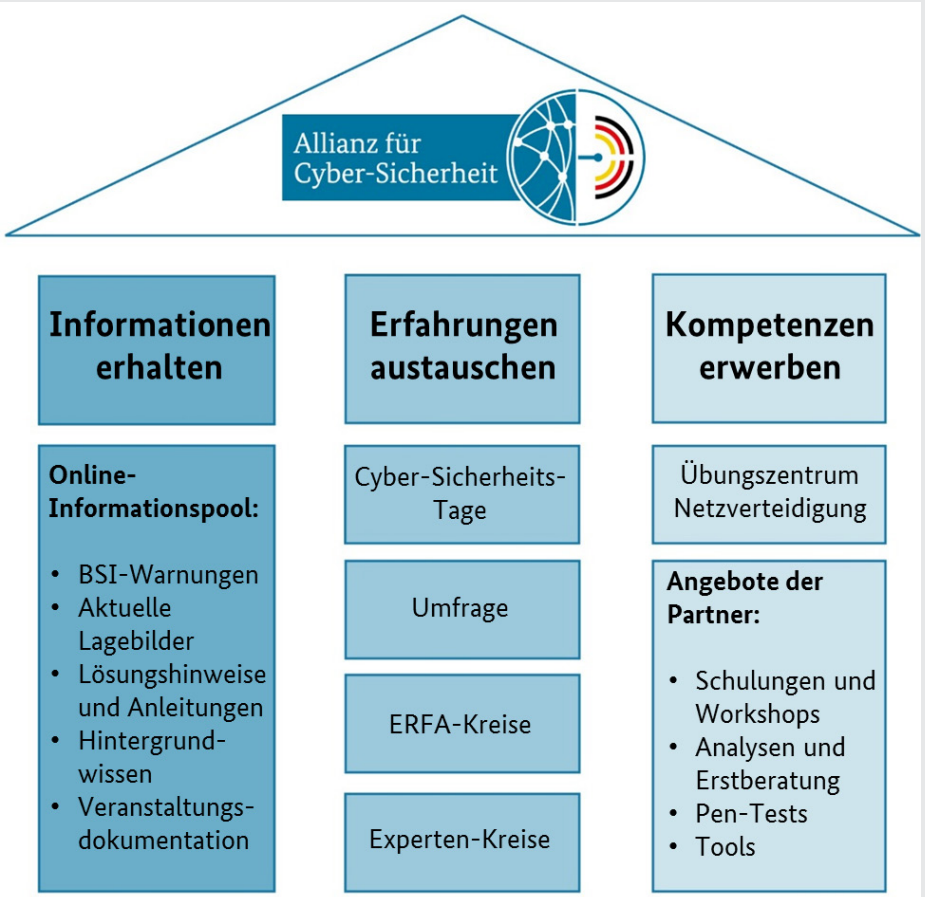
Die fachliche Arbeit erfolgt in 14 Arbeitskreisen, von Strategie und Organisation über Softwarelizenzen bis zu Informationssicherheit.

Veröffentlichungen u.a. Prozesslandkarte Campusmanagement, Leitfaden zur Ausbildung im Bereich Informationstechnologie, Handreichung zur nachhaltigen Unterstützung der Digitalisierung, Hochschulrechenzentrum 2025, alle abrufbar unter https://www.zki.de/publikationen/

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

Allianz für Cyber-Sicherheit

Zentren für Kommunikation und Informationsverarbeitung e.V.



Als Teilnehmer der Allianz für Cyber-Sicherheit profitieren Sie von…

NETZWERKE SCHÜTZEN NETZWERKE

www.allianz-fuer-cybersicherheit.de
Bundesamt für Sicherheit in der Informationstechnik

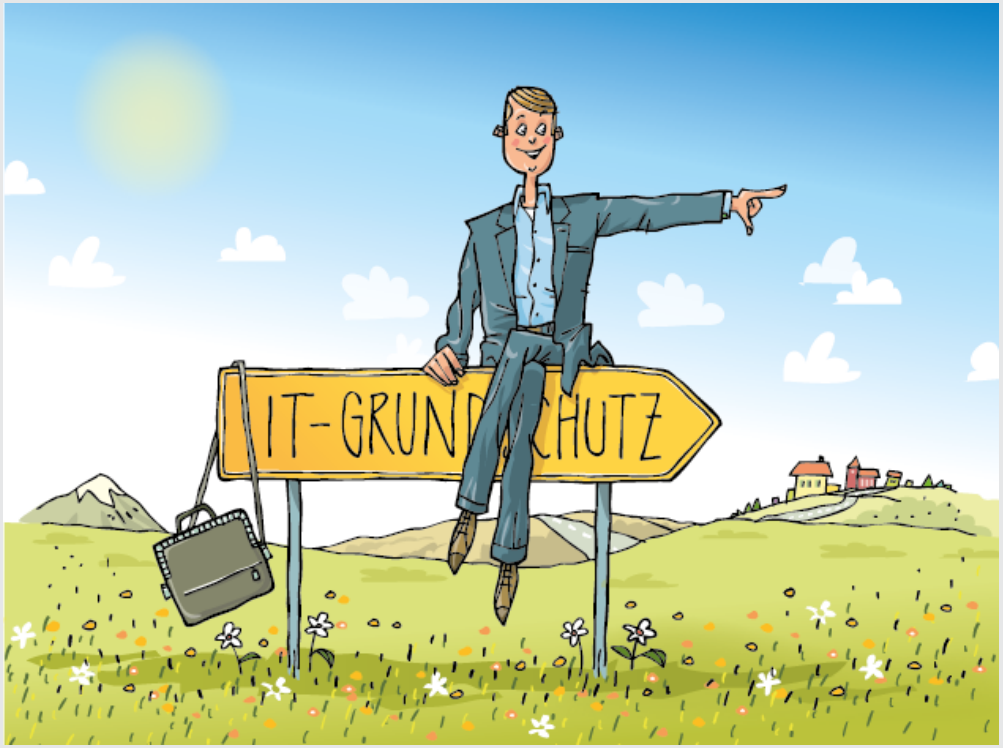
- der Expertise des BSI und der Partner der Allianz für Cyber-Sicherheit,
- dem vertrauensvollen Erfahrungsaustausch mit anderen Unternehmen und Institutionen zu Themen wie Angriffsvektoren, geeigneten Schutzmaßnahmen, Tipps zum Sicherheitsmanagement, Vorfallsbehandlung etc.
- sowie den exklusiven und für alle Teilnehmer kostenfreien Partner-Angeboten zum Ausbau Ihrer Cyber-Sicherheitskompetenz.

IT-Grundschutz

Zentren für Kommunikation und Informationsverarbeitung e.V.

Viele Wege führen zur Informationssicherheit…

…warum auf IT-Grundschutz setzen?



IT-Grundschutz

Zentren für Kommunikation und Informationsverarbeitung e.V.

Mit dem Original der Informationssicherheit in eine sichere Digitalisierung

- **Praxiserprobt**
  Im Alltag erprobte Methode für den angemessenen Schutz von Informationen.
- **Stets aktuell**
  Das IT-Grundschutz-Kompendium wird jährlich aktualisiert, dabei wird auch ein Abgleich mit anerkannten Standards durchgeführt.
- **Schlank & ausführlich**
  Flexibles und schlankes Baukastenprinzip („Bausteine“), keine Risikoanalyse bei normalen Schutzbedarf notwendig. Umsetzungshinweise erläutern im Detail geeignete Sicherheits-maßnahmen zur Umsetzung der Anforderungen aus den Bausteinen.
- **Stand der Technik**
  Seit mehr als 25 Jahren vom Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich weiterentwickelt und kostenfrei zur Verfügung gestellt.
- **Kompatibel zu ISO 27001**
  Die bewährte Standard-Absicherung des IT-Grundschutzes erfüllt die ISO 27001.
- **Nachweis der Umsetzung**
  ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz bietet die Möglichkeit zum Nachweis der erfolgreichen Umsetzung.

IT-Grundschutz

Zentren für Kommunikation und Informationsverarbeitung e.V.

IT-Grundschutz verfolgt einen **ganzheitlichen** Ansatz.

Infrastrukturelle, **organisatorische**, **personelle** und **technische** Standard-Sicherheitsanforderungen helfen, ein **Standard-Sicherheitsniveau** aufzubauen, um geschäftsrelevante Informationen zu schützen.

An vielen Stellen werden bereits höherwertige Sicherheitsanforderungen geliefert, die die Basis für sensiblere Bereiche sind.

ISO 27001 vs. IT-Grundschutz

Zentren für Kommunikation und Informationsverarbeitung e.V.

	IT-Grundschutz	ISO 27001 / ISO 27002
Umfang	875 (BS) + 779 (UH) Seiten	35 (27001) & 90 (27002) Seiten
Aktualisierung	Jährlich, unterjährig FD	bisher ca. 8 Jahre (Korrigendum möglich)
Kosten	kostenlos	ca. € 103,- DIN EN ISO/IEC 27001 ca. € 191,- DIN EN ISO/IEC 27002
Grad der Detaillierung	Konkrete Anforderungen in den Bausteinen	Generische Anforderungen
Hilfsmittel	Umsetzungshinweise als Hilfsmittel	Nicht von der ISO, diverse Anbieter
Zertifizierung	ISO 27001 auf der Basis von IT-Grundschutz	ISO 27001

ISO 27001 vs. IT-Grundschutz

Zentren für Kommunikation und Informationsverarbeitung e.V.

- → IT-Grundschutz ist **ein** Weg, die ISO 27001 zu erfüllen – mit der ISO 27001 erfülle ich aber **nicht zwangsläufig** den IT-Grundschutz!
  - → Vergleichbarkeit von ISO 27001 Implementationen bzw. ISO 27001 Zertifikaten **nicht** gegeben.
- → Die ISO 27001 ist sehr allgemein gehalten, internationale Abstimmung zeitaufwendig, größere Zyklen der Aktualisierung.
- → Die „nur“ 35 Seiten der ISO 27001 bedeuten **weniger Inhaltstiefe**:
  - → Würden Sie bei dem Maßnahmenziel **Compliance** (ISO 27001, Anhang A.18) an die **regelmäßige Wartung der Feuerlöschern** in Serverräumen denken?
- → **Baukastenprinzip** – nur die Bausteine sind anzuwenden, dessen Komponenten eingesetzt werden.
  - → Nicht von der Anzahl der Seiten oder Bausteinen „blenden“ lassen – oder würden Sie auch ein Lexikon mit nur 35 Seiten kaufen?

IT-Grundschutz-Profile

Zentren für Kommunikation und Informationsverarbeitung e.V.

Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept für ein ausgewähltes Szenario (Verbund oder Prozess), es bereitet

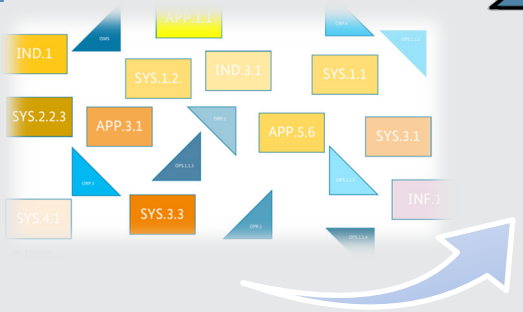
- das Ergebnis mehrerer Prozessschritte der IT-Grundschutz-Vorgehensweise

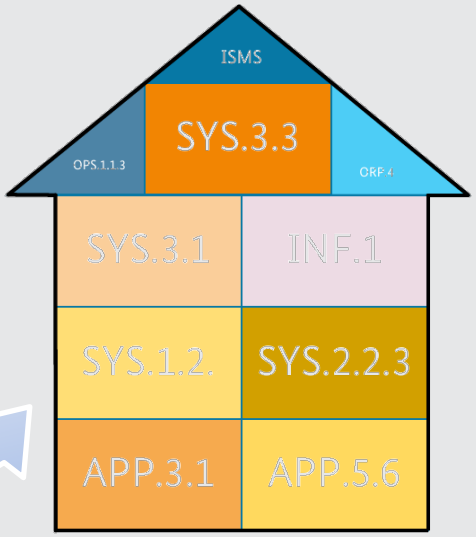
und

- einer Auswahl mehrerer Anforderungen der IT-Grundschutz-Bausteine

so auf, dass es als Schablone von ähnlichen Institutionen adaptiert werden kann!

- Vergleichbar mit einer „Dokumentenvorlage“





IT-Grundschutz-Profil für Hochschulen

Zentren für Kommunikation und Informationsverarbeitung e.V.

BSI-Grundschutztag 10.10.2018

(Jean Beaufort, publicdomainpictures.net)

Erfindung des Rades: zu oft? → Idee: IT-Grundschutz-Profil für Hochschulen
Umsetzung: in mehreren Workshops: ZKI mit dem BSI/Allianz für Cybersicherheit

ZKI Arbeitskreis Informtionssicherheit ist Mitglied in der Allianz (damit indirekt auch die ZKI Mitglieder)
Tipp: Werden Sie als Hochschule ebenfalls Mitglied/Multiplikator in der Allianz für Cybersicherheit!

Übersicht

Zentren für Kommunikation und Informationsverarbeitung e.V.

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

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 DOSV-Portal OPS.2.2 Uni-Assist (extern)	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 Storage System SYS.1.1 SYS.1.8	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10 Serverraum INF.2

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

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, • Austeben 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 ePrüfungs-System APP.3.1 APP.3.2 APP.4.3 • LPLUS • EvaExam eLearning System APP.3.1 APP.3.2 APP.4.3 • Moodle • Ilias • StudIP Papierarchiv	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 Storage System SYS.1.1 SYS.1.8 Windows 10 Client SYS.2.1 SYS.2.2.3 Drucker, Kopierer, Multifunktionsgeräte SYS.4.1	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10 Serverraum INF.2 Büroraum INF.7 Archiv INF.6

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Infrastruktur für Studierende	Statische Arbeitsumgebung E-Prüfungen E-Learning	Pool PC (Windows/Linux/MacOS) Remote Unix Desktop Virtueller Remote Desktop, (Citrix, Horizon View, XEN-App) E-Learning Plattform APP.3.2 • Moodle • Ilias • StudIP	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	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10 Serverraum INF.2 Poolraum INF.10

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) SYS.1.5 IPsec-VPN (OpenSwan/StrongSwan) SYS.1.1 SYS.1.2.2 OpenVPN (SSL-VPN) SYS.1.1 SYS.1.3 RadsecProxy, SecureW2 (eduroam) SYS.2.1 SYS.2.2.3 Virtueller Remote Desktop, (Citrix (GU), Horizon View, XEN-App) SYS.2.1 SYS.2.4 Windows 10 Arbeitsplatz SYS.1.1 Client mit Office, Browser,E-Mail APP.1.1 APP.1.2 Arbeitsplatz bereitstellen (SCCM, Zenworks, Jamf) APP.1.4 DNS APP.3.6 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	VMWare Virtualisierung SYS.1.1 Virtual Appliance 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 VPN Gateway/Firewall SYS.1.1 Desktop/Notebook SYS.2.1 SYS.3.1 Speichersystem SYS.1.1 SYS.1.8 Netze • LAN, Switches, • Router, Firewall, • VoIP NET.1.1 NET.1.2 NET.3.1 NET.3.2 NET.4.2 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	Gebäude (Hauptsitz) INF.1 INF.3 INF.4 INF.10 Serverraum INF.2 Büroraum INF.7 Home Office INF.8 Mobiler Arbeitsplatz INF.9

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.5.1 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

Übergeordnete Maßnahmen

Zentren für Kommunikation und Informationsverarbeitung e.V.

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

Vorgehen: Prozessauswahl

Auswahl von 5 Prozessen:

- vorhandene Prozesslandkarte Campus-Management (ZKI):
  → 1. Bewerbung und Zulassung
  → 2. Immatrikulation und Studierenden-Management
  → 3. Prüfung
  (Abdeckung: inhaltlich ca. 50% der Prozesslandkarte!)

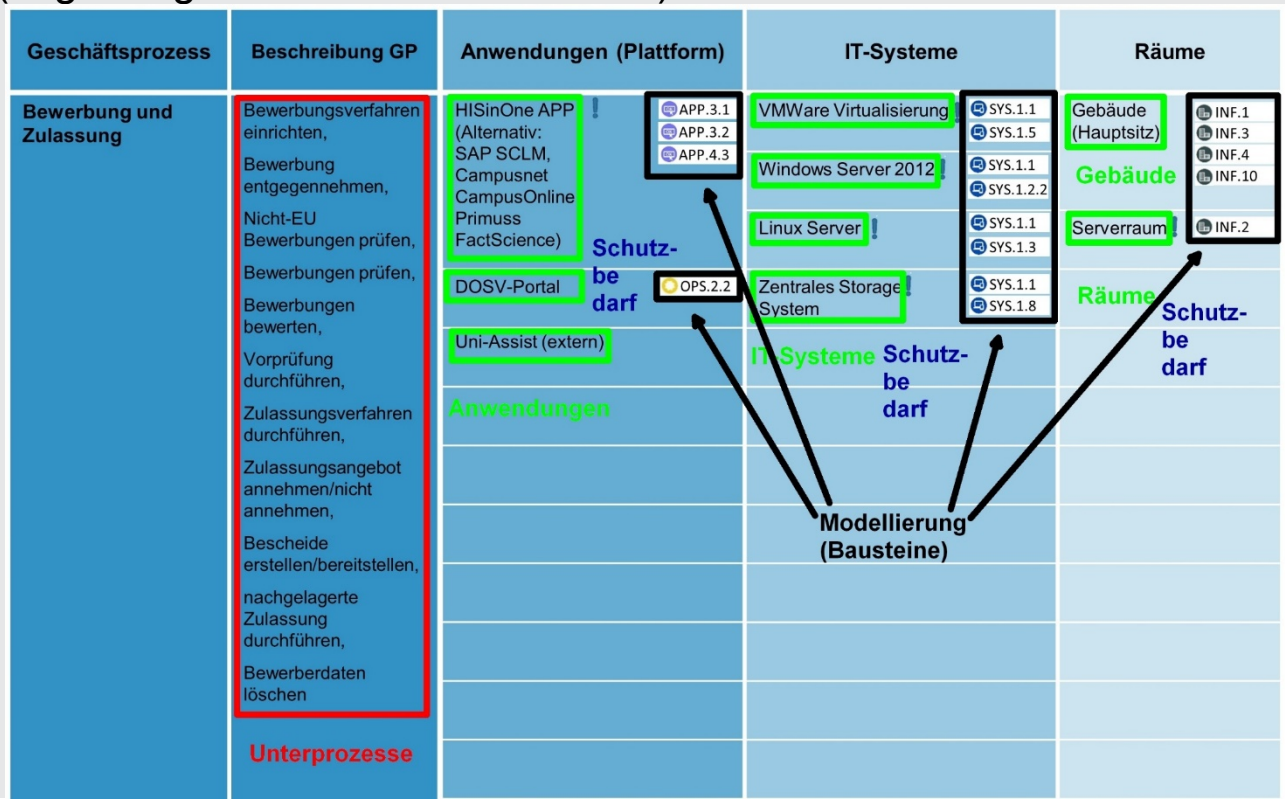
- ein weiterer Prozess:
  → 4. IT-Infrastruktur für Studierende

- übergreifende Anwendungen als weiterer „Prozess“ (oben benötigt)
  → 5. Übergreifende Prozesse
  (z.B. zentrale Dienste, Netzinfrastruktur)

Prozess Bewerbung und Zulassung

Zentren für Kommunikation und Informationsverarbeitung e.V.

- **Unterprozesse** sowie zugehörige **Anwendungen** bestimmen, dann **IT-Systeme**, **Räume**, **Gebäude**
- **Schutzbedarf** festlegen (! = hoch in Vertraulichkeit, Integrität oder Verfügbarkeit), „nichts“ = normal
- **Modellierung** (zugehörige **Bausteine** bestimmen)



Stand Grundschutzprofil für Hochschulen

Zentren für Kommunikation und Informationsverarbeitung e.V.

Insgesamt werden 78 Bausteine aus Hochschulsicht kommentiert

- **Umsetzungshinweise für vom BSI empfohlene Maßnahmen**
- **31** übergeordnete Bausteine (**prozessorientierte Bausteine**)
  - Als Übersicht dem gesamten Informationsverbund zugeordnet
- **47 systemorientierte Bausteine**,
  - in Landkarten, Zielobjekten zugeordnet

Stand heute:

- Version 0.9 (Draft) des IT-Grundschutzprofils für Hochschulen ist zum Download verfügbar
  www.zki.de/publikationen
- hochschulspezifische Umsetzungshinweise zu den 78 Bausteinen werden gerade erstellt bzw. kommentiert (Weitere Unterstützer gesucht!)
- Umsetzungsempfehlungen für die ersten Bausteine sind ab sofort über den ZKI Arbeitskreis Informationssicherheit verfügbar

Beispiel: Stand Baustein ORP.3

Zentren für Kommunikation und Informationsverarbeitung e.V.

(a) ORP.3: Sensibilisierung und Schulung

Erstellt von Bernhard Brandel, zuletzt geändert von Julia Synnatzschke am 26. Sep. 2019

ORP.3: Sensibilisierung und Schulung

Anforderungen	**ORP.3.A1-A3 sowie A4 - A8** Die Anforderungen A1 - A8 sind anzuwenden. **ORP.3.A9** Die Anforderung A9 ist bei hohem Schutzbedarf ebenfalls anzuwenden.
Ausnahmen	keine
Priorisierung	**R1 (und innerhalb der R1- Prozesse zeitgleich zu ISMS.1 beginnen)** Sensibilisierung betrifft alle Zielgruppen einer Hochschule, beginnend mit der Hochschulleitung, die die Gesamtverantwortung für den Informationssicherheitsprozess trägt und die Rahmenbedingungen für Informationssicherheit (s. (a) ISMS.1 Sicherheitsmanagement, Leitlinie) setzt und mit gutem Beispiel vorangehen muss. Gleichzeitig betrifft Sensibilisierung auch die Professorenschaft und das mittlere Management sowie die wissenschaftlichen Beschäftigten, Verwaltungsmitarbeiter, das IT-Personal und die Studierenden. Die Realisation von ORP.3 sollte zeitgleich mit ISMS.1 beginnen, was die Umsetzung beider Bausteine beschleunigt. Sinnvoll ist es, auch die Standardanforderungen A5 - A8 möglichst von Beginn an umzusetzen.
Allgemeine Empfehlungen zum Baustein	Begrifflichkeiten: "Institution" ist die entsprechende Hochschule (Fachhochschule oder Universität) Hochschulen haben als Zielgruppe nicht nur "Mitarbeiter". Genauso müssen die "Studierenden" und fallweise weitere Nutzergruppen in die Sensibilisierungs- und Schulungsmaßnahmen mit einbezogen werden. In Baustein und Umsetzungshinweisen sind daher i.d.R. unter "Mitarbeitern" "Mitarbeiterinnen und Mitarbeiter, Lehrbeauftragte sowie Studierende" zu verstehen. An dualen Hochschulen ist der Begriff noch weiter zu fassen (siehe auch (a) ORP.4 Identitäts- und Berechtigungsmanagement)

Beispiel: Stand Baustein ORP.3 (Seite 2)

Zentren für Kommunikation und Informationsverarbeitung e.V.

Empfehlungen zur Umsetzung der Anforderung **siehe** https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/ORP/Umsetzungshinweise_zum_Baustein_ORP_3_Sensibilisierung_und_Schulung.html	Die Sensibilisierungsmaßnahmen müssen auf die Bedürfnisse der Zielgruppen zugeschnitten werden. Der Unterarbeitskreis Awareness des ZKI sammelt und entwickelt Beispiele für Schulungsmaterialien und Sensibilisierungsmaßnahmen, die bei Bedarf genutzt und gerne ergänzt werden können. **ORP.3.A1** Leitungspersonen benötigen kurze, nicht technik-lastige Informationen über Risiken, Folgen und Lösungsmöglichkeiten, wie sie ihrer Gesamtverantwortung für die Informationssicherheit am besten nachkommen können.
	ORP.3.A2 Es empfiehlt sich, in allen Organisationseinheiten (Fakultäten, zentralen Einrichtungen etc.), Multiplikatoren zu benennen und zu befähigen (festzulegen in ISMS.1, Leitlinie). Bereits existierende Organisationsstrukturen/Kanäle sollten dafür genutzt werden (z.B. Administratorentreffen).
	ORP.3.A3 Wichtig ist die Kontinuität der Maßnahmen. Neue Beschäftigte, Wiedereinsteigende und Studierende sollten gleich zu Beginn sensibilisiert werden.
	ORP.3.A7 Den Sicherheitsverantwortlichen müssen die notwendigen Ressourcen (Zeit, Geld, Personal, Schulungen) zur Verfügung gestellt werden (siehe ISMS.1).
	ORP.3.A6 und ORP.3.A8 Sensibilisierung "im laufenden Geschäftsbetrieb" ist besonders wirkungsvoll. Deshalb ist der Einsatz geeigneter Software, die Angriffssimulationen wie Spear-Phishing-Kampagnen samt Messung und anonymisierter Auswertung des Lernerfolgs ermöglicht, sehr zu empfehlen. Vor der Durchführung ist es notwendig, die Kampagnen mit den Personalräten/MitarbeiterInnenvertretungen abzustimmen.

Weiteres Vorgehen

Zentren für Kommunikation und Informationsverarbeitung e.V.

Nächstes Ziel:

- Verabschiedung des IT-Grundschutz-Profils 1.0 im März 2020 geplant (ZKI-Tagung in Leipzig)
- Fertigstellung der Arbeiten an den 78 Bausteinen

Was kommt danach?

- Der ZKI Arbeitskreis Informationssicherheit wird das Grundschutzprofil für Hochschulen weiterentwickeln (BSI sagt Unterstützung bei der weiteren Entwicklung zu)
  - weitere Prozesse aus Forschung und Verwaltung
  - Laufende Updates
- Bitte um Input an den ZKI Arbeitskreis Informationssicherheit über Modellierung eigener Prozesse

Projekterfahrungen/Umsetzungstipps

Zentren für Kommunikation und Informationsverarbeitung e.V.

Das IT-Grundschutzprofil für Hochschulen ist unser gemeinsames Kind
Aber: Informationssicherheit ist ein Prozess und kein einmaliges Projekt!

- die deutschlandweite Zusammenarbeit untereinander (Hochschulen) macht Spaß
- genauso wie die Zusammenarbeit mit dem BSI
- beides schafft Vertrauen und bringt Know-How über Informationssicherheit
- Wir brauchen tatkräftige Unterstützung

Strahlwirkung nicht unterschätzen:

- 5 Prozesse klingen nach wenig, aber mit ihrer Umsetzung (Bausteine) werden viele andere Prozesse miterledigt!

Tipps zur Umsetzung des Profils an Ihrer Hochschule:

- Mit Prozessbausteinen beginnen (v.a: ISMS und Sensibilisierung!)
- Mit Basis-Absicherung beginnen
- Perspektivisch: Standard-Absicherung anstreben

ISO27001 und BSI Grundschutz- kein Widerspruch!

Zentren für Kommunikation und Informationsverarbeitung e.V.

- **IT-Grundschutz und ISO27001 widersprechen sich nicht.**
- **Man ist nicht endgültig festgelegt: Man kann risikolos mit IT-Grundschutz beginnen und ohne großen Zeitverlust auf ISO27001 schwenken.**
- **Schutzbedarfsanalyse nach Grundschutz ist auch schon eine grobe, schnelle Risikoanalyse**
- **2. Beispiel: zuerst Grundschutz und dann für Forschungsbereich ISO-Zertifizierung**