ZDH
ZENTRALVERBAND DES
DEUTSCHEN HANDWERKS

IT-Grundschutz-Profil für Handwerksbetriebe

Berlin, 28. März 2019

DAS HANDWERK
DIE WIRTSCHAFTSMACHT. VON NEBENAN.

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	28.03.2019	Herausgeber: ZDH	Finale Version 1.0

Inhalt

1 Einleitung 4

2 Formale Aspekte 5

3 Haftungsausschluss 5

4 Urheberrecht 5

5 Management Summary 5

6 Festlegung des Geltungsbereichs 6

7 Gegenstand des IT-Grundschutz-Profils – Abgrenzung des Informationsverbunds 6

8 Relevante Zielobjekte – Referenzarchitektur 7

9 Zu erfüllende Anforderungen und umzusetzende Maßnahmen 8

9.1. Arbeitshilfe: „Landkarte“ 8

9.2 Liste der relevanten IT-Grundschutz-Bausteine 10

10 Sicherheitsanforderungen und Umsetzungshinweise 13

11 Anhang 14

11.1 Netzplan 14

11.2 Landkarten 15

1 Einleitung

Die Digitalisierung stellt Handwerksbetriebe vor verschiedene Herausforderungen. Speziell das Thema Informationssicherheit hat nicht den Stellenwert, den es auf Grund zunehmender Cyberangriffe, auch auf Handwerksbetriebe, haben müsste. Oft fehlt es in den Betrieben an den entsprechenden Fachkenntnissen, der Zeit und zielgruppenspezifischen Hilfestellungen.

Vor diesem Hintergrund initiierten der Zentralverband des Deutschen Handwerks (ZDH) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen ihrer im Oktober 2017 vereinbarten Kooperation gemeinsam den Prozess zur Erstellung eines IT-Grundschutz-Profils für Handwerksbetriebe. Expertinnen und Experten aus Handwerksorganisationen (Handwerkskammern und Handwerksverbände) haben – in einer vom Bundesamt für Sicherheit in der Informationstechnik (BSI) moderierten und vom Zentralverband des Deutschen Handwerks (ZDH) begleiteten Workshop-Reihe – das nun vorliegende Muster-Sicherheitskonzept entwickelt.

Der IT-Grundschutz des BSI ist eine seit Jahren bewährte Methodik, um das Niveau der Informationssicherheit in Betrieben jeder Größenordnung zu erhöhen. Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept, das als Schablone für Betriebe mit vergleichbaren Rahmenbedingungen dient.

Das vorliegende Dokument „IT-Grundschutz-Profil für Handwerksbetriebe“ soll einfache Wege aufzeigen, wie Betriebe das Thema IT-Sicherheit zielgerichtet angehen und umsetzen können. Es bildet das Beispiel eines Betriebes unabhängig vom Gewerk ab. Dadurch stehen möglichst vielen Handwerksbetrieben Anregungen für die Erhöhung der Informationssicherheit zur Verfügung. Ausgehend von vier als relevant betrachteten Geschäftsprozessen umfasst es u. a.

- eine Liste der relevanten Zielobjekte (Anwendungen, IT-Systeme sowie Räumlichkeiten), die es zu schützen gilt,
- eine Zuordnung der dazu passenden IT-Grundschutz-Bausteine mit Anforderungen und Umsetzungshinweisen sowie
- Empfehlungen zur Umsetzungsreihenfolge.

Zentrale Hilfestellungen für die Umsetzung im Betrieb bieten

1. „Landkarten“ als Entscheidungsgrundlage für die Unternehmensleitung und „Umsetzungs-Fahrplan“ für IT-Fachleute (siehe Anhang),

2. der Routenplaner “Cyber-Sicherheit für Handwerksbetriebe“: Anschauliche Routenpläne und zielgruppengerechte Arbeitshilfen führen auf die für Handwerksbetriebe maßgeblichen IT-Grundschutz-Bausteine und dazu passenden Umsetzungshinweise des BSI in der jeweils aktuellen Edition. Handwerksbetriebe können so ihren individuellen Sicherheitsprozess nach IT-Grundschutz des BSI bedarfsgerecht gestalten.

Zu finden auf den Webseiten: *www.handwerkdigital.de/angebote/cybersicherheit/* und *http://www.allianz-fuer-cybersicherheit.de/routenplaner*.

Hinweis: Das hier beschriebene Beispiel muss nicht notwendigerweise in allen Punkten mit den Gegebenheiten in dem konkret zu betrachtenden Handwerksbetrieb übereinstimmen. Vielmehr soll dieses IT-Grundschutz-Profil als Vorlage dienen. Ohne allzu großen Aufwand sollten sich kleinere Anpassungen an die tatsächlichen Gegebenheiten im Unternehmen vornehmen lassen. Hinweise, wie bei Abweichungen zu verfahren ist, sind ebenfalls in diesem Dokument zu finden.

2 Formale Aspekte

Titel (Kurztitel):	IT-Grundschutz-Profil für Handwerksbetriebe
Autorenschaft:	Vertreterinnen und Vertreter aus den Handwerksorganisationen
Herausgeberschaft:	Zentralverband des Deutschen Handwerks (ZDH)
Versionsstand:	Veröffentlicht am 28.03.2019, Version 1.0, finalisiert im März 2019
Revisionszyklus:	Die Aktualität des Dokuments soll spätestens alle zwei Jahre überprüft werden.
Vertraulichkeit:	Das Dokument in der hier vorliegenden Version ist offen zugänglich.

3 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, so dass sie daher naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

4 Urheberrecht

5 Management Summary

Zielgruppe:	Dieses IT-Grundschutz-Profil richtet sich an Handwerksbetriebe.
Zielsetzung:	Das IT-Grundschutz-Profil für Handwerksbetriebe ermöglicht durch eine breite und grundlegende Erst-Absicherung den Einstieg in die Informationssicherheit für die in Handwerksbetrieben typischen Geschäftsprozesse Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung. Die erarbeitete Strukturbeschreibung erleichtert den Einstieg in einen systematischen Informationssicherheitsprozess gemäß der IT-Grundschutz-Vorgehensweise „Basis-Absicherung“. Anwenderinnen und Anwender können die Sicherheitsbetrachtungen auf die individuellen betrieblichen Rahmenbedingungen übertragen und das Sicherheitsniveau im Unternehmen Schritt für Schritt modular erhöhen.
Aufgaben der Leitungsebene:	Die Autorinnen und Autoren des vorliegenden Dokuments empfehlen Handwerksbetrieben die Anwendung dieses IT-Grundschutz-Profils als Grundlage für die Sicherheitskonzeption.

Handwerksbetriebe, die Teile ihrer technischen Infrastruktur durch Dritte betreiben lassen (möchten), sollten das vorliegende IT-Grundschutz-Profil als Grundlage für die Zusammenarbeit mit entsprechenden Dienstleistern verwenden. Die hier formulierten Anforderungen sollten in den Vertragsbedingungen enthalten sein.

6 Festlegung des Geltungsbereichs

Zielgruppe:

Dieses IT-Grundschutz-Profil richtet sich an Handwerksbetriebe.

Schutzbedarf:

Die in diesem IT-Grundschutz-Profil verwendete Vorgehensweise der Basis-Absicherung betrachtet den Schutzbedarf nicht, da es sich um eine grundlegende Absicherung in der Breite und nicht Tiefe handelt. Erst mit der darauf aufbauenden Vorgehensweise der Standard-Absicherung findet er Berücksichtigung.

Betriebe, die über eine IT-Fachkraft verfügen, die sich mit einem Großteil ihrer Arbeitszeit ausschließlich dem Bereich IT im Unternehmen widmet, sollten mindestens die Abdeckung der Empfehlungen zu den „Standard-Anforderungen“ anstreben.

IT-Grundschutz-Vorgehensweise:

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen für Handwerksbetriebe und verwenden die Basis-Absicherung nach dem BSI-Standard 200-2.

ISO 27001-Kompatibilität:

Diesem IT-Grundschutz-Profil liegt prinzipiell die Basis-Absicherung gemäß IT-Grundschutz zugrunde. Wird davon abweichend durchgängig mindestens die IT-Grundschutz-Vorgehensweise „Standard-Absicherung" umgesetzt, ist diese zu der ISO 27001 kompatibel.

Rahmenbedingungen:

Dieses IT-Grundschutz-Profil basiert auf dem IT-Grundschutz-Kompendium des BSI in der Edition 2018.

7 Gegenstand des IT-Grundschutz-Profils – Abgrenzung des Informationsverbunds

Bestandteile des Informationsverbundes:

Zum Informationsverbund gehören alle Prozesse und Verfahren in einem Handwerksbetrieb, die für die Abwicklung des Kerngeschäfts notwendig sind. Gegenstand des IT-Grundschutz-Profils für Handwerksbetriebe sind die folgenden Anwendungsgebiete:

- Auftragsgewinnung
- Angebotserstellung
- Auftragsdurchführung
- Abrechnung

Nicht berücksichtigte Objekte:	Dieses IT-Grundschutz-Profil fokussiert wertschöpfende Prozesse in einem Handwerksbetrieb (Kernprozesse). Andere für das Unternehmen relevante Prozesse bleiben unberücksichtigt.
Verweis auf andere IT-Grundschutz-Profile:	Das vorliegende IT-Grundschutz-Profil bezieht sich auf das Beispiel eines Betriebes unabhängig vom Gewerk. Im Rahmen der Kooperation von BSI und ZDH ist geplant, dieses IT-Grundschutz-Profil für einzelne Gewerke anzupassen. Informationen zur Unterstützung in dem entsprechenden Erstellungsprozess sind zu finden auf *www.allianz-fuer-cybersicherheit.de*. Die nach und nach erarbeiteten IT-Grundschutz-Profile werden auf *www.zdh.de/fachbereiche/wirtschaft-energie-umwelt/digitalisierung-im-handwerk* und *www.bsi.bund.de/profile* veröffentlicht. Handwerksorganisationen, die für ihr jeweiliges Gewerk ein spezifisches IT-Grundschutz-Profil auf Basis dieses vorliegenden Dokuments erarbeiten möchten, können im Rahmen der BSI-ZDH-Kooperation Unterstützung erhalten. Interessierte können ihre Anfragen an die Allianz für Cyber-Sicherheit des BSI richten: *info@cyber-allianz.de*

8 Relevante Zielobjekte – Referenzarchitektur

Das IT-Grundschutz-Profil soll möglichst alle relevanten Zielobjekte wie zum Beispiel PCs, Netzwerkkomponenten, Software-Programme beinhalten, auf die sich geeignete Schutzmaßnahmen zur Erhöhung der Informationssicherheit in einem Handwerksbetrieb beziehen.

Im Rahmen der zur Identifizierung der Zielobjekte notwendigen Strukturanalyse wurde ausgehend von den vier Geschäftsprozessen Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung die sogenannte Referenzarchitektur (im IT-Grundschutz auch Untersuchungsgegenstand genannt) entwickelt. Diese legt fest, auf welche konkreten Zielobjekte die Anforderungen des IT-Grundschutzes angewendet werden müssen. Hierzu zählen im Einzelnen:

- Anwendungen,
- IT-Systeme (Server, Desktop-Systeme, Mobile Devices etc.) sowie Netze, Netzkomponenten und Kommunikationsverbindungen,
- Infrastruktur (z. B. Gebäude und Räume)

Liste der identifizierten Zielobjekte:

IT-Systeme:

- Server
- PC
- Laptop
- Smartphone
- Multifunktionsgeräte (Drucker, Scanner, Fax)
- IoT (Messgeräte, Waagen, Aufmaß)
- Produktionshardware

Netze und Kommunikation:

- Netz
- WLAN
- Router
- Telefonanlage
- IP-Telefonie
- Cloud

Infrastruktur:

- Gebäude
- Fuhrpark
- Home-Office
- Mobiles Arbeiten

Der sich daraus beispielhaft ergebende Netzplan ist im Anhang zu finden.

Praxistipp: Umgang mit Abweichungen von der Referenzarchitektur

Weicht der zu schützende Informationsverbund im jeweiligen Betrieb von der in diesem IT-Grundschutz-Profil dargestellten Referenzarchitektur ab, sind die zusätzlichen oder nicht vorhandenen Zielobjekte zu dokumentieren. Wie nach der IT-Grundschutz-Methodik üblich, sind diesen Objekten dann geeignete Bausteine des IT-Grundschutz-Kompendiums, sofern vorhanden, zuzuordnen.

9 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Anhand der Referenzarchitektur und der identifizierten Zielobjekte lassen sich passende Bausteine aus dem IT-Grundschutz-Kompendium des BSI zuordnen. Darin sind Gefährdungen und Sicherheitsanforderungen für ein bestimmtes Thema der Informationssicherheit übersichtlich auf rund zehn Seiten erläutert. Zu vielen Bausteinen gibt es zusätzlich Umsetzungshinweise mit detaillierten Beschreibungen passender Sicherheitsmaßnahmen, die als Grundlage für Sicherheitskonzeptionen verwendet werden können.

9.1. Arbeitshilfe: „Landkarte“

Für jeden der vier hier betrachteten Geschäftsprozesse wurde eine „Landkarte“ erstellt. Die Landkarte zeigt alle wesentlichen Erkenntnissen 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 inkl. Empfehlungen zur Priorisierung (siehe „Hinweise zur Nutzung“) dargestellt. Wo keine Zuordnung bestehender Bausteine erfolgen kann, wird deutlich, dass eine eigene Risikoanalyse und ggf. unternehmens- und/oder branchenspezifische Lösungen notwendig sind.

In Form von Grafiken bieten die Landkarten quasi alles auf einen Blick und eröffnen so einen Einstieg in den individuellen IT-Sicherheitsprozess. Sie kann sowohl als Entscheidungsgrundlage für die Unternehmensleitung als auch als „Umsetzungs-Fahrplan“ für IT-Fachleute dienen.

Die Landkarten zu den hier behandelten Geschäftsprozessen sind im Anhang zu finden

- Auftragsgewinnung (Kapitel 11.2, Abbildung 1)
- Angebotserstellung (Kapitel 11.2, Abbildung 2)
- Auftragsdurchführung (Kapitel 11.2, Abbildung 3)
- Abrechnung (Kapitel 11.2, Abbildung 4)

Hinweise zur Nutzung:

Die „Landkarte“ ist **spaltenweise** und nicht zeilenweise zu lesen. In Spalte 1 werden die relevanten Geschäftsprozesse benannt. In Spalte 2 werden die Geschäftsprozesse anhand von typischen Aufgaben in diesem Bereich näher beschrieben. Daraus ergeben sich Anwendungen, die für die Erfüllung der Aufgaben benötigt werden (Spalte 3). Diese Anwendungen laufen auf entsprechenden IT-Systemen (Spalte 4), die sich in bestimmten Räumlichkeiten des Betriebes befinden (Spalte 5).

Die **Kennzeichnung mit einem oder zwei Ausrufezeichen** verweist auf eine herausgehobene Priorisierung eines Objekts, welches für die Durchführung der Aufgaben im jeweiligen Geschäftsprozess von besonderer Bedeutung ist. Das könnte zum Beispiel für die Unternehmensleitung ein Hinweis darauf sein, die Anstrengungen zur Sicherung dieses Zielobjekts zu priorisieren:

- keine Kennzeichnung = normale Priorität
  Der Geschäftsprozess bzw. die Fachaufgabe kann mit tolerierbarem Mehraufwand mit anderen Mitteln (z. B. manuell) durchgeführt werden.
- ein Ausrufezeichen = hohe Priorität
  Der Geschäftsprozess bzw. die Fachaufgabe kann nur mit deutlichem Mehraufwand mit anderen Mitteln durchgeführt werden.
- zwei Ausrufezeichen = sehr hohe Priorität
  Der Geschäftsprozess bzw. die Fachaufgabe kann ohne die Anwendung überhaupt nicht durchgeführt werden.

Die **weißen Schilder** bezeichnen die passenden IT-Grundschutz-Bausteine, die auf das jeweilige Zielobjekt anzuwenden sind. Es kommt vor, dass ein Baustein in mehreren Geschäftsprozessen eine Rolle spielt. Bei der Umsetzung der entsprechenden Sicherheitsanforderungen können sich so Synergien ergeben, indem die Maßnahmen, die für einen priorisierten Geschäftsprozess umgesetzt werden, bereits auf andere ausstrahlen und dort wirken.

Die Markierung mit **weißen Sternchen** (*) an den Anwendungen, IT-Systemen und Räumen zeigt, dass hier weitere Schritte zur Erreichung des angestrebten Sicherheitsniveaus notwendig sind. Im Einzelnen bedeuten die Markierungen:

- kein Kennzeichnung
  Die aufgeführten Bausteine aus dem IT-Grundschutz-Kompendium sind für die Erreichung des angestrebten Sicherheitsniveaus ausreichend.
- ein Stern (*)
  Die hier aufgeführten Bausteine aus dem IT-Grundschutz-Kompendium sind für die Erreichung des angestrebten Sicherheitsniveaus allein nicht ausreichend. Weitere Anforderungen und Umsetzungshinweise sind individuell zu entwickeln.

- zwei Sterne (**)
  Aktuell liegt im IT-Grundschutz-Kompendium dazu kein Baustein vor. Anforderungen und Umsetzungshinweise sind individuell zu entwickeln.

9.2 Liste der relevanten IT-Grundschutz-Bausteine

Tipp zur Umsetzungsreihenfolge:

Die folgenden Bausteine sind mit Hinweisen zur Bearbeitungsreihenfolge versehen:

- 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.

Übersicht I: Allgemeine Bausteine (für das Unternehmen insgesamt von Relevanz)

ISMS (Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess)

- ISMS.1 Sicherheitsmanagement (R1)

ORP (Organisatorische und personelle Sicherheitsaspekte)

- ORP.1 Organisation (R1)
- ORP.2 Personal (R1)
- ORP.3 Sensibilisierung und Schulung (R1)
- ORP.4 Identitäts- und Berechtigungsmanagement (R1)
- ORP.5 Compliance Management (Anforderungsmanagement) (R3)

CON (Konzepte und Vorgehensweisen)

- CON.1 Kryptokonzept (R3)
- CON.2 Datenschutz (R2)
- CON.3 Datensicherungskonzept (R1)
- CON.4 Auswahl und Einsatz von Standardsoftware (R2)
- CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen (R3)
- CON.6 Löschen und Vernichten (R1)

OPS (Sicherheitsaspekte des operativen IT-Betriebs)

- OPS.1.1.2 Ordnungsgemäße IT-Administration (R1, wenn IT von Betrieb eigenständig administriert wird)
- OPS.1.1.3 Patch- und Änderungsmanagement (R1)

- OPS.1.1.4 Schutz vor Schadprogrammen (R1)
- OPS.1.1.5 Protokollierung (R1)
- OPS.1.1.6 Software-Tests und -Freigaben (R1)
- OPS.1.2.3 Informations- und Datenträgeraustausch (R3)
- OPS.2.4 Fernwartung (R3)

DER (Detektion von Sicherheitsvorfällen und Reaktion bei Vorfällen)

- DER.1 Detektion von sicherheitsrelevanten Ereignissen (R2)
- DER.2.1 Behandlung von Sicherheitsvorfällen (R2)
- DER.2.2 Vorsorge für die IT-Forensik (R3)
- DER.3.1 Audits und Revisionen (R3)
- DER.4 Notfallmanagement (R3)

Übersicht II: Geschäftsrelevante Bausteine

OPS (Sicherheitsaspekte des operativen IT-Betriebs)

- OPS.1.2.4 Telearbeit (R3)
- OPS.2.1 Outsourcing für Kunden (R2)
  (Darin beispielhaft Verweise auf Bausteine zur Konkretisierung von Anforderungen an externe Dienstleister in Bezug auf konkrete Zielobjekte:

  - APP.3.1 Webanwendungen

  - APP.3.2 Webserver

  - SYS.1.1 Allgemeiner Server

  - SYS.1.2.2 Windows Server 2012
- OPS.2.2 Cloud-Nutzung

APP (Anwendungen und Dienste)

- APP.1.1 Office-Produkte (R2)
- APP.1.2 Web-Browser (R2)
- APP.1.4 Mobile Anwendungen (Apps) (R2)
- APP.5.1 Allgemeine Groupware (R2)
- APP.5.2 Microsoft Exchange und Outlook (R2)

SYS (IT-Systeme)

- SYS.2.1 Allgemeiner Client (R2)
- SYS.2.2.2 Clients unter Windows 8.1 (R2)
- SYS.2.2.3 Clients unter Windows 10 (R2)

- SYS.3.1 Laptops (R2)
- SYS.3.2.1 Allgemeine Smartphones und Tablets (R2)
- SYS.3.2.3 iOS (for Enterprise) (R2)
- SYS.3.2.4 Android (R2)
- SYS.3.3 Mobiltelefon (R2)
- SYS.3.4 Mobile Datenträger (R2)
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte (R2)
- SYS.4.4 Allgemeines IoT-Gerät (R2)

NET (Netzverbindungen und Kommunikation)

- NET.1.1 Netzarchitektur und -design (R2)
- NET.2.1 WLAN-Betrieb (R2)
- NET.2.2 WLAN-Nutzung (R2)
- NET.3.1 Router und Switches (R2)
- NET.3.2 Firewall (R2)
- NET.3.3 VPN (R2)
- NET.4.1 TK-Anlagen (R2)
- NET.4.2 VOIP (R2)
- NET.4.3 Fax (R2)

IND (Industrielle IT – Produktion)

- IND.2.1 Allgemeine ICS-Komponente (R2)
- IND.2.2 Speicherprogrammierbare Steuerung (SPS) (R2)
- IND.2.3 Sensoren und Aktoren (R2)
- IND.2.4 Maschine (R2)

INF (Aspekte der infrastrukturellen Sicherheit)

- INF.1 Allgemeines Gebäude (R2)
- INF.2 Rechenzentrum sowie Serverraum (R2)
- INF.3 Elektrotechnische Verkabelung (R2)
- INF.4 IT-Verkabelung (R2)
- INF.7 Büroarbeitsplatz (R2)
- INF.8 Häuslicher Arbeitsplatz (R2)
- INF.9 Mobiler Arbeitsplatz (R2)

10 Sicherheitsanforderungen und Umsetzungshinweise

Für die praktische Umsetzung des „IT-Grundschutz-Profils für Handwerksbetriebe“ haben Expertinnen und Experten aus Handwerksorganisationen und dem BSI Arbeitshilfen entwickelt. Daraus ist der Routenplaner „Cyber-Sicherheit für Handwerksbetriebe“ entstanden. Herausgeber sind die Allianz für Cyber-Sicherheit des BSI und das Kompetenzzentrum Digitales Handwerk des ZDH.

Der Routenplaner zeigt praktische Wege auf, wie kleine und mittelständische Unternehmen das Thema Informationssicherheit zielgerichtet angehen und umsetzen können. Handwerksbetriebe können aus verschiedenen Routen auswählen und ihren individuellen Sicherheitsprozess nach IT-Grundschutz des BSI bedarfsgerecht gestalten. Anschauliche Routenpläne und zielgruppengerechte Arbeitshilfen führen auf die für Handwerksbetriebe maßgeblichen IT-Grundschutz-Bausteine und dazu passenden Umsetzungshinweise des BSI in der jeweils aktuellen Edition.

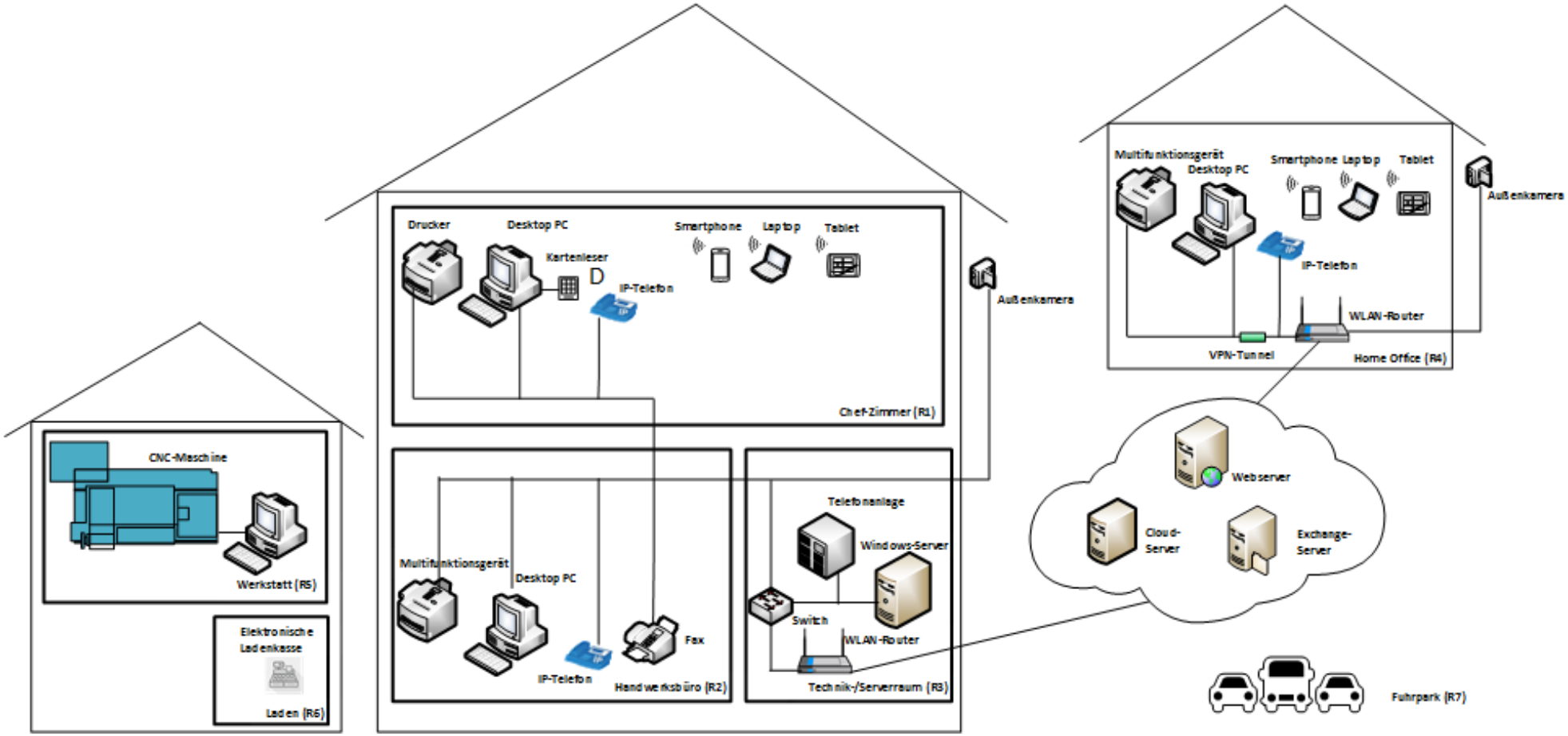
Link zum Routenplaner „Cyber-Sicherheit für Handwerksbetriebe“:

www.handwerkdigital.de/angebote/cybersicherheit

https://www.allianz-fuer-cybersicherheit.de/routenplaner

11 Anhang

11.1 Netzplan



11.2 Landkarten

Abbildung 1: Auftragsgewinnung

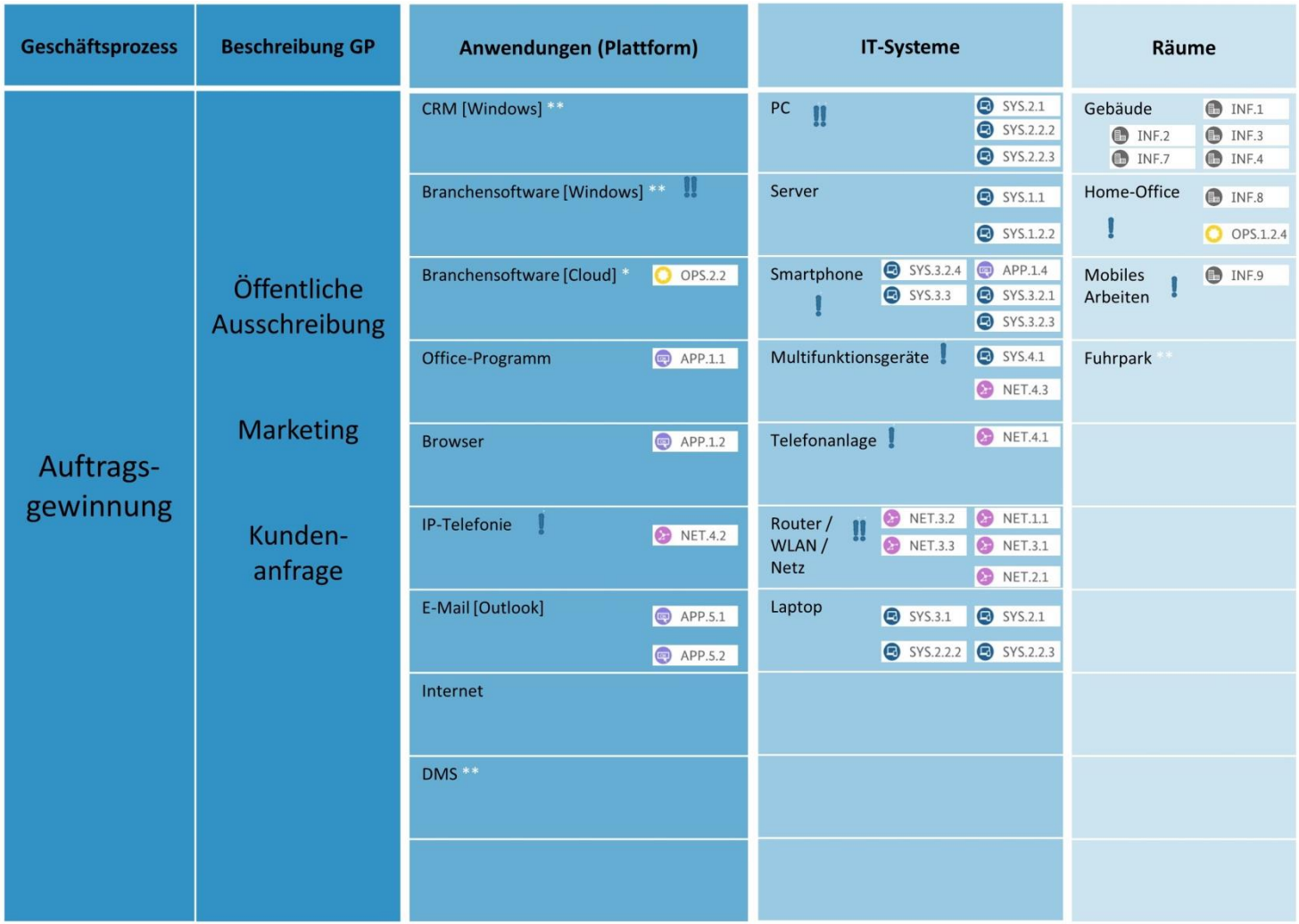


Abbildung 2: Angebotserstellung

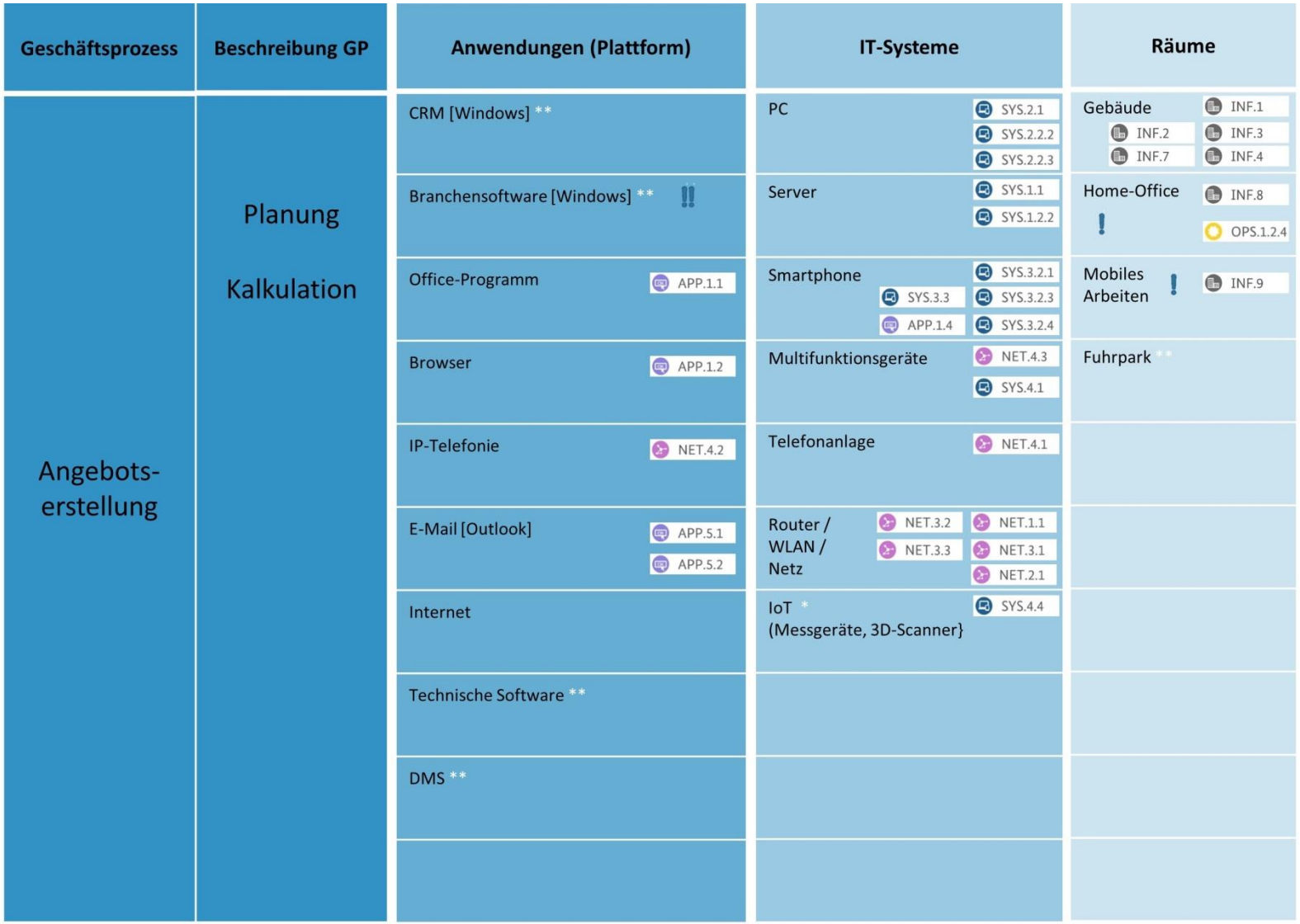


Abbildung 3: Auftragsdurchführung

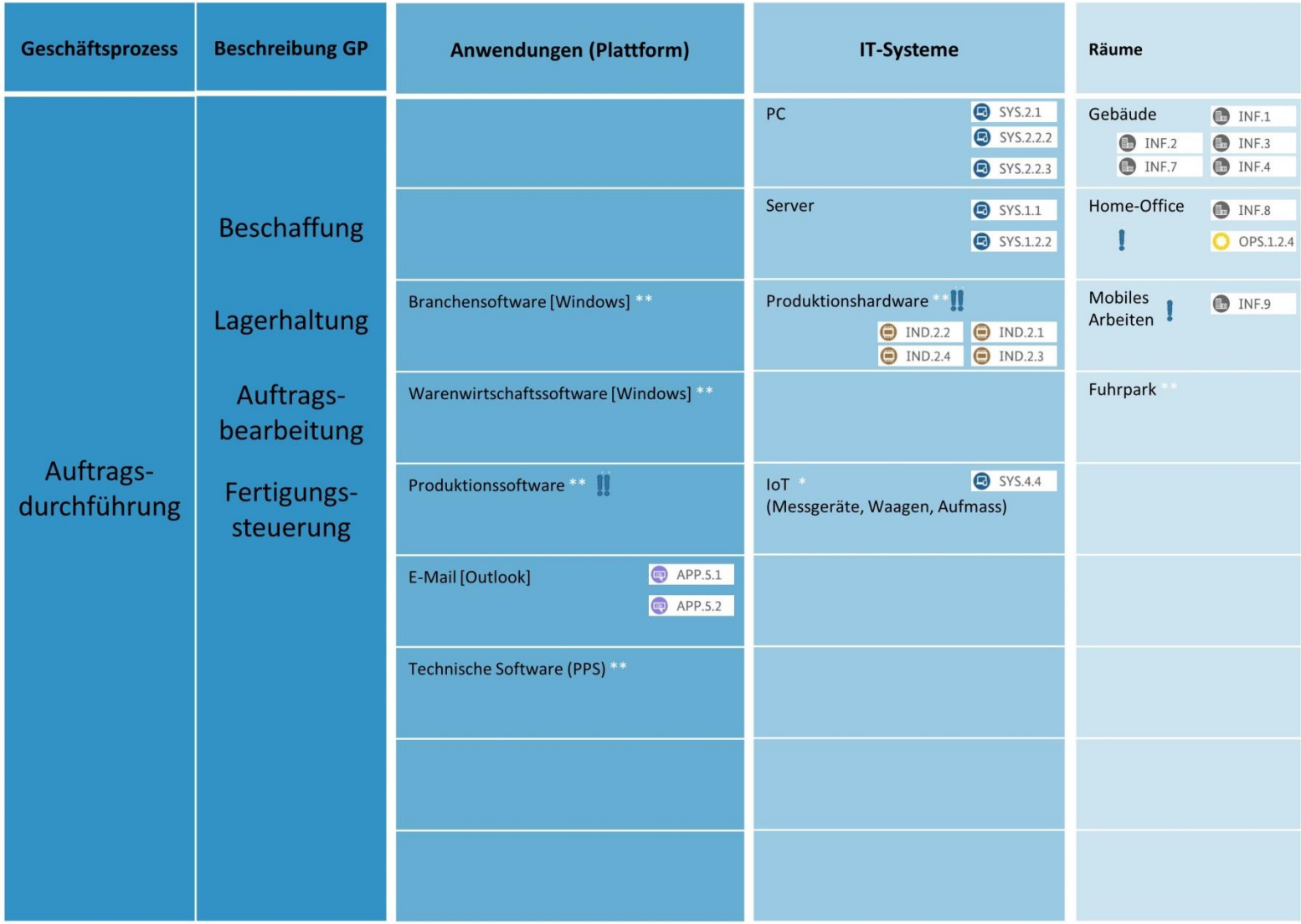


Abbildung 4: Abrechnung