Zentren für Kommunikation und Informationsverarbeitung e.V.

Allianz für Cyber-Sicherheit

Erfahrungen, Learnings, Tipps für weitere Profil-Ersteller

IT-Grundschutz-Profil für Hochschulen
Stand 09.10.2019

Katholische Universität Eichstätt-Ingolstadt

Bernhard Brandel
AK Informationssicherheit des ZKI

Erstellungsprozess
IT- Grundschutz-Profil für Hochschulen

Allianz für Cyber-Sicherheit

Vorgeschichte: BSI-Grundschutztag 10.10.2018

(Jean Beaufort, publicdomainpictures.net)

Erfindung des Rades: zu oft?

Idee: IT-Grundschutz-Profil für Hochschulen

Umsetzung: in mehreren Workshops mit dem BSI/Allianz für Cybersicherheit:

ZKI: Verein der „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“
https://www.zki.de

1. Tipp: BSI/Allianz für Cybersicherheit ansprechen! Mitglied/Multiplikator werden!

Zentren für Kommunikation und Informationsverarbeitung e.V.

Erstellungsprozess IT-Grundschutz-Profil für Hochschulen

1. **Kick-Off-Workshop (im Rahmen der ZKI-Tagung im März 2019 in Erfurt)**

Zielgruppe: Leitungsebene (IT-Leiter + Spezialisten aus IT bzw. IT-Sicherheit)
Input: IT-Grundschutz (Methode, Vorteile, Bausteine) ,IT-Grundschutz-Profile

Themen des 1. Workshops

- ✓ Definition relevanter Geschäftsprozesse von Hochschulen
- ✓ Ableitung Geltungsbereich und Informationsverbund
- ✓ Beginn Erstellung Referenzarchitektur (Prozesse und Teilprozesse)

2. Tipp: geeignete Kollaborationsplattform und –methoden für Arbeiten außerhalb der Workshops nutzen
z.B.: Confluence-Umgebung (Wiki),
kurzfristige Videokonferenzen (DFN)

3. Tipp: Komplexität klein halten:
- nur wenige Prozesse modellieren!
- Vorhandenes (Vorarbeiten, Know-how, …) verwenden!

Erstellungsprozess IT-Grundschutz-Profil für Hochschulen

KickOff-Workshop konkret:

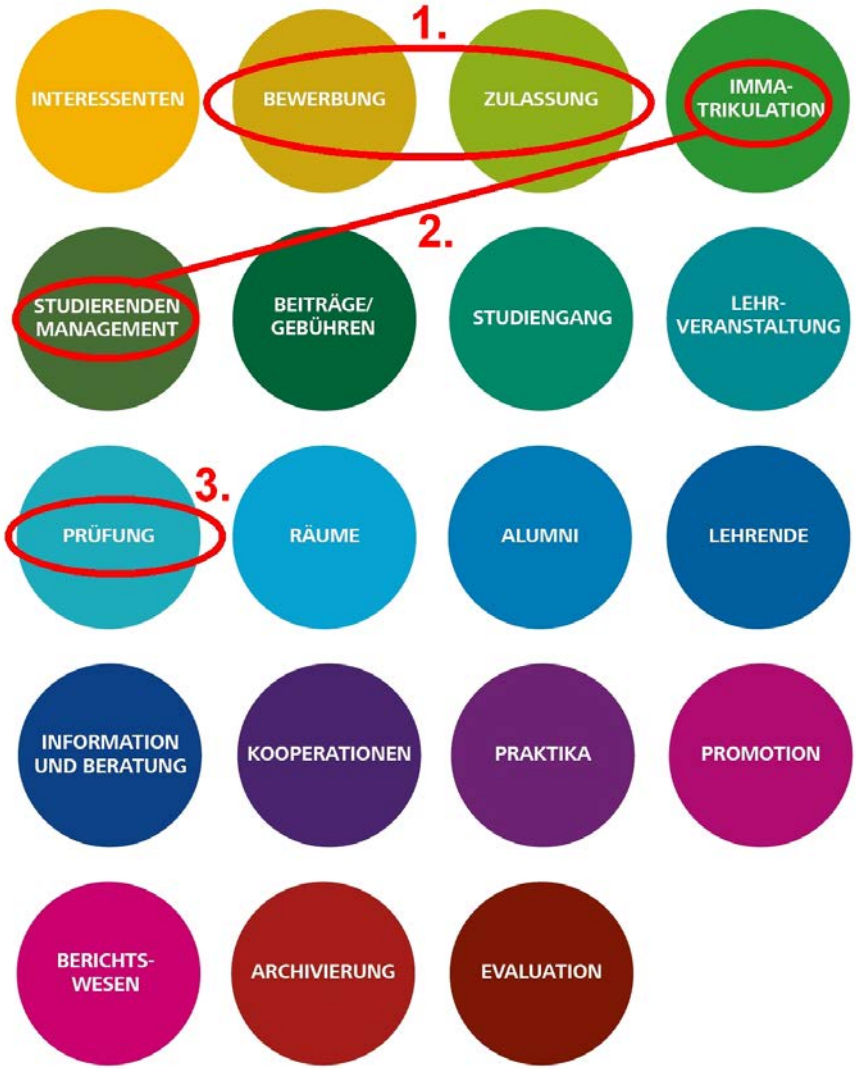
Auswahl von 4 (5) Prozessen:

- drei aus vorhandener Prozesslandkarte Campus-Management (ZKI):
  → 1. Bewerbung und Zulassung
  → 2. Studierenden-Management
  → 3. Prüfung

(Abdeckung: ca. 50% der Prozesslandkarte!)

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

- ★ 4. Tipp:
  Übergreifende Anwendungen als weiteren Prozess „vor die Klammer ziehen!“
  → 5. Übergreifende Prozesse
  (z.B. zentrale Dienste, Netzinfrastruktur)



Erstellungsprozess
IT-Grundschutz-Profil für Hochschulen

IT-Grundschutz-Profil – Prozess

Allianz für Cyber-Sicherheit

Workshop 2

Zielgruppe
Beschäftigte aus dem Bereich IT bzw. IT-Sicherheit

Input
Schutzbedarfsfestellung
Hinweise zur Risikoanalyse

Arbeitsergebnisse
- ✓ Finalisierung Referenzarchitektur
- ✓ Erstellung einer „Landkarte“
- ✓ Auswahl relevanter IT-Grundschutz-Bausteine
- ✓ Vereinbarungen zur weiteren Vorgehensweise

Bundesamt für Sicherheit in der Informationstechnik

Fand im Rahmen einer gemeinsamen AK Sitzung Netzdienste und Informationssicherheit im Mai 2019 in Magdeburg statt

Erstellungsprozess IT-Grundschutz-Profil für Hochschulen

Workshop 2: konkrete Arbeiten/Ergebnisse:

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 BewerberInnen, 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

Workshop 2 b)

Unterprozesse	Anwendungen	Workshop 2 a)	Schutzbedarf (CIA)	IT-Systeme	2 a)	Räume	2 a)	Gebäude	2 a)
Bewerbungsverfahren einrichten Bewerbung entgegennehmen	APP.3.1 APP.3.2 APP.4.3	Campus Management System (z.B. HISinOne APP (Webserver, Datenbank, Applikationsserver)	nhn	SYS.1.1 SYS.1.2.3	Windows Server 2016	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
				SYS.1.1 SYS.1.3	Linux Server	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
				SYS.1.1 SYS.1.8	Zentrales Storage-System	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
		DOSV-Portal	nnn		(Cloud-Dienst)		-	-	-
Nicht-EU Bewerbungen prüfen		Uni-Assist (extern)	nnn		(Cloud-Dienst)		-	-	-
Bewerbungen prüfen Bewerbungen bewerten Vorprüfung durchführen Zulassungsverfahren durchführen Zulassungsangebot annehmen/nicht annehmen	APP.3.1 APP.3.2 APP.4.3	Campus Management System (z.B. HISinOne APP (Webserver, Datenbank, Applikationsserver)	nhn	SYS.1.1 SYS.1.2.3	Windows Server 2016	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
				SYS.1.1 SYS.1.3	Linux Server	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
				SYS.1.1 SYS.1.8	Zentrales Storage-System	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
Bescheide erstellen/bereitstellen		DOSV-Portal	nnn		(Cloud-Dienst)		-	-	-
nachgelagerte Zulassung durchführen Bewerberdaten löschen	APP.3.1 APP.3.2 APP.4.3	HISinOne APP (Webserver, Datenbank, Applikationsserver)	nhn	SYS.1.1 SYS.1.2.3	Windows Server 2016	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
				SYS.1.1 SYS.1.3	Linux Server	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)
				SYS.1.1 SYS.1.8	Zentrales Storage-System	INF.2	Serverraum	INF.1, INF.3 INF.4 INF.10	Hauptsitz (Musterstraße)

Kick-Off-Workshop

BSI: Modellierung 2c)

Erstellungsprozess IT-Grundschutz-Profil für Hochschulen

Workshop 2: durchgeführte Arbeiten:

- Für jeden der 5 Prozesse und deren Teilprozesse
  - Anwendungen, IT-Systeme, Räume und Gebäude identifizieren
    - 5. Tipp: auf verbreitete, „besonders beliebte“ Anwendungen beschränken!
      Z.B.: HISinOne-Produkte als Campus-Management-Systeme
  - Schutzbedarfsaspekte „C,I,A“ bewerten (gering, normal, hoch, sehr hoch)

- **Im Nachgang: Modellierung durch BSI :**
  - Bausteine + resultierenden Schutzbedarf bestimmen (Danke, Herr Klein!)

- **Hausaufgaben bis Workshop 3:**
  - 75 Bausteine sind insgesamt aus Hochschulsicht zu kommentieren
    - 36 übergeordnete Bausteine (nicht in Landkarte, da dem gesamten Informationsverbund zugeordnet)
    - 39 Bausteine, in Landkarten, Zielobjekten zugeordnet
    - -> Bausteinpaten gesucht und gefunden
  - Rahmendokument „IT-Grundschutz-Profil für Hochschulen“ vorbereiten

Erstellungsprozess
IT-Grundschutz-Profil für Hochschulen

IT-Grundschutz-Profil – Prozess

Workshop 3

Zielgruppe:
Beschäftigte aus dem Bereich IT bzw. IT-Sicherheit

Input (bei Bedarf):
Umsetzungshinweise inkl. Dokumentation

Arbeitsergebnisse (geplant):
- ✓ Textabstimmung „Strukturbeschreibung“
- ✓ Vereinbarung zur Veröffentlichung
- ✓ ggf. Vereinbarungen zum weiteren Vorgehen (Folgetreffen, Revision, Erfahrungsaustausch etc.)

Teilweise erledigt
Aktueller Stand: AK-SEC Arbeitsumgebung

Bernhard Brandel, Kath. Univ. Eichstätt-Ingolstadt

Stand und Planung

- IT-Grundschutz-Profil „Lite“
  - Vorstellung beim Workshop Informationssicherheit der Hochschulrektorenkonferenz am 25./26.112019 in Berlin,
  - Veröffentlichung als Draft
- Verabschiedung des IT-Grundschutz-Profils 1.0 im März 2020 geplant (ZKI-Tagung in Leipzig)
- Umsetzungshinweise zu den ca. 75 Bausteinen werden gerade erstellt bzw. schon kommentiert
- BSI sagt Unterstützung bei der weiteren Entwicklung zu (evtl. weitere Prozesse aus Forschung und Verwaltung)

Beispiel: Stand Baustein ORP.3

(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)

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.

Allgemeine Erfahrungen und Tipps

- Prozess sachte, aber stetig steuern und betreuen!
  - Teamwork zwischen den Workshops am Leben halten
  - alle machen freiwillig mit, haben aber wenig Zeit

- Es lohnt sich!
  - Zusammenarbeit mit dem BSI macht Spass
  - genauso wie die deutschlandweite Zusammenarbeit untereinander (Hochschulen) -
  - beides schafft Vertrauen und
  - bringt Know-How über Informationssicherheit

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

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

- **Erstellen Sie zusammen Ihr eigenes IT-Grundschutz-Profil für Ihre Branche! Es lohnt sich!**

Kontakt/Anregungen/Rückfragen

Allianz für Cyber-Sicherheit

- ZKI-Arbeitskreis IT-Sicherheit
  https://www.zki.de/top-themen/it-sicherheit/

- Bernhard Brandel
  Katholische Universität Eichstätt-Ingolstadt
  E-Mail: bernhard.brandel@ku.de
  Telefon: 0841/937-21888
  https://www.ku.de/rechenzentrum/team/brandel/

- Prof. Dr. Manfred Paul
  Hochschule München
  E-Mail: manfred.paul@hm.edu