



DHKT
DEUTSCHER
HANDWERKSKAMMERTAG

IT-Grundschutz-Profil für Handwerkskammern

Berlin, 11. Juli 2018

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	16.04.2018	BSI	Anlegen des Templates
1.0	12.05.2018	Team Dokumentation	Ausfüllen der Punkte 1 bis 5
1.0	11.07.2018	Team Dokumentation	Finalisieren des Dokuments

Inhalt

1	Einleitung	3
2	Formale Aspekte	4
3	Management Summary	4
4	Festlegung des Geltungsbereichs (Scope)	5
5	Abgrenzung des Informationsverbunds	5
6	Referenzarchitektur	6
7	Zu erfüllende Anforderungen und umzusetzende Maßnahmen	8
	ISMS.1: Sicherheitsmanagement	8
	ORP: Organisation und Personal	9
	OPS: Betrieb	9
	CON: Konzeption und Vorgehensweisen	9
	DER: Detektion und Reaktion	9
	APP: Anwendungen	10
	SYS: IT-Systeme	10
	IND: Industrielle IT	10
	NET: Netze und Kommunikation	11
	INF: Infrastruktur	11
8	Restrisikobetrachtung / Risikobehandlung	11
9	Anwendungshinweise	12
	I. Hinweise zur Schutzbedarfsfeststellung	12
	II. Hinweise zur Durchführung einer Risikoanalyse	15

1 Einleitung

Handwerkskammern erfüllen als Körperschaften des öffentlichen Rechts hoheitliche Aufgaben wie beispielsweise das Führen der Lehrlings- und Handwerksrolle, in der sämtliche Mitgliedsbetriebe erfasst werden; sie regeln die Berufsausbildung und sind in ihrem Kammerbezirk für das fachliche Prüfungswesen verantwortlich. Als Selbstverwaltungseinrichtungen der Wirtschaft fördern sie Betriebe und repräsentieren die Interessen des Handwerks gegenüber Politik und Verwaltung.

Ihren Mitgliedern bieten die Handwerkskammern ein breites Spektrum von Dienstleistungen an. Im Sinne eines modernen Dienstleisters nutzen die Kammern dabei auch intensiv die Potenziale der Digitalisierung, um Geschäftsprozesse zunehmend elektronisch anzubieten.

Unternehmen und Handwerkskammern sehen sich heute vielfältigen Risiken durch Cyber-Bedrohungen ausgesetzt. Diese können erhebliche wirtschaftliche oder auch rechtliche Konsequenzen nach sich ziehen. Um die entsprechenden Risiken zu minimieren ist die Erstellung und Umsetzung eines individuellen Sicherheitskonzepts für die jeweilige Institution besonders wichtig.

Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik ist eine seit Jahren bewährte Methodik, um das Niveau der Informationssicherheit in Institutionen jeder Größenordnung zu erhöhen. Im Rahmen der im Oktober 2017 vereinbarten Kooperation des Zentralverbands des Deutschen Handwerks (ZDH) mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde gemeinsam der Prozess zur „Erstellung eines IT-Grundschutz-Profiles für Handwerkskammern“ initiiert. Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept, das als Schablone für Institutionen mit vergleichbaren Rahmenbedingungen dient. Die Schritte des IT-Grundschutzes können vorab festgelegt werden, so dass es allen interessierten Handwerkskammern möglich ist, mit Hilfe der Strukturbeschreibung die Informationssicherheit zu erhöhen. Das spart viel Zeit und Arbeit.

Am 27. März 2018 trafen sich im Meistersaal des ZDH in Berlin rund 50 Vertreterinnen und Vertreter aus Handwerkskammern und anderen handwerksnahen Organisationen zu einem Kick-Off-Workshop. Die Veranstaltung bot den Teilnehmerinnen und Teilnehmern Gelegenheit, die Systematik des IT-Grundschutzes sowie der Bausteine des IT-Grundschutz-Kompodiums kennenzulernen und sich intensiv über Anforderungen sowie Umsetzungsschritte für mehr IT-Sicherheit in ihren Institutionen auszutauschen. Gemeinsam konnten für Handwerkskammern typische Geschäftsprozesse am Beispiel „Der (digitale) Weg zum Meister“ identifiziert und damit das weitere Vorgehen zur Erstellung des "IT-Grundschutz-Profiles für Handwerkskammern" festgelegt werden. Im Mai und Juni 2018 folgten zwei weitere Workshops, in denen die Inhalte des vorliegenden Dokuments erarbeitet wurden.

2 Formale Aspekte

Titel (Kurztitel):	IT-Grundschutz-Profil für Handwerkskammern
Autorenschaft:	Handwerkskammern in Kooperation mit dem Deutschen Handwerkskammertag (DHKT)
Herausgeberschaft:	Deutscher Handwerkskammertag (DHKT)
Registrierungsnummer:	HWK/2018/1.0
Versionsstand:	Veröffentlicht am 11.07.2018, Version 1.0, erstellt am 12.05.2018
Revisionszyklus:	Die Aktualität des Dokuments soll alle zwei Jahre überprüft werden.
Vertraulichkeit:	Das Dokument in der hier vorliegenden Version ist offen zugänglich. Darüber hinaus wird es eine als vertraulich eingestufte Version geben, die nur Anwenderinnen und Anwendern aus Handwerkskammern zugänglich ist. Es ist vorgesehen, dass die Einstufung nach TLP (Traffic Light Protocol) „amber“ erfolgt.

3 Management Summary

Zielgruppe:	Dieses IT-Grundschutz-Profil richtet sich an Handwerkskammern.
Zielsetzung:	Das IT-Grundschutz-Profil für Handwerkskammern definiert in der Basisversion einen Mindest-Schutzbedarf für den Prozess „Der (digitale) Weg zum Meister“. Neben den anzuwendenden Bausteinen gemäß der IT-Grundschutz-Vorgehensweise „Standardsicherung“ umfasst das Profil in der Basisversion zusätzlich Hinweise zu Schutzbedarfsfeststellung und Risikoanalyse.
Aufgaben der Leitungsebene:	Die Autorinnen und Autoren des vorliegenden Dokuments empfehlen den Handwerkskammern die Anwendung dieses Profils als Grundlage für die Sicherheitskonzeption. Das IT-Grundschutz-Profil bezog sich in der Erarbeitung zunächst auf Geschäftsprozesse im Zusammenhang mit dem Gesamt-Prozess „Der (digitale) Weg zum Meister“ und nicht auf die Gesamtorganisation der Handwerkskammer. Im Erstellungsprozess wurde deutlich, dass Bestandteile des Profils auch auf die Gesamtorganisation übertragbar sind. Im Bedarfsfall sind hierfür jedoch zusätzliche Schutzmaßnahmen auszuwählen.

4 Festlegung des Geltungsbereichs (Scope)

Zielgruppe:	Dieses IT-Grundschutz-Profil richtet sich an Handwerkskammern.
Schutzbedarf:	Hinsichtlich des Schutzniveaus definiert das vorliegende Profil ein Niveau, das der Standard-Absicherung der IT-Grundschutz-Vorgehensweise entspricht. Gegebenenfalls wird auf Grundlage der noch im Detail durchzuführenden Schutzbedarfsfeststellung abweichend davon in Teilen ein erhöhter Schutzbedarf festgestellt. Informationen dazu werden den Anwenderinnen und Anwendern im vertraulichen Dokument zur Verfügung gestellt. In jedem Fall ist die Schutzbedarfsfeststellung bei der Anwendung des IT-Grundschutz-Profiles zu berücksichtigen.
IT-Grundschutz-Vorgehensweise:	Die in diesem Profil aufgeführten Anforderungen sind Empfehlungen für Handwerkskammern. Sie decken mindestens die Anforderungen der „Standard-Absicherung“ des BSI-Standards 200-2 ab, ggf. müssen außerdem Anforderungen aus dem Bereich des hohen Schutzbedarfs umgesetzt werden.
ISO 27001-Kompatibilität:	Wird mindestens die IT-Grundschutz-Vorgehensweise „Standard-Absicherung“ umgesetzt, ist diese zu der ISO 27001 kompatibel. Bei einem geringeren Erfüllungsgrad der Anforderungen gegenüber der „Standard-Absicherung“ ist durch den Ersteller des IT-Grundschutz-Profiles die Kompatibilität zu prüfen, wenn diese notwendig ist.
Rahmenbedingungen:	-

5 Abgrenzung des Informationsverbunds

Bestandteile des Informationsverbundes:	<p>Als Grundlage für die Identifizierung relevanter Geschäftsprozesse wurde beispielhaft der Prozess „Der (digitale) Weg zum Meister“ herangezogen. Daraus ergibt sich der nun gewählte Informationsverbund, zu dem alle Prozesse und Verfahren in der Handwerkskammer gehören, die für die Abwicklung der identifizierten Prozesse notwendig sind. Auf technischer Ebene sind hierfür in der Regel der Web-Auftritt, die Datenbanken, E-Mail- und sonstige Kommunikationsserver und die entsprechende Netzinfrastruktur einzubeziehen sowie weitere IT-Systeme, die für den Gesamt-Prozess wesentlich sind.</p> <p>Handwerkskammern, die Teile ihrer technischen Infrastruktur durch Dritte betreiben lassen (möchten), sollten das vorliegende Profil als Grundlage für die Zusammenarbeit mit entsprechenden Dienstleistern verwenden. Die hier formulierten Anforderungen sollten in den Vertragsbedingungen enthalten sein.</p>
Nicht berücksichtigte Objekte:	Das Profil betrachtet in der offenen Version in erster Linie die hoheitlichen Aufgaben des „digitalen“ Wegs zum Meister mit den Prozessen: Zulassung, Anmeldung, Prüfung.

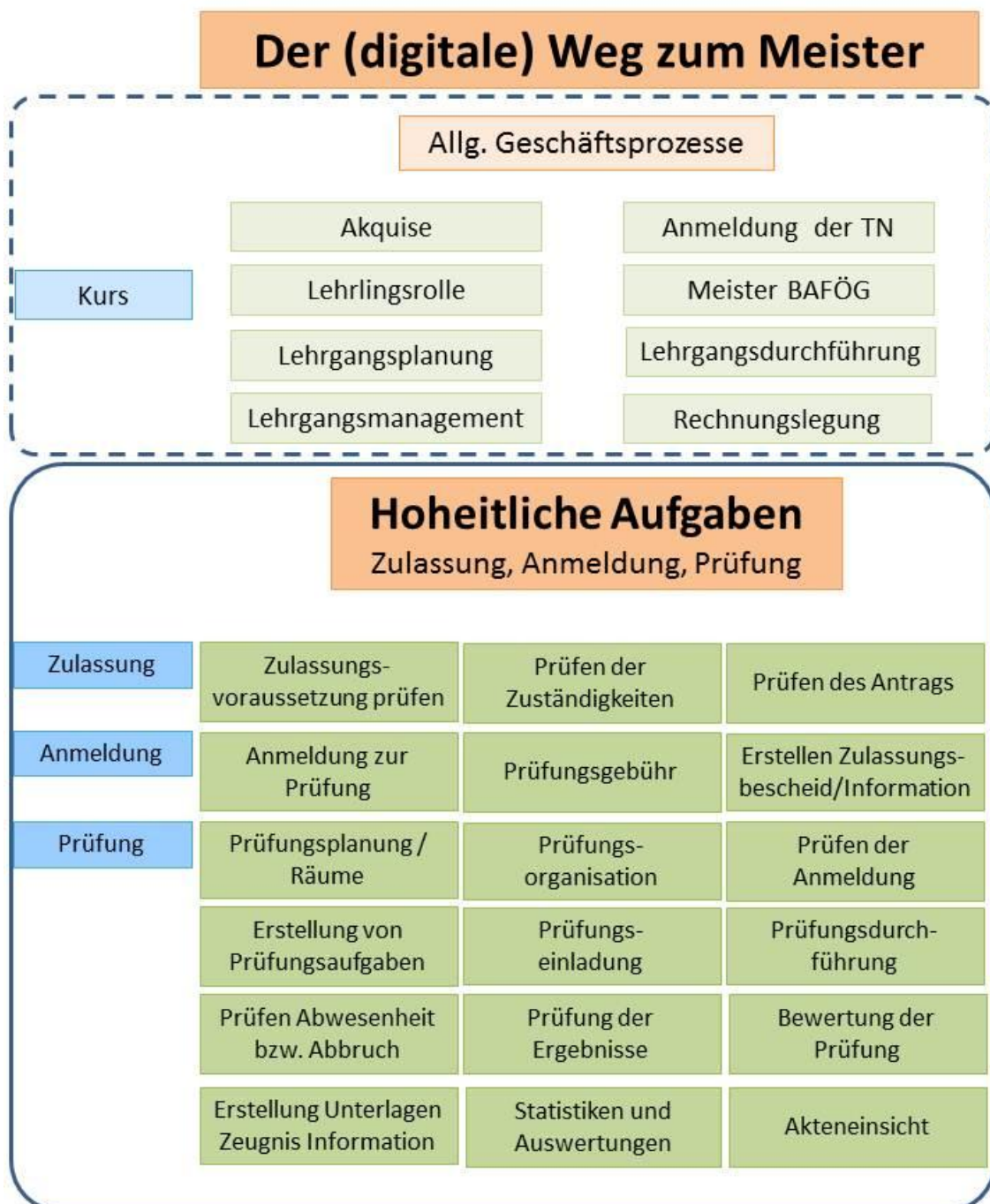
6 Referenzarchitektur

Die Referenzarchitektur (im IT-Grundschutz-Profil auch Untersuchungsgegenstand genannt) legt fest, auf welche Objekte die Anforderungen des IT-Grundschutzes im Kontext des IT-Grundschutz-Profiles angewendet werden müssen.

Hierzu zählen im Einzelnen

- Geschäftsprozesse,
- räumliche Gegebenheiten/Infrastruktur (Liegenschaften, Gebäude, Räume),
- eingesetzte Netze, Kommunikationsverbindungen und externe Schnittstellen und die
- vorhandenen IT-Systeme (Clients, Server, Netzkopplungselemente, Mobile Devices usw.).

Geschäftsprozesse



Infrastruktur

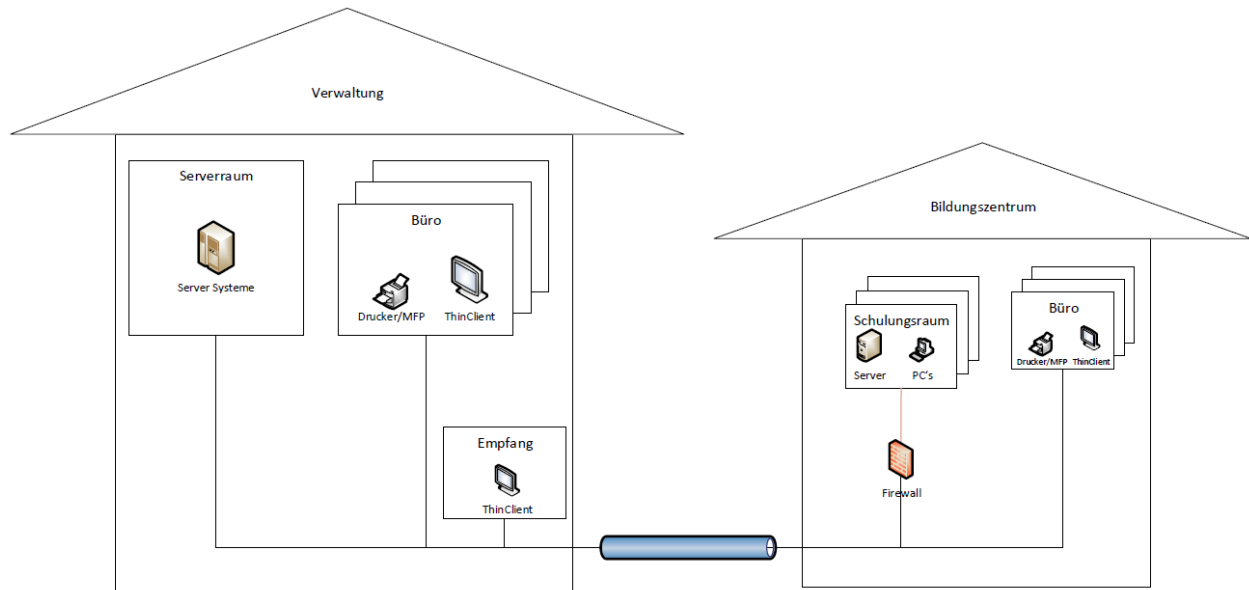
- [R1] Gebäude
- [R2] Server-Raum
- [R3] Technik-Raum
- [R4] Büro-Raum
- [R5] Empfang
- [R6] Werkstätten
- [R7] Prüfungsraum (theoretische Prüfung)
- [R8] Videoüberwachung

Netze und Kommunikation

- [N1] Firewall
- [N2] Router
- [N3] VoIP
- [N4] Switch
- [N5] W-LAN
- [N6] VPN
- [N7] Provider Standleitung
- [N8] VLAN
- [N9] LAN
- [N10] Schnittstellen

IT-Systeme

- [S1] Citrix-Anwendungen
- [S2] Datenbank-Server
- [S3] Windows-Server
- [S4] Linux-Server
- [S5] E-Mail-Server
- [S6] Verzeichnis-Server
- [S7] Dokumentenmanagement-Server
- [S8] File-Server
- [S9] Virtualisierung
- [S10] Mobile-Devices
- [S11] Client-Desktop-Virtualisierung
- [S12] Backup-Server
- [S13] Viren-Scanner
- [S14] Drucker-Multifunktionsgerät
- [S15] Software z.B. Office
- [S16] Telefonanlage
- [S17] Fax
- [S18] Cloud-Server
- [S19] Web-Server



7 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Die folgenden obligatorischen Prozess-Bausteine sind anzuwenden.

ISMS.1: Sicherheitsmanagement

- ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene [Institutionsleitung]
- ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie [Institutionsleitung]
- ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit [Institutionsleitung]
- ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten [Institutionsleitung]
- ISMS.1.A5 Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten [Institutionsleitung]
- ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [Institutionsleitung]
- ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen
- ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess [Vorgesetzte]
- ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse [Institutionsleitung]

Standard-Anforderungen

- ISMS.1.A10 Erstellung eines Sicherheitskonzepts
- ISMS.1.A11 Aufrechterhaltung der Informationssicherheit
- ISMS.1.A12 Management-Berichte zur Informationssicherheit [Institutionsleitung]
- ISMS.1.A13 Dokumentation des Sicherheitsprozesses
- ISMS.1.A14 Sensibilisierung zur Informationssicherheit
- ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit

Anforderungen bei erhöhtem Schutzbedarf

- ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien (CIA)
- ISMS.1.A17 Abschließen von Versicherungen (A)

ORP: Organisation und Personal

- [ORP.1 Organisation](#)
- [ORP.2 Personal](#)
- [ORP.3 Sensibilisierung und Schulung](#)
- [ORP.4 Identitäts- und Berechtigungsmanagement](#)
- [ORP.5 Compliance Management \(Anforderungsmanagement\)](#)

OPS: Betrieb

- [OPS.1.1.2 Ordnungsgemäße IT-Administration](#)
- [OPS.1.1.3 Patch- und Änderungsmanagement](#)
- [OPS.1.1.4 Schutz vor Schadprogrammen](#)
- [OPS.1.1.5 Protokollierung](#)
- [OPS.1.1.6 Software-Tests und -Freigaben](#)
- [OPS.1.2.2 Archivierung](#)
- [OPS.1.2.3 Informations- und Datenträgeraustausch](#)
- [OPS.1.2.4 Telearbeit](#)
- [OPS.2.1 Outsourcing für Kunden](#)
- [OPS.2.4 Fernwartung](#)
- [OPS.3.1 Outsourcing für Dienstleister](#)

CON: Konzeption und Vorgehensweisen

- [CON.1 Kryptokonzept](#)
- [CON.2 Datenschutz](#)
- [CON.3 Datensicherungskonzept](#)
- [CON.4 Auswahl und Einsatz von Standardsoftware](#)
- [CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen](#)
- [CON.6 Löschen und Vernichten](#)
- [CON.7 Informationssicherheit auf Auslandsreisen](#)

DER: Detektion und Reaktion

- [DER.1 Detektion von sicherheitsrelevanten Ereignissen](#)
- [DER.2.1 Behandlung von Sicherheitsvorfällen](#)
- [DER.2.2 Vorsorge für die IT-Forensik](#)
- [DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle](#)
- [DER.3.1 Audits und Revisionen](#)
- [DER.4 Notfallmanagement](#)

APP: Anwendungen

<u>APP.1.1</u>	<u>Office-Produkte</u>
<u>APP.1.2</u>	<u>Web-Browser</u>
<u>APP.2.1</u>	<u>Allgemeiner Verzeichnisdienst</u>
<u>APP.2.2</u>	<u>Active Directory</u>
<u>APP.3.1</u>	<u>Webanwendungen</u>
<u>APP.3.2</u>	<u>Webserver</u>
<u>APP.3.3</u>	<u>Fileserver</u>
<u>APP.3.4</u>	<u>Samba</u>
<u>APP.3.6</u>	<u>DNS-Server</u>
<u>APP.4.3</u>	<u>Relationale Datenbanksysteme</u>
<u>APP.5.1</u>	<u>Allgemeine Groupware</u>
<u>APP.5.2</u>	<u>Microsoft Exchange und Outlook</u>

SYS: IT-Systeme

<u>SYS.1.1</u>	<u>Allgemeiner Server</u>
<u>SYS.1.2.2</u>	<u>Windows Server 2012</u>
<u>SYS.1.3</u>	<u>Server unter Unix</u>
<u>SYS.1.5</u>	<u>Virtualisierung</u>
<u>SYS.1.8</u>	<u>Speicherlösungen</u>
<u>SYS.2.1</u>	<u>Allgemeiner Client</u>
<u>SYS.2.2.2</u>	<u>Clients unter Windows 8.1</u>
<u>SYS.2.2.3</u>	<u>Clients unter Windows 10</u>
<u>SYS.2.3</u>	<u>Clients unter Unix</u>
<u>SYS.3.1</u>	<u>Laptops</u>
<u>SYS.3.2.1</u>	<u>Allgemeine Smartphones und Tablets</u>
<u>SYS.3.2.2</u>	<u>Mobile Device Management (MDM)</u>
<u>SYS.3.2.3</u>	<u>iOS (for Enterprise)</u>
<u>SYS.3.2.4</u>	<u>Android</u>
<u>SYS.3.4</u>	<u>Mobile Datenträger</u>
<u>SYS.4.1</u>	<u>Drucker, Kopierer und Multifunktionsgeräte</u>
<u>SYS.4.4</u>	<u>Allgemeines IoT-Gerät</u>

IND: Industrielle IT

<u>IND.1</u>	<u>Betriebs- und Steuerungstechnik</u>
<u>IND.2.1</u>	<u>Allgemeine ICS-Komponente</u>
<u>IND.2.2</u>	<u>Speicherprogrammierbare Steuerung (SPS)</u>
<u>IND.2.3</u>	<u>Sensoren und Aktoren</u>
<u>IND.2.4</u>	<u>Maschine</u>

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

INF: Infrastruktur

INF.1	Allgemeines Gebäude
INF.2	Rechenzentrum sowie Serverraum
INF.3	Elektrotechnische Verkabelung
INF.4	IT-Verkabelung
INF.7	Büroarbeitsplatz
INF.8	Häuslicher Arbeitsplatz
INF.9	Mobiler Arbeitsplatz
INF.10	Besprechungs-, Veranstaltungs- und Schulungsräume

8 Restrisikobetrachtung / 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-Profiles 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 9 zu finden.

9 Anwendungshinweise

I. Hinweise zur Schutzbedarfsfeststellung

Das vorliegende IT-Grundschutz-Profil fokussiert hoheitliche Geschäftsprozesse, die Handwerkskammern per Gesetz zum Führen bestimmter Aufgaben verpflichtet; hier insbesondere das Führen der Handwerksrolle, der Lehrlingsrolle sowie die Durchführung von Prüfungen.

Unter Umständen sind Schäden zu erwarten, die eine Beeinträchtigung der Institution zur Folge haben wie beispielsweise massiver Datenverlust oder Datendiebstahl von Betriebs-/Lehrlings- bzw. Prüfungsdaten, Reputationsverlust, Schadenersatzforderungen von Betroffenen, Bußgelder gemäß DSGVO.

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen decken mindestens die Anforderungen der „Standard-Absicherung“ des BSI-Standards 200-2 ab, ggf. müssen außerdem Anforderungen aus dem Bereich des hohen Schutzbedarfs umgesetzt werden.

Bei den zugrundeliegenden hoheitlichen Geschäftsprozessen ist grundsätzlich von einem Sicherheitsniveau der Stufe "normal" auszugehen, eine individuelle Schutzbedarfsfeststellung wird dringend empfohlen.

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 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.

Schutzbedarfskategorie "normal"	
Verstoß gegen Gesetze/ Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
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.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
Negative Innen- oder Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauens- beeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.

Tabelle 1: Schutzbedarfskategorie „normal“

Schutzbedarfskategorie "hoch"	
Verstoß gegen Gesetze/Vorschriften/ Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen Vertragsverletzungen mit hohen Konventionalstrafen
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.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
Negative Innen- oder Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Tabelle 2: Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie "sehr hoch"	
Verstoß gegen Gesetze/ Vorschriften/Verträge	Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind
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.
Beeinträchtigung der persönlichen Unversehrtheit	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
Negative Innen- oder Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabelle 3: Schutzbedarfskategorie „sehr hoch“

II. 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**

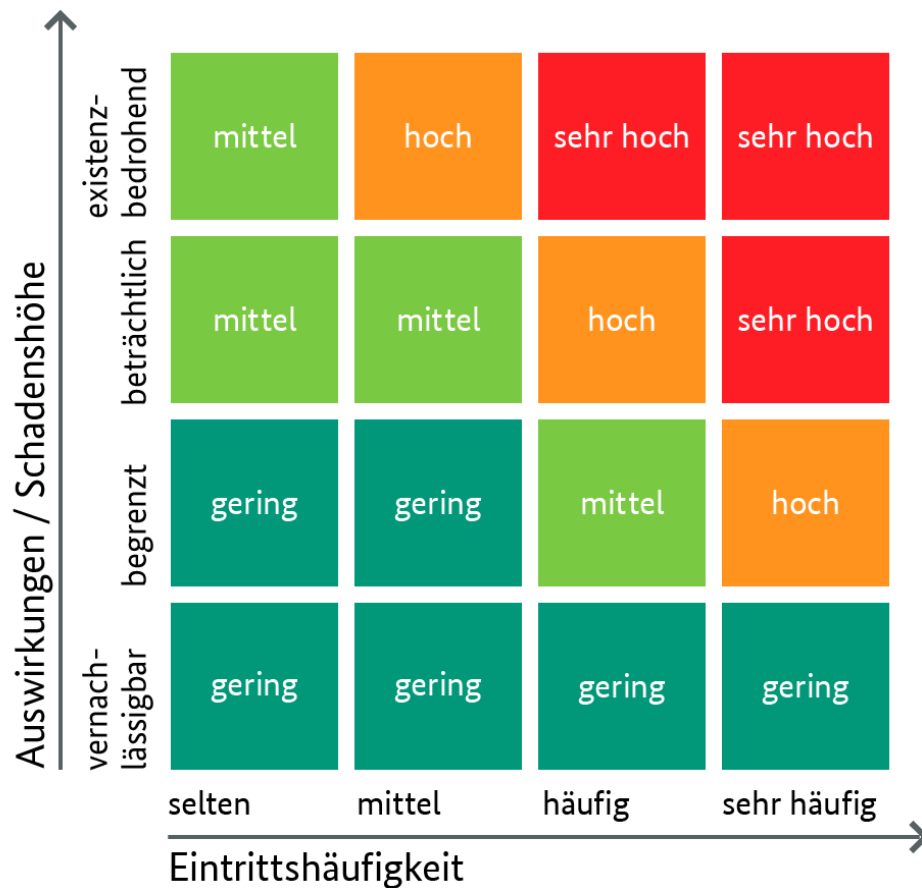
Auch wenn die Zusammenstellung elementarer Gefährdungen vielfältige Bedrohungen berücksichtigt, denen Informationen und Informationstechnik ausgesetzt sind, so kann dennoch nicht ausgeschlossen werden, dass weitere Gefährdungen zu betrachten sind. Dies gilt insbesondere dann, wenn es für ein Zielobjekt 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, dass 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.