KOMPETENZZENTRUM
DIGITALES HANDWERK

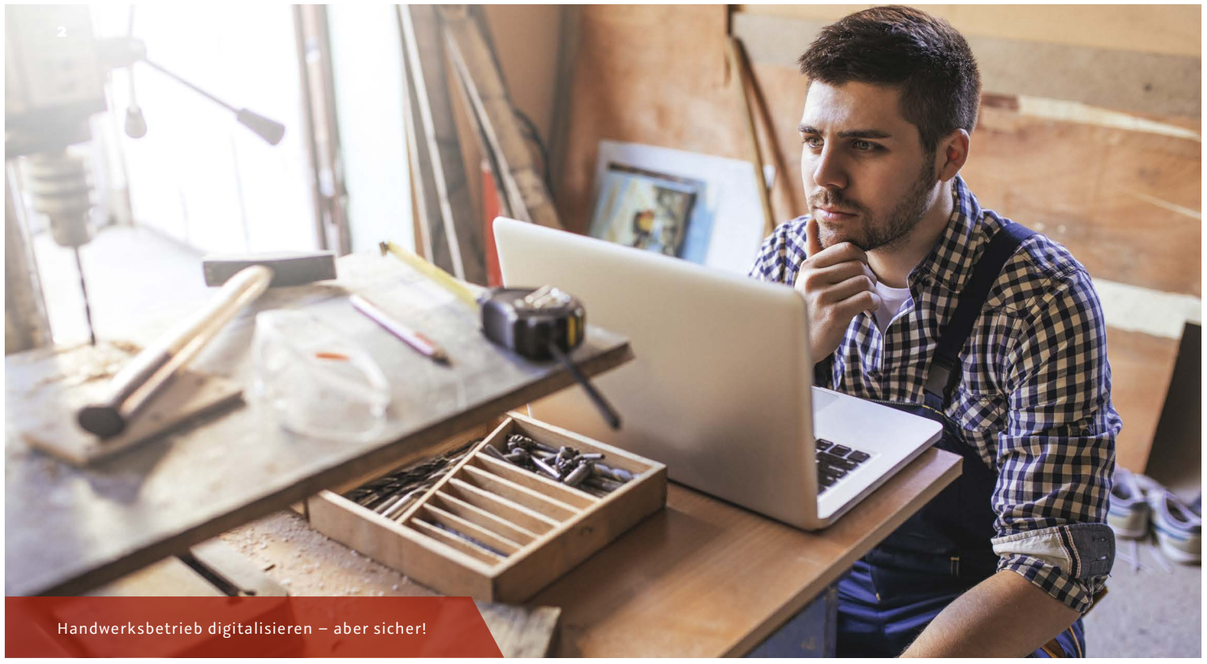
ROUTENPLANER:

Cyber-Sicherheit für Handwerksbetriebe.

www.handwerkdigital.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages



Handwerksbetrieb digitalisieren – aber sicher!

Inhalt.

Hintergrundinformationen zum Routenplaner.

Fachliche Einordnung
Der hier vorliegende Routenplaner "Cyber-Sicherheit für Handwerksbetriebe" basiert auf dem "IT-Grundschutz-Profil für Handwerksbetriebe", herausgegeben vom Zentralverband des deutschen Handwerks (ZDH). Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (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.

In einer vom BSI moderierten und vom ZDH begleiteten Workshop-Reihe haben Expertinnen und Experten aus Handwerkskammern, -verbänden und -instituten ein Sicherheitskonzept entwickelt. Darin sind die passenden Bausteine aus dem IT-Grundschutz-Kompendium des BSI aufgeführt, die zur Steigerung der Informationssicherheit eines „typischen" Handwerksbetriebs anzuwenden sind. Auch wird deutlich, wenn zu bestimmten Anwendungen, IT-Systemen und Räumen aktuell keine Bausteine zur Verfügung stehen.

Der Routenplaner konzentriert sich auf die zum Zeitpunkt der Veröffentlichung zur Verfügung stehenden IT-Grundschutz-Bausteine. Durch ihre Umsetzung wird das Sicherheitsniveau eines Betriebs signifikant erhöht. Darüber hinaus finden Sie wertvolle Hinweise und Empfehlungen im IT-Grundschutz-Profil selbst unter: **www.bsi.bund.de/profile.** Und nicht zuletzt befinden sich stets weitere Bausteine in der Ausarbeitung: **www.bsi.bund.de/grundschutz**

Autorenschaft
Die Einleitungstexte "Cyber-Sicherheit – Was geht mich das an?", "Ihre Route zu mehr Cyber-Sicherheit", die FAQ im Kapitel "IT-Grundschutz-Bausteine kurz & bündig – Arbeitshilfen" sowie die Einleitungstexte für die einzelnen Bausteine in den Arbeitshilfen wurden von der Allianz für Cyber-Sicherheit des BSI erstellt. Die „Hinweise zum besseren Verständnis" sowie die „Empfehlungen zu einzelnen Anforderungen" in den Arbeitshilfen haben die Vertreterinnen und Vertreter aus den Handwerksorganisationen im Rahmen des Erstellungsprozesses für das oben genannte IT-Grundschutz-Profil erstellt.

Haftungsausschluss
Der Routenplaner wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorinnen und Autoren haben keinen Einfluss auf die Nutzung des Routenplaners durch Anwenderinnen und Anwender und kennen auch nicht die individuellen Anforderungen an ihre Sicherheitskonzepte, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

Cyber-Sicherheit – Was geht mich das an?

Die kurze Antwort lautet: Viel! Unter Umständen haben Sie ja bereits einen Cyber-Vorfall erlebt. Es gibt im Zusammenhang mit der Datenschutz-Grundverordnung (DSGVO) oder der Einführung der elektronischen Rechnung Anforderungen zu beachten. Auch Kundinnen und Kunden fragen vermehrt nach der Sicherheit ihrer Daten. Daher wird Unternehmen zunehmend bewusst: Informationssicherheit ist die notwendige Voraussetzung für eine erfolgreiche Digitalisierung. Daran führt kein Weg vorbei.

Mit überschaubarem Aufwand viel erreichen.

Natürlich bleibt das eigentliche Handwerk Kern des Geschäfts. Die Informationstechnik nimmt eine unterstützende Rolle ein. Sie abzusichern, ist jedoch wichtig für den Erfolg des Geschäfts. Deshalb sind IT-Sicherheitsmaßnahmen notwendig, diese dürfen die Unternehmen aber nicht überfordern. Cyber-Sicherheit muss sich auch in kleineren Betrieben neben dem geschäftlichen Alltag umsetzen lassen. Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eine modulare und flexible Methodik für die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit. Im Rahmen der Kooperation von ZDH und BSI wurde ein IT-Grundschutz-Profil entwickelt, das es Handwerksbetrieben ermöglicht, mit überschaubarem personellen und finanziellen Aufwand die ersten Schritte in Richtung Informationssicherheit zu gehen.

Einfach machen.

Mit dem Routenplaner „Cyber-Sicherheit für Handwerksbetriebe" haben Sie eine praktische Arbeitshilfe an der Hand, die Sie Schritt für Schritt durch den Sicherheitsprozess führt. Expertinnen und Experten aus Handwerksorganisationen und dem BSI schlagen Ihnen individuelle Routen gemäß IT-Grundschutz des BSI vor. So können Sie das Sicherheitsniveau in Ihrem Betrieb bedarfsgerecht erhöhen. Folgen Sie der von Ihnen gewählten Route und erreichen Sie das Ziel: **Digital UND sicher zum Erfolg!**

Der Ernstfall: „Und plötzlich ging nichts mehr!"

Ransomware. Alles verschlüsselt. Kein Zugriff mehr auf IT-Systeme und Daten. Fällt das Datennetz aus, kommen die Geschäfte zum Erliegen: Kundendaten sind nicht abrufbar, der Überblick über die Disposition fehlt, Aufträge und Rechnungen können nicht erstellt, Ware und Material nur mit erheblichem Mehraufwand geordert werden. Ohne ein aktuelles Daten-Back-up droht der unwiederbringliche Verlust von Unternehmenswerten. Die Folgeschäden sind erheblich: Kunden springen ab, Lieferanten werden ungeduldig, Folgeaufträge gehen verloren. Die Betriebsabläufe wieder in gewohnte Bahnen zu bringen, erfordert zudem meist erhebliche Anstrengungen unter oft großem Zeitdruck.
Wie gehen Betriebe damit um? Wie kann man sich schützen? Lernen Sie aus den Erfahrungen anderer: Auf der Website der Allianz für Cyber-Sicherheit des BSI finden Sie Beispiele aus der betrieblichen Praxis – in Wort, Ton und Bild.

Ihre Route zu mehr Cyber-Sicherheit.

„Wo fange ich an?“, fragen sich viele, wenn es darum geht, die Informationssicherheit im Betrieb zu erhöhen. Keine Sorge! Dieser Frage haben sich Expertinnen und Experten aus Handwerksorganisationen in einer Workshop-Reihe im Rahmen der Kooperation von ZDH und BSI bereits intensiv gewidmet. Das Ergebnis ist das „IT-Grundschutz-Profil für Handwerksbetriebe“, veröffentlicht im März 2019, auf dem dieser Routenplaner basiert.

Komplexität auflösen, individuelle Routen planen.

Wer eine längere Reise plant, teilt sie in Etappen auf – so lässt sich auch der betriebliche Prozess zur Steigerung der Informationssicherheit Schritt für Schritt umsetzen. Starten Sie an einem Punkt Ihrer Wahl, durchlaufen Sie nach und nach die vorgeschlagenen Stationen. Das Tempo Ihres Vorgehens bestimmen Sie selbst. Sie setzen die Prioritäten und entscheiden, bis wann etwas fertiggestellt sein soll.
Stellen Sie an einer der Stationen fest, dass es in Ihrem Betrieb Teile der benannten IT-Systeme nicht gibt, überspringen Sie diese Bausteine einfach. Folgen Sie dem jeweiligen Routenverlauf und nutzen Sie nur die Bausteine, die auf Ihren Betrieb zutreffen. Haken Sie die Stationen nach und nach ab. Ihr Routenplaner begleitet Sie wie eine Checkliste für mehr Cyber-Sicherheit in Ihrem Betrieb.

Sie haben die Wahl.

Betrieblich, räumlich oder ganz nah am IT-Grundschutz – welchen Ansatz möchten Sie wählen, um sich dem Thema Informationssicherheit in Ihrem Betrieb zu widmen? Im Folgenden finden Sie verschiedene Routen, aus denen Sie Ihren individuellen Sicherheitsprozess nach IT-Grundschutz des BSI auswählen können.
Ziel ist es, sich im Laufe des Prozesses alle für Sie relevanten Bausteine erarbeitet zu haben. Doch der damit verbundene Aufwand lohnt sich. Sie investieren in eine sichere digitale Zukunft für Ihr Unternehmen. Denn nur wenn Informationssicherheit gewährleistet und mit höchster Priorität behandelt wird, kann diese Stütze den wirtschaftlichen Erfolg dauerhaft tragen.

1, 2, 3 – So wird's gemacht: Kleine Bedienungshilfe für Ihren Routenplan.

1

Passende Route wählen:
Route 1 (betrieblich) Welche Aufgabenbereiche sind besonders relevant für den Erfolg des Betriebs: Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung oder Abrechnung? Starten Sie mit dem für Sie wichtigsten Bereich.
Route 2 (räumlich) Bei Ihnen steht demnächst eine Renovierung der Büroräume an? Oder die Werkstatt muss mal wieder in Ordnung gebracht werden? Dann können Sie auch gleich mit den IT-Themen aufräumen und den Prozess für mehr Informationssicherheit von dem betreffenden Raum aus starten.
Route 3 (thematisch) Sie haben sich entschlossen, das „IT-Grundschutz-Profil für Handwerksbetriebe“ nach Themen sortiert von Anfang bis Ende einfach umzusetzen? Dann liegen Sie mit der Route 3 genau richtig.

2

Bearbeiten der Bausteine:
Jede Route beinhaltet verschiedene Stationen mit Bausteinen. Diese müssen nach und nach bearbeitet werden. Gibt es Teile der benannten IT-Systeme oder -Anwendungen nicht in Ihrem Betrieb, lassen Sie diese Bausteine einfach weg. Eine allgemeine Anleitung und Informationen zu den jeweiligen Bausteinen finden Sie im Kapitel „IT-Grundschutz-Bausteine kurz & bündig – Arbeitshilfen“.

3

Durchhalten – Tipp für die Praxis:
Nutzen Sie die Bilder und Checklisten zur Route Ihrer Wahl zum Abhaken der erledigten Bausteine. So behalten Sie den Überblick, was noch zu tun ist – und können sich über das freuen, was schon geschafft ist.

Ein sicherer Weg in die digitale Zukunft

IT-Grundschutz – Acht Pluspunkte für Ihre Informationssicherheit.

Mit dem Original der Informationssicherheit in eine sichere Digitalisierung.

- **Praxiserprobt:** Im Alltag gelebte Methode für den angemessenen Schutz von Informationen und Daten.
- **Stand der Technik:** Seit mehr als 25 Jahren vom Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich weiterentwickelt.
- **Strukturiert:** Die IT-Grundschutz-Methode schlägt eine Reihenfolge für die Umsetzung vor.
- **Modular:** Übersichtliche IT-Grundschutz-Bausteine bieten konkrete Anforderungen für ca. 100 Top-Themen der Informationssicherheit.
- **Zeitsparend:** Die Risikoanalyse zu fast 50 potenziellen Gefährdungen beinhalten den Bausteinen bereits.
- **Realisierbar:** Die Basis-Absicherung ermöglicht eine grundlegende Erstabsicherung, insbesondere auch für kleine und mittlere Betriebe.
- **Branchenspezifisch:** IT-Grundschutz-Profile dienen als Muster-Sicherheitskonzept für eine Branche und sind individuell übertragbar auf den jeweiligen Betrieb.
- **International anerkannt:** Bewährte Standard-Absicherung kompatibel zu ISO 27001.

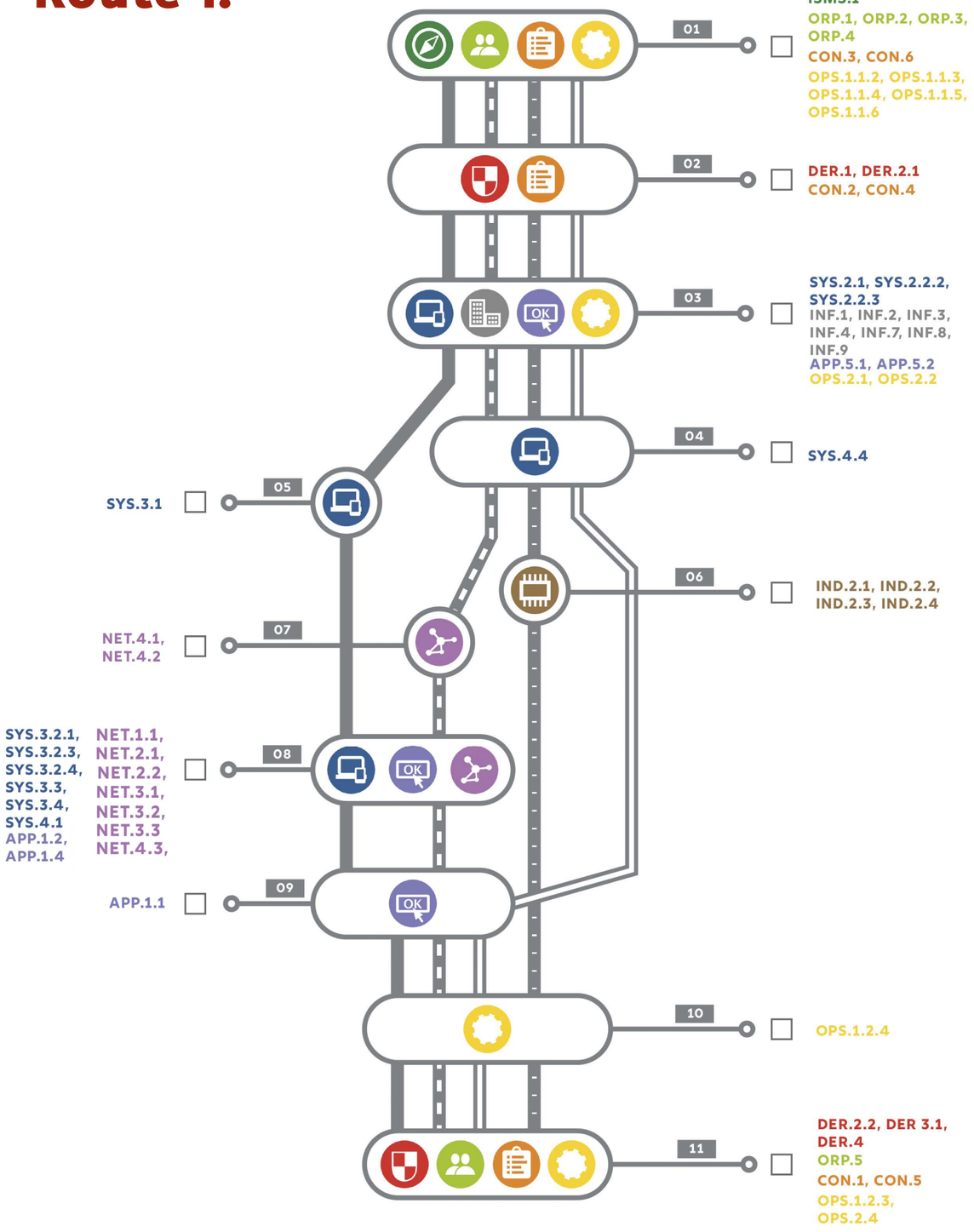
Wer kann den Betrieb bei der Umsetzung unterstützen?

Für den Einstieg:
IT-Sicherheitsbotschafter
Bundesweit unterstützen speziell ausgebildete „IT-Sicherheitsbotschafter“ der Handwerkskammern die Betriebe durch maßgeschneiderte Beratungen und Lösungen. Ansprechpersonen in Ihrer Nähe sind zu finden unter:
www.it-sicherheit-handwerk.de/no_cache/startseite.html.

Im Sicherheitsprozess:
Einen geeigneten IT-Dienstleister finden
Der Deutsche Industrie- und Handelskammertag e.V. (DIHK) hat einen Kriterienkatalog zusammengestellt, der Betrieben ohne eigene Sicherheitsexpertise bei der Auswahl eines vertrauenswürdigen IT-Dienstleisters hilft:
www.ihk.de/it-sicherheits-kriterien.

Zum Dranbleiben:
Allianz für Cyber-Sicherheit des BSI
Die Erfahrung zeigt: Ein Schutz vor Cyber-Angriffen lässt sich am besten gemeinsam erreichen. Profitieren Sie von der Expertise des BSI und seiner Partner aus Wirtschaft und Forschung. Denn Netzwerke schützen Netzwerke:
www.allianz-fuer-cybersicherheit.de/ACS/Registrierung.

Route 1:



Erklärung zu den IT-Grundschutzbausteinen siehe Seite 12.

Betrieblich.

IT-unterstützte Abläufe sind in vielen Betrieben nicht mehr wegzudenken – sei es in der Auftragsgewinnung, der Angebotserstellung, Auftragsdurchführung oder Abrechnung.

Mit der Route 1 durchlaufen Sie typische Aufgabenbereiche Ihres Betriebs. Welcher Bereich ist für Ihren Geschäftserfolg besonders relevant? Machen Sie ein Ranking. Starten Sie mit dem wichtigsten Bereich und widmen Sie sich danach den anderen. Egal, mit welchem Weg Sie beginnen: Sie generieren in jedem Fall Synergien. Denn sobald sie einen der vier Wege in dieser Route absolviert haben, sind bereits große Teile der anderen Wege erledigt. Wurden alle der insgesamt elf Stationen angesteuert, haben Sie das vollständige Profil geschafft.

Ihre Wege im Überblick.

Auftragsgewinnung:
Sie durchlaufen die Stationen 1, 2, 3, 5, 8, 9, 10 und 11. Für das vollständige Profil fehlen nur noch die Stationen 4, 6 und 7.

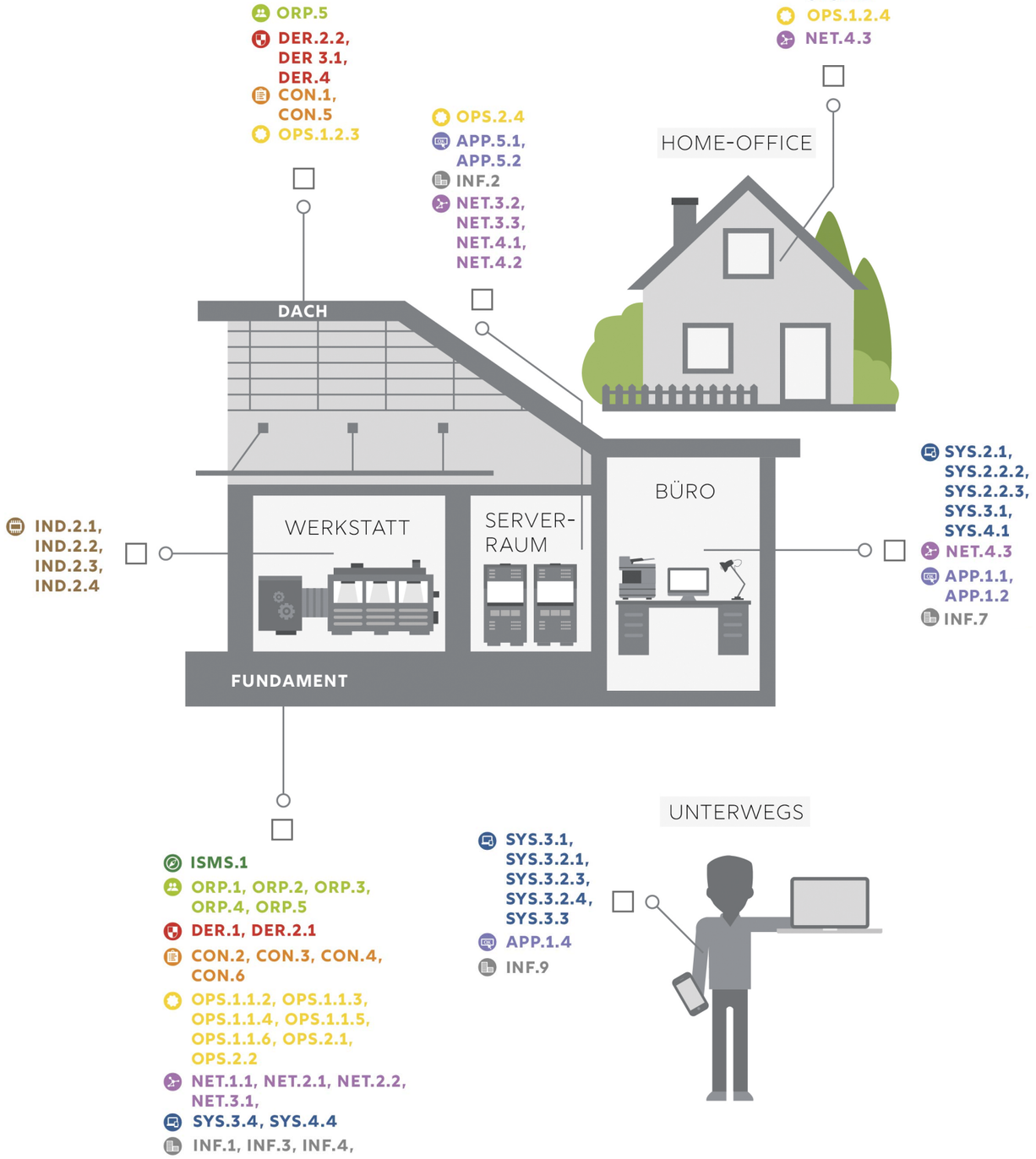
Angebotserstellung:
Mit den Stationen 1, 2, 3, 4, 7, 8, 9, 10 und 11 haben Sie den größten Teil der Route absolviert – das vollständige Profil erreichen Sie über die Stationen 5 und 6.

Auftragsdurchführung:
Dieser Weg ist eine Art Schnelldurchgang über die Stationen 1, 2, 3, 4, 6, 10, 11. Vollständig wird das Profil, wenn Sie noch die Stationen 5, 6, 7, 8 und 9 nachlegen.

Abrechnung:
Für Schnellrechner: Wer auf diesem Weg die Stationen 1, 2, 3, 4, 9, 10, 11 zurücklegt, muss für das vollständige Profil nur noch die Stationen 5, 6, 7 und 8 schaffen.

Tipp für die Praxis:
Kleine Ergänzung zur Bedienungshilfe „1, 2, 3 – So wird's gemacht" (S.4): Sie finden in der Abbildung S.6 neben den Bausteinen an den elf Stationen jeweils eine Checkbox. Hier kommt der Haken hin, wenn Sie eine Etappe geschafft haben.

Route 2:



Räumlich.

Beim Rundgang durch die Betriebsstätte wird eines deutlich: Die Digitalisierung ist im Handwerk angekommen. Am Empfang ein PC, in der Ecke des Büros der Router, in der Werkstatt vielleicht eine IT-unterstützte Maschine, unterwegs ein Smartphone, im Home-Office ein Laptop. Räumen Sie auf und machen Sie Ihre Räume mitsamt IT-System(en) sicher.

Route 2 führt Sie von Raum zu Raum – und auch unterwegs – zu mehr Informationssicherheit im Betrieb. Beginnen Sie dort, wo Sie schon immer einmal Ordnung machen wollten und nehmen Sie sich dann nach und nach die anderen Räume vor. Auf diese Weise erarbeiten Sie sich alle notwendigen Bausteine. Es gibt allerdings eine Bedingung: Fundament und Dach sind Pflicht.

Ihre Räume im Überblick.

Pflichtprogramm zu Beginn: Fundament:
Bloß nicht auf Sand bauen – die hier aufgelisteten Bausteine sind für den gesamten Betrieb wichtig, damit legen Sie eine solide Basis für Ihre Informationssicherheits-Architektur.

Serverraum:
An diesem Ort läuft vieles zusammen – Im Serverraum befindet sich die Hardware, die der Bereitstellung von Diensten und Daten im Betrieb dient.

Büro:
Büro ist nicht gleich Büro, aber jeder Raum der Betriebsstätte, in dem IT-unterstützt Angebote erstellt werden oder die Abrechnung erfolgt, kann als Büroraum im Sinne dieser Route gewertet werden.

Werkstatt:
Gehören Sie zum produzierenden Handwerk? Dann sollten Ihre IT-unterstützten Maschinen sicher sein.

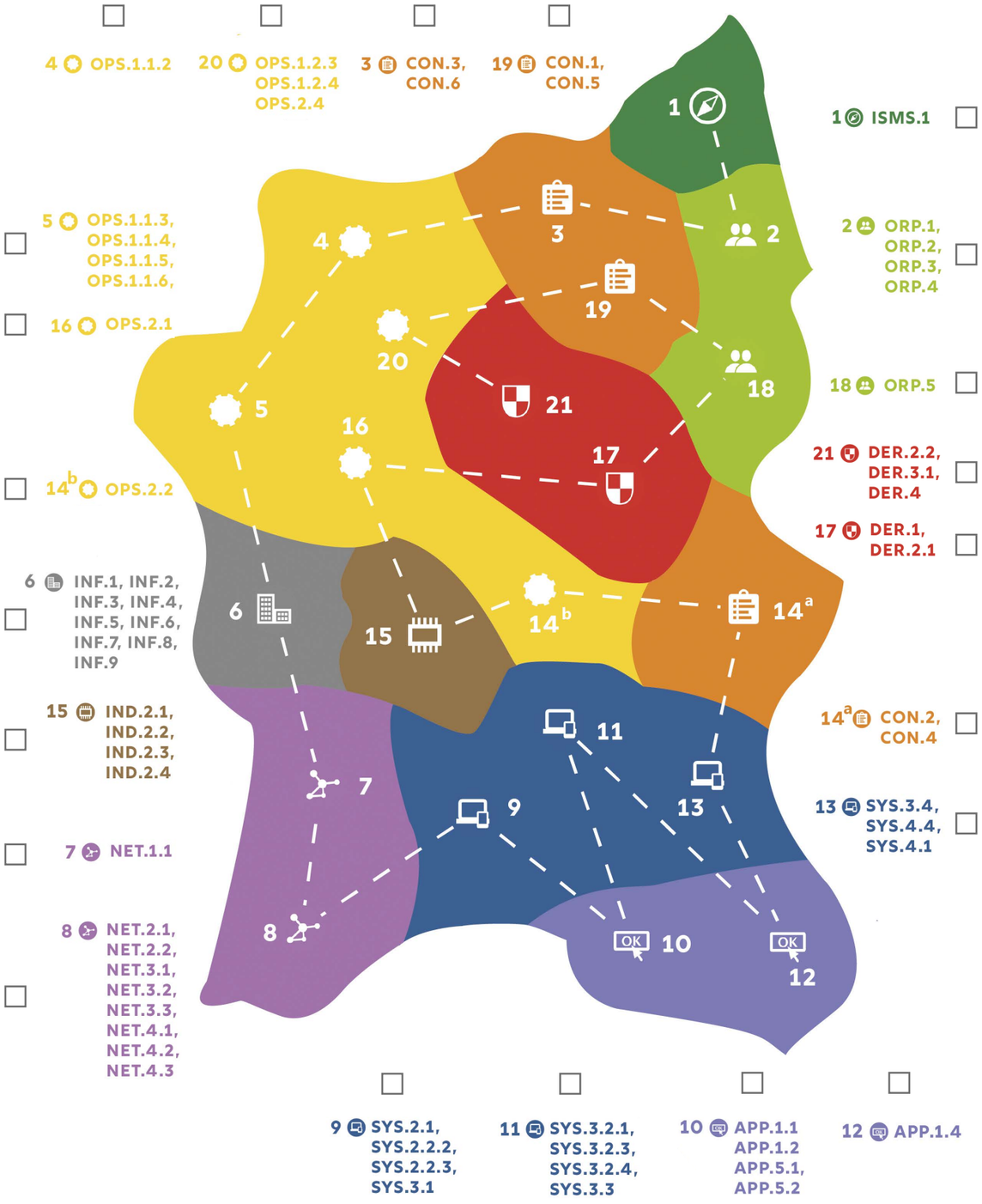
Home-Office:
Home Secure Home – so sollte das Motto lauten, wenn betriebseigene Informationen an einem häuslichen Arbeitsplatz bearbeitet werden.

Unterwegs von Raum zu Raum:
Ob auf der Straße, beim Kunden, auf Geschäftsreisen oder zwischendurch mal von zu Hause aus – wechselnde Arbeitsplätze bedeuten unterschiedliche Umgebungen und damit erhöhte Anforderungen an die Informationssicherheit.

Pflichtprogramm zum Schluss: Dach:
Setzen Sie zum Schluss Ihren Räumen die Krone auf.

Tipp für die Praxis:
Kleine Ergänzung zur Bedienungshilfe „1, 2, 3 – So wird's gemacht" (S.4): Bitte beachten Sie insbesondere die Reihenfolge (R1 bis R3) in der Bearbeitung der Bausteine und gehen Sie vom Wesentlichen zum eher Nachrangigen. Und: In die Checkbox kommt ein Haken, wenn Sie diesen Raum erledigt haben.

Route 3:



Thematisch.

Sie interessieren sich für die zentralen Themen der Informationssicherheit? Und Sie möchten alle Bausteine aus dem „IT-Grundschutz-Profil für Handwerksbetriebe“ von Anfang bis Ende systematisch durcharbeiten?

Route 3 orientiert sich deutlich an der IT-Grundschutz-Methode und leitet Sie Schritt für Schritt durch die zehn Schichten unter Beachtung der empfohlenen Umsetzungsreihenfolge R1 bis R3.

ISMS: Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess

ORP: Organisatorische und personelle Sicherheitsaspekte

CON: Konzepte und Vorgehensweisen

OPS: Sicherheitsaspekte des operativen IT-Betriebs

DER: Detektion von Sicherheitsvorfällen und Reaktion bei Vorfällen

APP: Anwendungen und Dienste

SYS: IT-Systeme

IND: Industrielle IT – Produktion

NET: Netzverbindungen und Kommunikation

INF: Aspekte der infrastrukturellen Sicherheit

Ihre Stationen im Überblick.

1. Grundlage für Ihre Informationssicherheit
2. Organisation und Personal
3. Konzeptionelle Grundlagen für Datensicherheit
4. Die eigenständige IT-Administration? (sonst überspringen)
5. Grundlagen für den technischen Betrieb
6. Schaffung einer sicheren Infrastruktur
7. Planvolle Entwicklung und Aufbau eines Netzwerks
8. Sicherung einzelner Netzwerkkomponenten
9. Standard IT – Hardware
10. Standard IT – Software
11. Mobile IT – Hardware
12. Mobile IT – Software
13. Sonstige IT und Peripherie
14. a Aufbauende Konzepte
14. b Aufbauende Konzepte
15. Sichere Produktion
16. Die extern gehostete Website
17. Grundlagen der Detektion und Reaktion
18. Informationssicherheit und Rechtliches
19. Verschlüsselung und Software-Entwicklung
20. IT-Sicherheit in komplexen Einsatzszenarien
21. Professionelles Cyber-Vorfallmanagement

Tipp für die Praxis:
Kleine Ergänzung zur Bedienungshilfe „1, 2, 3 – So wird’s gemacht“ (S.4): Nutzen Sie die auf Seite 10 dargestellte Übersicht als Checkliste.

IT-Grundschutz-Bausteine kurz & bündig – Arbeitshilfen.

Jede Station Ihrer Route umfasst IT-Grundschutz-Bausteine. Die dort beschriebenen Basis-Anforderungen sind umzusetzen, wenn Sie die Grundsteine für mehr Informationssicherheit in Ihrem Betrieb legen möchten. Damit Sie Zeit und Arbeit sparen und nur das Wesentliche lesen und bearbeiten müssen, finden Sie in diesem Kapitel Arbeitshilfen zu jedem einzelnen Baustein.

Bedienungsanleitung.

Wo finde ich die Arbeitshilfen zu dem jeweiligen Baustein?
Gemäß IT-Grundschutz des BSI ist jeder Baustein einer von zehn verschiedenen „Schichten" zugeordnet und mit einem entsprechenden Kürzel aus Buchstaben und fortlaufenden Zahlen – wie „OPS.1.1.4 oder NET.3.2 – gekennzeichnet.
Für jede Schicht gibt es ein farbiges Symbol. Im Routenplaner sind die Arbeitshilfen für die Bausteine zur besseren Auffindbarkeit entsprechend farblich gestaltet und in einer Art Register fortlaufend sortiert.
Beispiel: Sie suchen die Arbeitshilfe zum Baustein „OPS.1.1.4 – Schutz vor Schadprogrammen". Sie finden diese im „Bausteine-Register" im Farbbereich gelb. Hinter dem Buchstabenkürzel, das für alle Bausteine der Schicht gleichlautend ist, sind die Zahlen fortlaufend nummeriert. Die gesuchte Arbeitshilfe befindet sich demnach zwischen OPS.1.1.3 und OPS.1.1.5.

Welche Informationen finde ich in der Arbeitshilfe?
Die einleitenden Sätze beinhalten gute Gründe, warum dieser Baustein für die Sicherheit Ihres Betriebs umzusetzen ist.

Unter „Priorisierung" ist die Empfehlung der Bearbeitungsreihenfolge gemäß IT-Grundschutz angegeben:
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.

Hinweise zum besseren Verständnis sollen dazu beitragen, einen Bezug zum Handwerksbetrieb herzustellen. Unter Anforderungen sind die Basis-Anforderungen in einem IT-Grundschutz-Baustein benannt, die es umzusetzen gilt. Empfohlen wird in einigen Fällen zudem, Standard-Anforderungen zu erfüllen.

Expertinnen und Experten aus Handwerksorganisationen haben zu einzelnen Basis-Anforderungen, gelegentlich auch zu Standard-Anforderungen, Empfehlungen oder vertiefende Hinweise zur Umsetzung erarbeitet. Die eigentlichen IT-Grundschutz-Bausteine und, soweit vorhanden, dazu passende Umsetzungshinweise des BSI sind über die QR-Codes per Verlinkung (siehe z. B. Seite 15) auf **www.bsi.bund.de/grundschutz** zugänglich. Weitere Online-Materialien, wie weiterführende Links, Videos, Podcasts etc. sind per QR-Code über die Website der Allianz für Cyber-Sicherheit des BSI zu finden.

Wie arbeite ich zeitsparend und zielgerichtet mit dem Original IT-Grundschutz-Baustein?
Der eigentliche IT-Grundschutz-Baustein ist auf der Website des BSI verortet und über die Arbeitshilfe per QR-Code erreichbar. Die Struktur ist immer gleich, die einzelnen Kapitel sind per „Sprungmarken" gezielt anzusteuern. Das spart viel Zeit, denn so gelangen Sie auf direktem Wege zu den für Sie relevanten Textpassagen.

Tipp für die Praxis – Routenplaner als Handbuch:
Sie mögen es lieber handfester? Legen Sie sich doch einen Arbeitsordner an. Denn der Routenplaner ist eine Loseblattsammlung. Sie können Ihre Route und die Arbeitshilfen ausdrucken und in einem Aktenordner in der für Sie richtigen Reihenfolge abheften. Das erleichtert das strukturierte Vorgehen. Ein Lesezeichen zeigt Ihren Arbeitsfortschritt an.

ISMS: Sicherheitsmanagement — ISMS

ORP: Organisation und Personal — ORP

CON: Konzeption und Vorgehensweisen — CON

OPS: Betrieb — OPS

DER: Detektion und Reaktion — DER

APP: Anwendungen — APP

SYS: IT-Systeme — SYS

IND: Industrielle IT — IND

NET: Netze und Kommunikation — NET

INF: Infrastruktur — INF

Basis-Anforderungen sind ein MUSS.

Jede Basis-Anforderung mit der Nummerierung A.1 bis A.n beinhaltet MUSS-Sätze. Betrachten Sie den Textabschnitt wie eine Checkliste: Jeder Satz ist eine eigenständige Anforderung, die zu betrachten ist. Ist sie bereits in Ihrem Betrieb erfüllt – Haken dran. Ist sie NICHT erfüllt, dann gibt es noch etwas zu tun.

Wie kann ich die Umsetzungshinweise zum IT-Grundschutz-Baustein nutzen?
Für viele IT-Grundschutz-Bausteine hat das BSI praktische Umsetzungshinweise herausgegeben. Die gute Nachricht: Sie müssen die umfassenden Ausführungen nicht in ihrer Gänze lesen, sondern nur das, was Sie in dem Moment wirklich interessiert.

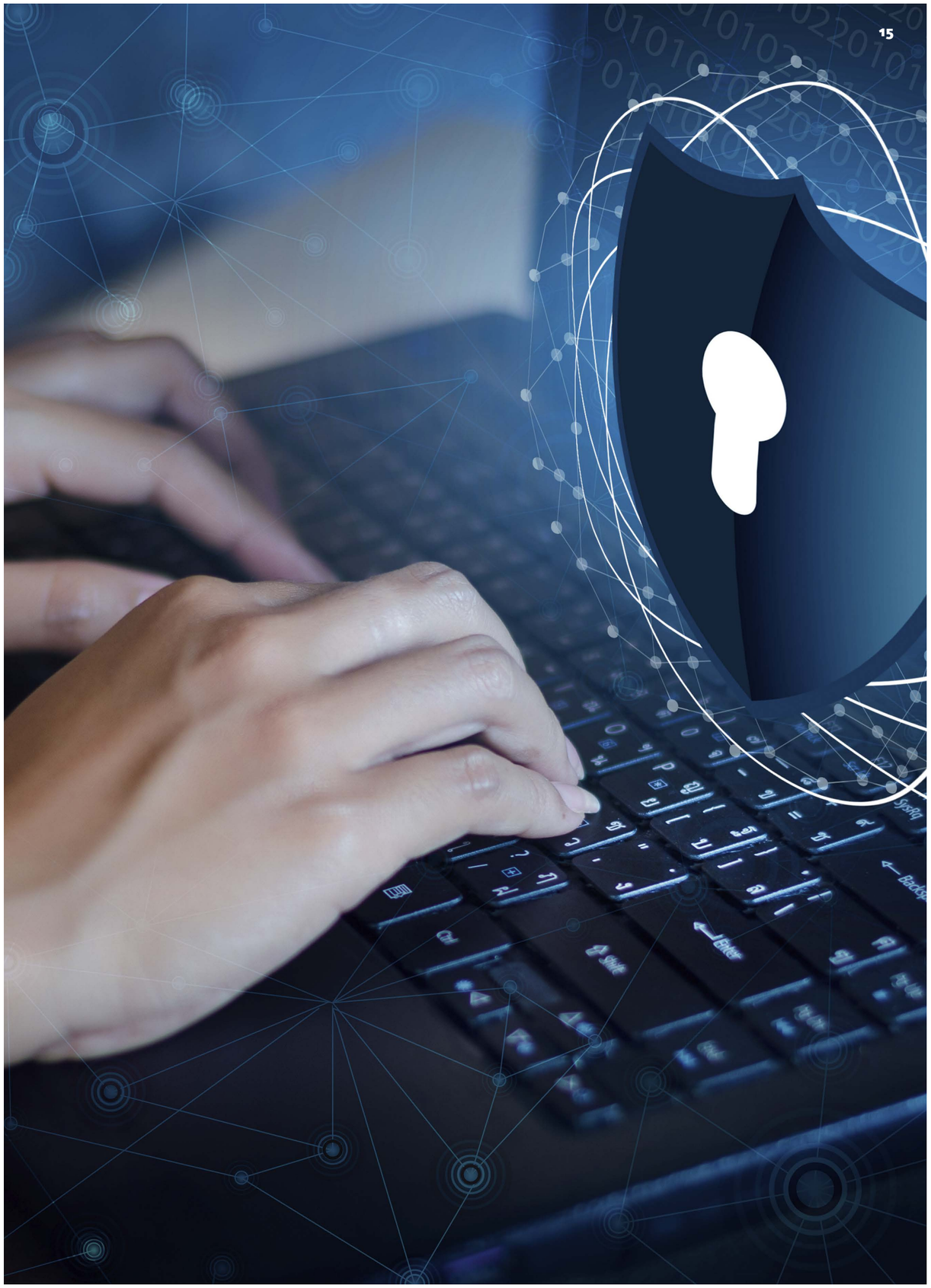
Der Trick: Aus A wird einfach M. Denn zu jeder Basis-Anforderung mit dem Kürzel A.Nummer im Baustein gibt es eine passende Maßnahme mit dem entsprechenden Kürzel M.Nummer in den Umsetzungshinweisen (sofern vorhanden). In der Online-Version erleichtern auch hier Sprungmarken den direkten Einstieg zu den „Basis-Maßnahmen".

Beispiel: Die Basis-Anforderung „OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen" im Baustein „OPS.1.1.4 – Schutz vor Schadprogrammen" korrespondiert mit der Maßnahme „OPS.1.1.4.M1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen" in den dazu passenden Umsetzungshinweisen.

Mir fehlt das notwendige technische Know-how zur Umsetzung eines Bausteins – was ist zu tun?
Wer kein handwerkliches Geschick hat, beauftragt entsprechende Fachleute. Wer über wenig Expertise in der IT verfügt, muss sich (punktuell) das Wissen zukaufen. Eine Checkliste für die Auswahl eines vertrauenswürdigen IT-Dienstleisters finden Sie unter **www.ihk.de/it-sicherheits-kriterien.** Auch die IT-Sicherheitsbotschafter in den Handwerkskammern können bei der Suche in Ihrer Region unterstützen. In jedem Fall werden sie mit den hier zugrunde liegenden Inhalten auch auf „Gespräche" mit IT-Dienstleistern vorbereitet.

Baustein-Lesehilfe.

Kapitel (Inhalt)	Leseempfehlung
1. Beschreibung (Einleitung, Zielsetzung, Abgrenzung zu anderen Bausteinen)	**KANN –** Bietet allgemeine Hintergrundinformationen und dient der Einordnung
2. Gefährdungslage	**KANN –** Überblick zu Risiken, die auftreten können, wenn die Anforderungen nicht umgesetzt werden
3. Anforderungen	
3.1 Basis-Anforderungen	**MUSS –** die Basis-Anforderungen sind die notwendigen Anforderungen für die Steigerung der Informationssicherheit in Ihrem Betrieb
3.2 Standard-Anforderungen	**EMPFOHLEN –** wenn z. B. in Arbeitshilfe entsprechend empfohlen oder **KANN –** wenn Standard-Absicherung angestrebt wird
3.3 Anforderungen bei erhöhtem Schutzbedarf	**KANN –** z. B. relevant, wenn dieser Baustein sich auf ein für Sie besonders schützenswertes Zielobjekt ihres Betriebs bezieht
4. Weiterführende Informationen (Literatur)	**KANN –** zur Vertiefung des Themas
5. Anlage: (Kreuzreferenztabelle zu elementaren Gefährdungen)	**KANN –** hier ist zu sehen, welche Risiken Sie mit der Umsetzung des Bausteins minimieren konnten



AdobeStock / © sarayut_sy

ISMS.1
Sicherheitsmanagement.

Durchdacht und wirksam – nur ein systematisches Managementsystem für die Informationssicherheit (ISMS) ist auf Dauer erfolgreich. Ein unzureichendes ISMS kann teuer werden, denn falsche Prioritäten führen zu falschen Entscheidungen – und kosten Zeit und Geld.

Minimieren Sie diese Risiken:

- Fehlende persönliche Verantwortung im Sicherheitsprozess
- Unzureichende strategische und konzeptionelle Vorgaben
- Unzureichende oder fehlgeleitete Investitionen
- Unzureichende Durchsetzbarkeit von Sicherheitsmaßnahmen
- Fehlende Aktualisierung im Sicherheitsprozess
- Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
- Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen
- Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

Priorisierung	R1
Hinweis zum besseren Verständnis	In der Regel ist in den meisten Handwerksunternehmen noch kein Sicherheitsmanagement vorhanden, ist aber durch die DSGVO zwingend erforderlich. Ein Handwerksbetrieb muss sich Gedanken machen, wie es solch ein Konzept erstellen und umsetzen kann und sollte dabei alle Beschäftigten mit einbeziehen.
Anforderungen	ISMS.1.A1 – A9; empfohlen: A10, A13, A17

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene
Zu ISMS.1.A1:
Unabhängig von ihrer Größe, sollten die hier beschrieben Prinzipien beachtet werden. Größere Betriebe sollten einen externen Dienstleister mit hinzuziehen bzw. das Thema evtl. auslagern (Outsourcing) – wobei die Verantwortung natürlich immer noch bei der Unternehmensleitung bleibt. Wichtig ist in diesem Zusammenhang auch das Verstehen von Datenschutz und Datensicherheit, das eine geht nicht ohne das andere – Datenschutz geht alle an und Datensicherheit obliegt der Verantwortung der Geschäftsleistung.

Erstellung einer Leitlinie zur Informationssicherheit
Zu ISMS.1.A3:
Der Prozess ist vergleichbar zur Einführung eines Qualitätsmanagementsystems (QM).

Benennung eines Informationssicherheitsbeauftragten
Zu ISMS.1.A4:
In der Regel wird die Aufgabe im kleinen Handwerksbetrieb selbst von dem Unternehmer bzw. der Unternehmerin übernommen. In größeren Handwerksunternehmen ab min. 20 Beschäftigten sollte eine Benennung realistisch sein.

Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
Zu ISMS.1.A6:
In größeren Handwerksunternehmen können alle Aspekte der Umsetzungshinweise wie Planung und Einrichtung der Informationssicherheitsorganisation, Funktion des Informationssicherheitsbeauftragten, Aufbau eines Informationssicherheitsmanagement-Teams, Auswahl des IS-Management-Teams, Benennung eines verantwortlichen Managers umgesetzt werden. Kleinere Betriebe können sich aber genauso Lösungen für die weiteren Aspekte erarbeiten: Definition von Zuständigkeiten (Funktionstrennung), Festlegung von Kommunikationswegen, Überprüfung der Informationssicherheitsorganisation, Anpassung und Verbesserung der Informationssicherheitsorganisation, Dokumentation.

Festlegung von Sicherheitsmaßnahmen
Zu ISMS.1.A7:
Diese Anforderungen sind für keinen Handwerksbetrieb vernachlässigbar, weil es nach DSGVO gefordert ist!

Integration der Mitarbeiter in den Sicherheitsprozess
Zu ISMS.1.A8:
Auch diese Anforderungen sind nicht vernachlässigbar, da auch hier der Querbezug zur DSGVO vorhanden ist. Alle Beschäftigten im Unternehmen müssen nach einem einheitlichen Sicherheitskonzept handeln, die Anforderungen der DSGVO kennen – dies muss alles dokumentiert werden, da die Unternehmerin bzw. der Unternehmer rechenschaftspflichtig ist. Hierzu zählen dann auch auch entsprechende Schulungen, siehe oben.

Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
Zu ISMS.1.A9:
Hier sollen die Beschäftigten über entsprechende Schulungen/Belehrungen im Unternehmen bei allen Prozessen mit einbezogen und entsprechend informiert werden. Diese Aspekte sind auch für die Parallelen zur DSGVO zu berücksichtigen und entsprechend anzuwenden (dokumentationspflichtig). Siehe die ausführliche Beschreibung in den Umsetzungshinweisen!

Erstellung eines Sicherheitskonzepts
Zu ISMS.1.A10:
Auch wenn diese Anforderung in der Liste der Standardanforderungen zu finden ist – nach DSGVO ist eine Pflicht, ein Sicherheitskonzept nachzuweisen. Der Umfang eines Sicherheitskonzeptes ist aber so angemessen zu bewerkstelligen, dass es auch für kleine Handwerksunternehmen passt.

Dokumentation des Sicherheitsprozesses
Zu ISMS.1.A13:
Aufgrund der Dokumentations- und Rechenschaftspflicht nach DSGVO muss der Unternehmer bzw. die Unternehmerin diese Anforderung entsprechend abarbeiten und nachweisen.

Abschließen von Versicherungen
Zu ISMS.1.A17:
Für Restrisiken ist es sinnvoll, eine (Cyber-)Versicherung abzuschließen, um eventuelle Schäden abzudecken.

ORP.1
Organisation.

Informationssicherheit ist „Chefsache“ – und die der Beschäftigten. Eine transparente Zuweisung von Verantwortlichkeiten und Befugnissen schafft Klarheit. Wichtig zu wissen: Auf diesem Baustein fußt die Umsetzung der Informationssicherheit durch andere Bausteine.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Regelungen
- Nicht beachtete Regelungen
- Fehlende, ungeeignete, inkompatible Betriebsmittel
- Unbefugter Zutritt zu schutzbedürftigen Räumen
- Unerlaubte Ausübung von Rechten
- Gefährdung durch Betriebsfremde
- Manipulation von Informationen und Geräten
- Zerstörung, Vandalismus, Sabotage
- Diebstahl und Verlust von Informationen und Geräten

Priorisierung	R1
Hinweis zum besseren Verständnis	Jedes Handwerksunternehmen muss eine Organisation haben, die das Zusammenspiel der verschiedenen Rollen und Einheiten mit den Geschäftsprozessen und Ressourcen im Betrieb steuert. Diese muss die Aufgaben zur Informationssicherheit umsetzen und mittragen!
Anforderungen	ORP.1.A1 – A5, empfohlen: A6 – A9

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Festlegung von Verantwortlichkeiten und Regelungen
Zu ORP.1.A1:
Die Regelungen für Informationssicherheit sollten mit denen für Datenschutz und Geheimschutz in geeigneter Weise zusammengeführt werden, damit sie von den Beschäftigten leichter adaptiert und besser wahrgenommen werden können. Wichtig ist auch, dass alle Regelungen zusammengenommen widerspruchsfrei sind.

Gibt es Vertraulichkeitsvereinbarungen?

Gibt es explizite Zuweisung der Verantwortlichkeiten und Befugnisse?

Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
Zu ORP.1.A2:
Um zu einer umfassenden Gesamtsicherheit zu gelangen, ist die Beteiligung aller Beschäftigten an der Umsetzung der erforderlichen Sicherheitsmaßnahmen erforderlich. Für alle Informationen, Geschäftsprozesse, Anwendungen und IT-Komponenten muss daher festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist.

Wurde der Schutzbedarf der Informationen, Geschäftsprozessen, Anwendungen und IT-Komponenten korrekt ermittelt?

Ist der Zugang bzw. Zugriff zu den Informationen, Anwendungen und IT-Komponenten geregelt?

Beaufsichtigung der Begleitung von Fremdpersonen
Zu ORP.1.A3:
Alle Beschäftigten sind darauf hinzuweisen, Betriebsfremde, die unbeaufsichtigt innerhalb des Unternehmens angetroffen werden, von diesem Moment an unter die eigene Obhut zu nehmen.

Wurden die Zugriffssperren bei den IT-Geräten aktiviert ?

Werden alle Arbeitsunterlagen verschlossen aufbewahrt?

Funktionstrennung zwischen operativen und kontrollierenden Aufgaben
Zu ORP.1.A4:
Operative und kontrollierende Funktionen müssen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu verhindern.

Ist die Datenerfassung und Zahlungsanordnungsbefugnis getrennt?

Ist die Revision und die Zahlungsanordnungsbefugnis getrennt?

Vergabe von Berechtigungen
Zu ORP.1.A5:
Auf den verschiedenen Ebenen MÜSSEN angemessene und praktikable Berechtigungen vergeben werden (z. B. für den Zutritt zu Räumen, Zugang zu IT-Systemen oder Zugriff auf Anwendungen).

Welche Zugriffsrechte erhalten Person im Rahmen ihrer Tätigkeiten?

Welche Personen erhalten in einem Notfall welche Zugriffsrechte?

ORP.2
Personal.

Mitarbeiterinnen und Mitarbeiter sind ein wesentlicher Erfolgsfaktor für die Informationssicherheit im Betrieb. „Steter Tropfen…!“ Einfach das Thema Informationssicherheit vom ersten bis zum letzten Arbeitstag der Beschäftigten mitberücksichtigen – so lassen sich viele Sicherheitsmaßnahmen wie selbstverständlich einspielen.

Minimieren Sie diese Risiken:

- Personalausfall
- Missbrauch von Berechtigungen
- Fehlende oder unzureichende Regelungen
- Unzureichende Kenntnis über Regelungen
- Fehlverhalten
- Social Engineering (Unberechtigter Zugang zu Informationen oder IT-Systemen durch soziale Handlungen der Opfer)
- Sorglosigkeit im Umgang mit Informationen
- Unberechtigte Verwendung eigener IT-Systeme
- Missbrauch sozialer Netzwerke
- Manipulation oder Zerstörung von Geräten, Informationen oder Software

Priorisierung	R1
Hinweis zum besseren Verständnis	Die Beschäftigten eines Handwerksunternehmens bilden die Grundlage für dessen Erfolg und sind ein wesentlicher Bestandteil der Informationssicherheit. Dieser Baustein beschäftigt sich in erster Linie mit den Sicherheitsmaßnahmen, die für und durch Beschäftigte im Handwerksbetrieb umgesetzt werden sollten. Darüber hinaus dürfen weitere Personengruppen, die mit den Informationen des Unternehmens in Berührung kommen, nicht vergessen werden. Hierzu zählen z.B. Beschäftigte von Dienstleistern (Reinigung, Wartung etc.) und Kunden bzw. Kundinnen.
Anforderungen	ORP.2.A1 – A5, empfohlen A.6 – A.10

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Geregelte Einarbeitung neuer Mitarbeiter
Zu ORP.2.A1:
Neue Beschäftigte müssen nicht nur in ihre neuen Aufgaben eingearbeitet werden, sondern auch über interne Regelungen, Gepflogenheiten und Verfahrensweisen informiert werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpersonen zu Fragen der Informationssicherheit nicht sowie die durchzuführenden Sicherheitsmaßnahmen und Sicherheitsstrategie, die das Unternehmen verfolgt.

Werden neue Beschäftigte für die Benutzung der für den Arbeitsplatz wesentlichen IT-Systeme und Anwendungen eingewiesen bzw. geschult?

Werden diese zur Sicherheitsstrategie des Unternehmens und die dafür verantwortliche Ansprechperson informiert?

Geregelte Verfahrensweise beim Weggang von Mitarbeitern
Zu ORP.2.A2:
Verlässt ein Mitarbeiter bzw. eine Mitarbeiterin den Handwerksbetrieb oder wechselt die Funktion, so ist u. a. folgendes zu beachten!

Erfolgt rechtzeitig eine Einweisung des Nachfolgers bzw. der Nachfolgerin?

Werden sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene Geräte (z. B. Tablet, Speichermedien etc.) zurückgefordert ?

Werden sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht?

Vertretungsregelungen
Zu ORP.2.A3:
Bei vorhersehbaren Personalausfall (Urlaub, Dienstreise etc.) und auch unvorhersehbaren Fällen (Krankheit, Unfall, Kündigung etc.), ist die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Eine jeweilige Vertretung sollte bestimmt werden. Der Bereich Informationsverarbeitung hat eine hohe Bedeutung, da häufig Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Beschäftigter für den Vertretungsfall nicht möglich ist.

Sind Vertretungsregelungen für die wesentlichen Geschäftsprozesse und Aufgaben vorhanden und werden diese regelmäßig aktualisiert?

Ist geregelt, dass der Vertreter bzw. die Vertreterin die erforderlichen Zugangs-, Zugriffs-und Zutrittsberechtigungen nur im Vertretungsfall erhält?

Ist bei nicht vorhandenen Vertretern geregelt, welche externen Kräfte für den Vertretungsfall eingesetzt werden können?

Regelungen für den Einsatz von Fremdpersonal
Zu ORP.2.A4:
Falls die entsprechenden personellen Ressourcen im Handwerksunternehmen nicht vorhanden sind, wird häufig auch auf externe Unterstützung zurückgegriffen. Bei längeren Zeiträumen kann es vorkommen, dass viele Beschäftigte schon nicht mehr genau wissen, ob es sich um eigene oder externe Kräfte handelt.

Werden Externe schriftlich auf die Einhaltung der geltenden Gesetze, Vorschriften und internen Regelungen verpflichtet?

Existieren auch für Externe Vertretungsregelungen?

Erfolgt bei Beendigung des Auftragsverhältnis eine geregelte Übergabe der Arbeitsergebnisse, der erhaltenen Unterlagen und Betriebsmittel?

Werden sämtliche eingerichteten Zugangs-, Zugriffs- und Zutrittsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht?

Gibt es einen Hinweis auf Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit?

Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal
Zu ORP.2.A5:
Häufig erhalten externe Mitarbeiter bzw. Mitarbeiterinnen für die Erfüllung ihrer Aufgaben Zugang zu vertraulichen Informationen oder erzielen Ergebnisse, die vertraulich behandelt werden müssen. In diesen Fällen müssen sie verpflichtet werden, diese entsprechend zu behandeln.

Werden mit Externen Vertraulichkeitsvereinbarungen abgeschlossen?

Hat der bzw. die Externe Zugang zu der organisationsinternen IT-Infrastruktur? Kennt bzw. unterzeichnet er oder sie auch die Sicherheitsrichtlinien für die Nutzung der jeweiligen IT-Systeme?

ORP.3 Sensibilisierung und Schulung.

Je besser die Beschäftigten, desto erfolgreicher der Betrieb – das gilt auch für die Informationssicherheit. Den Blick für Cyber-Risiken zu schärfen und die Umsetzung von Schutzmaßnahmen einzuüben, hält alle im Betrieb wach und schützt vor einer Vielzahl von Gefahren.

Minimieren Sie diese Risiken:

- Unzureichende Kenntnis über Regelungen
- Unzureichende Sensibilisierung für Informationssicherheit
- Wenig erfolgreiche Aktivitäten zur Sensibilisierung und Schulung
- Unzureichende Schulung der Mitarbeiter zu Sicherheitsfunktionalitäten
- Nicht erkannte Sicherheitsvorfälle
- Nichtbeachtung von Sicherheitsmaßnahmen
- Sorglosigkeit im Umgang mit Informationen
- Mangelhafte Akzeptanz von Informationssicherheit
- Social Engineering (Unberechtigter Zugang zu Informationen oder IT-Systemen durch soziale Handlungen der Opfer)

Priorisierung	R1
Hinweis zum besseren Verständnis	Um die Informationssicherheit innerhalb eines Handwerksunternehmens erfolgreich und effizient umzusetzen, sind die Beschäftigten ein notwendiger und bedeutender Erfolgsfaktor. Sie müssen die Sicherheitsziele des Unternehmens kennen sowie die Sicherheitsmaßnahmen verstehen und bereit sein, sie wirkungsvoll zu unterstützen. Dazu bedarf es einer permanenten Sensibilisierung und Schulung der Beschäftigten.
Anforderungen	ORP.3.A1 – A3; empfohlen: A6

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Sensibilisierung des Managements für Informationssicherheit
Zu ORP.3.A1:
Die Aufmerksamkeit der Beschäftigten zu Sicherheitsrisiken und damit verbunden Kosten, kann mit Hilfe von Berichten über Sicherheitsvorfälle erreicht werden. Dabei ist es wichtig auf die möglichen Auswirkungen der eigenen geschäftskritischen Prozesse hinzuweisen. Informationen zu rechtlichen Sicherheitsanforderungen (Datenschutz- und IT-Sicherheitsgesetz), zu Fachzeitschriften der Branche und der Besuch von Veranstaltungen, erhöhen Sensibilisierung.

Gibt es Informationen von Sicherheitsvorfällen z. B. zu Viren oder Hackerangriffen auf vergleichbare Betriebe aus dem nahen Umfeld?

Gibt es eine Auflistung von möglichen Sicherheitsrisiken auf die geschäftskritischen Prozesse des Unternehmens?

Gibt es Informationen zu den Regularien und Gesetze, die für die Branche zur Wirkung kommen können?

Ansprechpartner zu Sicherheitsfragen
Zu ORP.3.A2:
In jedem Handwerksbetrieb muss es eine Ansprechperson für Sicherheitsfragen geben. Es können eigene oder externe IT-Administratoren, IT-Anwendungsverantwortliche oder Informationssicherheitsbeauftragte sein.

Gibt es eigene oder externe Ansprechpersonen zu Sicherheitsfragen und sind diese allen Beschäftigten bekannt?

Wissen die Beschäftigten, dass jeder Verdacht eines Sicherheitsvorfalls zeitnah zu melden ist?

Gibt die Ansprechperson Informationen auch zur privaten Nutzung von IT-Systemen und -Anwendungen, wenn im Betrieb erlaubt?

Einweisung des Personals in den sicheren Umgang mit IT
Zu ORP.3.A3:
Viele Sicherheitsprobleme entstehen durch fehlerhafte Benutzung bzw. Konfiguration der IT. Deshalb müssen alle Beschäftigten und externe Benutzer bzw. Benutzerinnen in den sicheren Umgang mit den IT-Komponenten des Handwerkbetriebes eingewiesen und geschult werden, die für die Ausführung der Arbeitsaufgaben notwendig sind.

Gibt es eine Benutzerrichtlinie, die Regelungen für die allgemeine IT-Nutzung mit mindestens folgenden 10 Punkten enthalten?
- **Nutzung von Internet- und E-Mail-Diensten**
- **Durchführung von Datensicherungen**
- **Schutz vor Computer-Viren und anderer Schadsoftware**
- **Nutzungsverbot nicht freigegebener Software**
- **Einbringen von externen Daten in das eigene Haus (z. B. USB, Download oder E-Mail-Anhang)**
- **Umgang mit Passwörtern**
- **Hinweise zur sicheren Verwahrung und Aufstellung von IT-Systemen und Datenträgern**
- **Hinweis, dass keine IT-Systeme ohne ausdrückliche Erlaubnis benutzt werden dürfen**
- **Hinweis, dass nur diejenigen Mitarbeiter Informationen auf IT- Systemen ändern dürfen, die dazu autorisiert sind**
- **Hinweis, dass dienstliche IT-Systeme nur für dienstliche Zwecke eingesetzt werden dürfen, bzw. eine präzise Beschreibung möglicher Ausnahmen von dieser Regel, falls es sie gibt**

ORP.4 Identitäts- und Berechtigungsmanagement.

Kontrolle behalten: Nur wer dazu berechtigt ist, darf Zugang zu den Ressourcen des Betriebs haben. Eine systematische Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten ist in jedem Fall von Vorteil, denn fehlende Berechtigungen behindern die tägliche Arbeit und sinnlose Zugangsrechte eröffnen unnötige Sicherheitslücken.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Prozesse beim Identitäts- und Berechtigungsmanagement
- Fehlende zentrale Deaktivierungsmöglichkeit von Benutzerzugängen
- Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Priorisierung	R1
Hinweis zum besseren Verständnis	Auch Handwerksunternehmen haben Beschäftigte mit Benutzerzugängen zu diversen IT-Systemen, z. B. zu CNC-Maschinen, Produktiv-, Mess- oder Projektsystemen. Die Benutzerzugänge müssen über einem Identitäts- und Berechtigungsmanagement klar beschrieben werden. Eine ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten kann schnell zu gravierenden Sicherheitslücken führen und so ein Sicherheitsrisiko darstellen.
Anforderungen	ORP.4.A1 – A9; empfohlen: A11; A16; A19

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Regelung für die Einrichtung von Benutzern und Benutzergruppen
Zu ORP.4.A1:
Benutzer und Benutzergruppen im Handwerksbetrieb dürfen nur über eine separate administrative Rolle eingerichtet werden.

Gibt es Benutzer und Benutzergruppen?

Gibt es einen internen oder externen Administrator/Verantwortlichen für die Einrichtung von Benutzer und Benutzerkonten?

Ist geregelt, wie diese einzurichten sind?

Regelung für Einrichtung, Änderung und Entzug von Berechtigungen
Zu ORP.4.A2:
Benutzerkennungen und Berechtigungen dürfen nur anhand des tatsächlichen Bedarfs vergeben werden und müssen bei personellen Veränderungen wieder entfernt werden! Alle Berechtigungen müssen über eine separate administrative Rolle eingerichtet werden.

Gibt es Benutzergruppen und differenzierte Berechtigungen?

Werden bei personellen Veränderungen die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt ?

Gibt es einen internen oder externen Administrator/Verantwortlichen?

Dokumentation der zugelassenen Benutzer und Rechteprofile
Zu ORP.4.A3:
Eine Dokumentation der zugelassenen Benutzer und Rechteprofile MUSS vor unberechtigtem Zugriff geschützt werden.

Gibt es eine Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile?
Liegt sie in elektronischer Form vor und ist sie in das Datensicherungsverfahren mit einbezogen?

Aufgabenverteilung und Funktionstrennung
Zu ORP.4.A4:
Die für den IT-Einsatz relevanten Aufgaben und Funktionen müssen im Handwerksbetrieb definiert werden. Eine Trennung von nicht miteinander vereinbare Aufgaben und Funktionen muss vorliegen.

Gibt es nicht miteinander vereinbare Aufgaben und Funktionen?

Werden diese dokumentiert und umgesetzt?

Vergabe von Zutrittsberechtigungen
Zu ORP.4.A5:
Welche Zutrittsberechtigungen, an welche Personen im Rahmen ihrer Funktion vergeben werden, muss für den Handwerksbetrieb festgelegt werden.

Gibt es Zutrittsberechtigungen und wie werden diese umgesetzt?

Werden Zutrittsmittel wie z. B. Chipkarten verwendet?

Wird die Ausgabe bzw. der Entzug dokumentiert?

Regelung des Passwortgebrauchs
Zu ORP.4.A8:
Im Handwerksbetrieb MUSS der Passwortgebrauch verbindlich geregelt werden.

Werden entsprechend komplexe Passwörter vergeben und eingesetzt?

Werden die Passwörter geschützt und geheim gehalten?

Werden diese in angemessenen Zeitabständen geändert?

Identifikation und Authentisierung
Zu ORP.4.A9:
Der Zugang zu allen IT-Systemen und Diensten im Handwerksbetrieb MUSS durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer, Dienste oder IT-Systeme abgesichert sein.

Gibt es Möglichkeiten, über die die Authentizität eines Benutzers nachgewiesen werden kann, wie z. B. über
- **PINs (persönliche Identifikationsnummern)**
- **Passwörter**
- **Zugangskarten**
- **Biometrie?**
- **Werden für sicherheitskritische Anwendungsbereiche zwei Authentisierungstechniken kombiniert?**
- **Werden bei vorkonfigurierten IT-Produkten die Zugangskennungen geändert, z. B. bei der FRITZ!Box das WLAN Passwort?**

ORP.5 Compliance Management (Anforderungsmanagement).

Ob Datenschutz, eRechnung, GOBD, Haftung und vieles mehr – Gesetzliche und vertragliche Vorgaben kennen und umsetzen, gehört zum Betriebsalltag. Wer den Überblick behält, kann die Risiken besser minimieren.

Minimieren Sie diese Risiken:

- Verstoß gegen rechtliche Vorgaben
- Unzulässige Weitergabe von Informationen
- Unzureichende Identifikationsprüfung von Kommunikationspartnern
- Unbeabsichtigte Weitergabe interner Informationen

Priorisierung	R3
Hinweis zum besseren Verständnis	In jedem Handwerksbetrieb gibt es aus verschiedenen Richtungen gesetzliche, vertragliche, strukturelle und interne Richtlinien und Vorgaben, die beachtet werden müssen. Viele davon haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement. Weiterhin können Handwerksbetriebe externen Regelungen unterliegen und müssen die Einhaltung der Anforderungen (Compliance) sicherstellen und ein Compliance-Management-System betreiben, z. B. als Zulieferer oder Subunternehmen.
Anforderungen	ORP.5.A1 – A3; empfohlen: A6 – A7

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Identifikation der rechtlichen Rahmenbedingungen
Zu ORP.5.A1:
Bei der Verarbeitung von Informationen sind eine Vielzahl von gesetzlichen oder vertraglichen Rahmenbedingungen zu beachten. Typische Bereiche der Informationsverarbeitung, die besonderen gesetzlichen Regelungen unterliegen, sind z. B. der ordnungsgemäße Betrieb von IT-Systemen, inklusive Überwachung, Protokollierung und Auswertung, der Schutz von geistigem Eigentum und der Schutz personenbezogener Daten (siehe Datenschutzgrundverordnung (DSGVO)).

Wird die DSGVO im Betrieb umgesetzt?

Erfüllen alle installierten IT-Systeme (Hardware- und Software) die gültigen gesetzlichen Vorschriften?

Ist das vorhandene Wissen über die verschiedenen gesetzlichen, vertraglichen und sonstigen Vorgaben zentral zusammengetragen und, wenn nötig, wird es ergänzt?

Beachtung rechtlicher Rahmenbedingungen
Zu ORP.5.A2:
Führungskräfte, welche die rechtliche Verantwortung für den Handwerksbetrieb vor Ort tragen, müssen für die Identifizierung und Dokumentation der anzuwendenden gesetzlichen Vorschriften sorgen. Falls das erforderliche Wissen oder die nötigen Ressourcen nicht zur Verfügung stehen, sollte externe Rechtsberatung eingeholt werden.

Existieren für die einzelnen Bereiche des Unternehmens Unterlagen die den relevanten gesetzlichen und vertraglichen Vorgaben entsprechen?

Gibt es für die einzelnen Bereiche einen Verantwortlichen?

Gibt es einen externen oder internen Datenschutzbeauftragten?

Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
Zu ORP.5.A3:
Alle Beschäftigten müssen verpflichtet werden, einschlägige Gesetze (z. B. zum Datenschutz), Vorschriften und interne Regelungen einzuhalten. Die Verpflichtung sollte geeignet zentral dokumentiert werden. So ist z. B. eine Ablage von Verpflichtungserklärungen in der Personalakte einer Ablage bei den einzelnen Verantwortlichen, z. B. dem Datenschutzbeauftragten, vorzuziehen.

Gibt es eine zentrale Ablage von Verpflichtungserklärungen?

Werden alle Beschäftigten darauf hingewiesen, dass alle Arbeitsergebnisse und alle während der Arbeit erhaltenen Informationen ausschließlich zum internen und dienstlichen Gebrauch bestimmt sind?

Werden in Bezug auf die einschlägigen gesetzlichen Vorgaben regelmäßig geeignete Schulungsmaßnahmen angeboten?

28

CON.1
Kryptokonzept.

Wer sich dafür entscheidet, im Betrieb kryptografische Verfahren zur Verschlüsselung von Daten einzusetzen, sollte planvoll vorgehen, um Anwendungsfehler zu vermeiden.

Minimieren Sie diese Risiken:

- Unzureichendes Schlüsselmanagement bei Verschlüsselung
- Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptografischen Verfahren
- Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
- Software-Schwachstellen oder -Fehler in Kryptomodulen
- Ausfall eines Kryptomoduls
- Unsichere kryptografische Algorithmen oder Produkte
- Fehler in verschlüsselten Daten oder kryptografischen Schlüsseln
- Unautorisierte Nutzung eines Kryptomoduls
- Kompromittierung kryptografischer Schlüssel
- Gefälschte Zertifikate

Priorisierung	R3
Hinweis zum besseren Verständnis	Überblick über kryptografische Verfahren und Produkte, Kryptomodul für Basisschutz nicht relevant, Kryptografische Absicherung von z. B. E-Mail, Laptop etc. in anderen Bausteinen!
Anforderungen	CON.1.A1 – A2

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

CON

30

CON.2
Datenschutz.

In der Digitalisierung ist die technische Informationssicherheit eine wesentliche Voraussetzung für wirksamen Datenschutz. In diesem Baustein geht es um die Umsetzung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Rechte aus Sicht der Betroffenen (Standard-Datenschutzmodell – SDM).

Minimieren Sie diese Risiken:

- Missachtung von Datenschutz-Gesetzen oder Nutzung eines unvollständigen Risikomodells
- Festlegung eines zu niedrigen Schutzbedarfs

Priorisierung	R2
Hinweis zum besseren Verständnis	Der Baustein erläutert den u. a. den Zusammenhang zwischen Datenschutzanforderungen und IT-Grundschutz. Im Fokus steht das Standard-Datenschutzmodell (SDM) und eine daran orientierte datenschutzgerechte Ausgestaltung sowie Organisation von IT-Verfahren und Anwendungen. Bitte beachten: Rechtliches Thema, umfangreiche Vorgaben der EU-DSGVO berücksichtigen
Anforderungen	CON.2.A1

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

CON

CON.3 Datensicherungskonzept.

Ransomware? Kein Problem! Denn ist der aktuelle Datenbestand gesichert, lässt sich der IT-Betrieb kurzfristig wieder aufnehmen – das verkürzt Betriebsausfallzeiten. Die regelmäßige Datensicherung ist eine gute Voraussetzung dafür, die Aufbewahrungspflichten von Informationen jederzeit erfüllen zu können – auch bei Datenverlust.

Minimieren Sie diese Risiken:

- Fehlende Datensicherung
- Fehlende Wiederherstellungstests
- Ungeeignete Aufbewahrung der Backup-Datenträger
- Fehlende oder unzureichende Dokumentation
- Missachtung gesetzlicher Vorschriften
- Unsichere Cloud-Anbieter
- Ungenügende Speicherkapazitäten
- Unzureichendes Datensicherungskonzept

Priorisierung	R1
Hinweis zum besseren Verständnis	Ziele von Datensicherung gegenüber Archivierung verstehen (Anknüpfungspunkte zur Archivierung in OPS.1.2.2) Professionelle Datensicherung ist oft einzige Rettung bei Malware, vor allem bei Ransomware, aber auch bei versehentlichem Datenverlust!
Anforderungen	CON.3.A1 – A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erhebung der Einflussfaktoren der Datensicherung
Zu CON.3.A1:
Übersicht über Anwendungen und Daten (Umfang, Relevanz etc.) notwendig als Grundlage für ein korrektes Datensicherungskonzept, Konkretisierung / Erläuterung der sog. Einflussfaktoren

Festlegung der Verfahrensweise für die Datensicherung
Zu CON.3.A2:
Unbedingt Verantwortlichkeiten festlegen!
Wichtige Definitionen und Erläuterungen, praxisrelevant!

Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung
Zu CON.3.A3:
Juristischer Rat evtl. zielführend

Erstellung eines Minimaldatensicherungskonzeptes
Zu CON.3.A4:
Immer up to date halten! Praxisbeispiel in Umsetzungshinweisen beachten.

Regelmäßige Datensicherung
Zu CON.3.A5:
Hier werden konkrete Praxisbeispiele angegeben!

34

CON.4 Auswahl und Einsatz von Standardsoftware.

Installieren und einfach loslegen? Besser nicht! Wer mit Standard-Programmen arbeitet, sollte sicher gehen, dass von Beginn an die damit verarbeiteten Informationen geschützt werden.

Minimieren Sie diese Risiken:

- Fehlende Anpassung der Standardsoftware an den Bedarf des Betriebs
- Offenlegung schützenswerter Informationen durch fehlerhafte Konfiguration
- Bezug von Standardsoftware und Updates aus unzuverlässiger Quelle
- Manipulation von Daten durch Benutzer und Benutzerinnen
- Software-Schwachstellen in Standardsoftware
- Einsatz nicht-lizenzierter Standardsoftware
- Unerlaubtes Ausüben von Rechten in Standardsoftware
- Datenverlust durch fehlerhafte Nutzung von Standardsoftware

Priorisierung	R2
Hinweis zum besseren Verständnis	Bei der täglichen Arbeit in Handwerksbetrieben wird ein Großteil von Aufgaben mit entsprechender Software erledigt. In der Regel kommen dabei Standardsoftware-lösungen wie Office-Anwendungen oder Branchenprogramme zum Einsatz. Die universelle Nutzbarkeit von Software über Gewerke hinweg bis hin zum privaten Einsatz zeigt die Stärke der Software. Allerdings birgt diese universelle Nutzbarkeit auch Gefahren, wie z. B. fehlerhafte Konfiguration und dadurch eventuelle Offen-legung von sensiblen Informationen, nicht erkannter Softwareschwachstellen oder fehlerhafte Rechtevergaben in der Software.
Anforderungen	CON.4.A1 – A3

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Sicherstellen der Integrität von Standardsoftware
Zu CON.4.A1:
Achten Sie vor der Installation der Software darauf, dass es sich um Originalsoftware handelt. Diese sollte möglichst von Originaldatenträgern oder aus vertrauenswürdigen Download-Quellen stammen. Bevor die Software installiert wird, muss diese durch ein Antivirenprogramm auf mögliche Schadsoftware geprüft werden. Achten Sie bei der Vergabe von Nutzerrechten auf ihren Rechnern, dass das Recht zur Installation von Software ausschließlich Administratoren vorbehalten ist. Hierdurch wird verhindert, dass unbewusst oder bewusst Mitarbeiter ungeprüfte Software installieren können. Fertigen Sie nach der Installation Sicherheitskopien der installierten Software an.

Entwicklung der Installationsanweisung für Standardsoftware
Zu CON.4.A2:
Bei der Installation von Software ist es wichtig zu wissen, welche Funktionen für den Betrieb benötigt werden! Gewisse Funktionen werden häufig nicht deaktiviert, obwohl diese nicht benötigt werden. Das heißt: Machen Sie sich mit der Software vertraut, überprüfen Sie welche Funktionen Sie tatsächlich benötigen und machen Sie sich einen Plan, in dem festgelegt ist, durch wen die Software-Installation vorgenommen wird. Sollten Sie das nicht alleine schaffen, nutzen Sie die Hilfe eines Dienstleisters.

Sichere Installation und Konfiguration von Standardsoftware
Zu CON.4.A3:
Je mehr Funktionen ein Programm besitzt, umso höher ist die Wahrscheinlichkeit, dass gerade durch diese Funktionen Sicherheitslücken entstehen können. Durch gute Planung wissen Sie inzwischen wer diese Software installiert und welche Funktionen Sie für Ihren Betrieb benötigen. Setzen Sie diesen Plan bei der Installation und Konfiguration konsequent um! Sollten Sie Hilfe benötigen, fragen und nutzen Sie dafür spezialisierte IT-Dienstleister!

Ganz wichtig: Bevor Sie eine neue Software installieren, fertigen Sie unbedingt Datensicherungen/Backups des Systems an. Hierdurch können Sie den ursprünglichen Zustand Ihres Systems wieder herstellen, falls etwas mit der Installation schief läuft.
Läuft ihr Programm nach der Installation fehlerfrei, dann erstellen Sie nach der Installation erneut eine Datensicherung. Damit haben Sie ein arbeitsfähiges Backup Ihres Systems, falls doch irgendetwas schiefgehen sollte.

36

CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen.

Individuell konzipierte Software-Lösungen haben den Vorteil, dass Informationssicherheit von Beginn an mitberücksichtigt werden kann – bei der Erstellung, der Installation, der Schulung von Anwenderinnen und Anwendern sowie dem fortlaufenden Betrieb.

Minimieren Sie diese Risiken:

- Verlust der Vertraulichkeit oder Integrität in Fachanwendungen
- Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
- Unzugängliche vertragliche Regelungen mit einem externen Dienstleister
- Software-Konzeptionsfehler
- Software-Schwachstellen
- Undokumentierte Funktionen
- Fehlende oder unzureichende Sicherheitsmaßnamen in Anwendungen

Priorisierung	R3
Hinweis zum besseren Verständnis	Fachanwendungen im Handwerk sind komplexe Anwendungen, die für individuelle und spezifische fachliche Aufgaben konzipiert sind sowie in der Regel nicht als Standardlösungen gekauft und eingesetzt werden. Stattdessen können Basislösungen von Handwerksbetrieben für den individuellen Einsatzzweck selbst angepasst, vollständig durch Dritte oder dem Handwerksbetrieb selbst entwickelt werden. Zu diesen Fachanwendungen gehören beispielsweise Personalverwaltungssoftware, Verfahren zur Verwaltung von Sozial- oder Arbeitszeitdaten, aber auch CNC-Steuerungen für komplexe Anforderungen und integrierte CAM-Software für alle CNC-Anwendungen. Für die Gebäudeautomation (Smart Home) lassen sich mittels KNX Beleuchtung, Beschattung, Heizung, Klima, Lüftung, Alarm, Information, Fernzugriff (über Smartphone, Telefon, Internet), zentrales Steuern des Hauses und weiteres integriert zusammenschalten. Eine sorgfältige Planung von Sicherheitsmaßnahmen vor Auswahl und Einsatz einer Anwendung ist wesentlich für das Sicherheitsniveau, da Fehler in der Planung wie z. B. fehlende Sicherheitsfunktionen im laufenden Betrieb nicht oder nur mit sehr hohen Zusatzaufwänden ausgeglichen werden können.
Anforderungen	CON.5.A1– A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Festlegung benötigter Sicherheitsfunktionen der Fachanwendung
Zu CON.5.A1:
Bevor eine neue Anwendung geplant und projektiert wird, sollten die Rahmenbedingungen für den Einsatz geklärt werden, beispielsweise welche Geschäftsprozesse die Anwendung unterstützen soll, welche Informationen, mit welchem Schutzbedarf mit ihr verarbeitet werden sollen, wer auf welche Teile der Anwendung zugreifen darf bzw. muss und welche IT-Komponenten für den Betrieb der Anwendung benötigt werden, wie z. B. Hardware-Plattform, Betriebssysteme, Datenbanken.

Diskutieren Sie bei der Planung der neuen Anwendung über mögliche Bedrohungen und Risiken?

Führen Sie eine Analyse durch, um potenzielle Angriffe und andere Risiken für Vertraulichkeit, Integrität und Verfügbarkeit der neuen Anwendung frühzeitig zu identifizieren?

Test und Freigabe von Fachanwendungen
Zu CON.5.A2:
Für einen geordneten Betriebsübergang einer Anwendung und bei wesentlichen Änderungen, ist bei Test und Freigabe ein geeignetes Vorgehen zu wählen. Dabei sind, wenn vorhanden, die folgenden vier Ebenen zu berücksichtigen:

- Fachkompetenz (Vertreten durch Fachverantwortliche)
- IT-Betrieb (Vertreten durch den IT-Leiter)
- Informationssicherheit (Vertreten durch den IT-Sicherheitsbeauftragten)
- Datenschutz (Vertreten durch den Datenschutzbeauftragten)

Wird vorher geprüft, ob die Anwendung in die IT-Infrastruktur und in die IT-Betriebsabläufe integriert werden kann?

Wenn notwendig, wird eine datenschutzrechtliche Freigabe eingeholt?

Werden die Ergebnisse der Tests dokumentiert und bewertet?

Sichere Installation einer Fachanwendung
Zu CON.5.A3:
Nach erfolgreichem Abschluss der Tests und der Freigabe der Anwendung, ist die Installation der Anwendung zu planen. Hierbei ist es zweckmäßig eine Installationsanweisung zu erstellen (siehe Baustein CON.4). Um eine Neuinstallation der Anwendung zu vereinfachen, sollte die Installation einer Anwendung mit allen ihren Schritten dokumentiert werden.

Wer installiert die Anwendung – externer oder interner IT-Dienstleister?
Werden alle Schritten der Installation dokumentiert, um eine spätere Neuinstallation der Anwendung zu vereinfachen?

Heranführen von Nutzerinnen und Nutzern an die Anwendung
Zu CON.5.A4:
Um eine geordnete Nutzung der Anwendung sicherzustellen und um Schäden durch unsachgemäßen Umgang zu vermeiden, muss der Fachverantwortliche dafür Sorge tragen, dass Benutzer und Administratoren an die korrekte Nutzung und Administration der Anwendung (einschließlich der Sicherheitsfunktionen) über Schulungen, Einweisungen, Handbücher und weiteres herangeführt werden.

Gibt es Schulungen und Einweisungen für die Beschäftigten?

Erhalten die Beschäftrigten zur Einarbeitung in die Anwendung ausreichende Möglichkeiten und Zeit?

Existieren Handbücher und Online-Hilfen?

Sicherer Betrieb einer Fachanwendung
Zu CON.5.A5:
Während des Betriebes einer Anwendung oder eines Fachverfahrens sollte sichergestellt sein, dass die Benutzer ausreichend bei Fragen und Problemen unterstützt werden. Ein wichtiger Aspekt der Sicherheit einer Anwendung im laufenden Betrieb ist die geeignete Vergabe von Zugriffsrechten und die stets aktuelle Dokumentation von zugelassenen Benutzern und Rechteprofilen (siehe ORP.4).

Gibt es Schulungen und Einweisungen für die Beschäftigten?

Erhalten die Beschäftigten zur Einarbeitung in die Anwendung ausreichende Möglichkeiten und Zeit?

Existieren Handbücher und Online-Hilfen?

38

CON.6
Löschen und Vernichten.

Damit Informationen nicht in falsche Hände geraten, ist es unerlässlich, Daten und Datenträger vollständig und zuverlässig zu löschen oder zu vernichten.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichend dokumentierte Regelungen beim Löschen und Vernichten
- Vertraulichkeitsverlust durch Restinformationen auf Datenträgern
- Unstrukturierte Datenhaltung
- Vertraulichkeitsverlust durch Auslagerungs- und temporäre Dateien
- Ungeeignete Entsorgung der Datenträger und Dokumente

Priorisierung	R1
Hinweis zum besseren Verständnis	Hinweis auf CON.3 Datensicherungskonzept, OPS.1.2.2 Archivierung, OPS.1.2.3 Informations- und Datenträgeraustausch und OPS.1.2.6 Verkauf und Aussonderung von IT berücksichtigen.
Anforderungen	CON.6.A1– A2; empfohlen A3 - A8

Online-Material.

Baustein

Arbeitshilfen

CON

Empfehlungen für einzelne Anforderungen.

Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen
Zu CON.6.A1:
Grundlage jeder weiteren Betrachtung! Regelung und Zuständigkeiten festlegen. Die Regelung in Form einer Richtlinie (CON.6.A8) wird darüber hinaus empfohlen.

OPS.1.1.2 Ordnungsgemäße IT-Administration.

Die ordnungsgemäße und systematische Systemadministration ist eine wichtige Voraussetzung für Informationssicherheit im Betrieb. System-Administratoren verfügen über weitreichende Eingriffs- und Zugangsmöglichkeiten in Bezug auf die IT. Dadurch ergeben sich besondere Gefährdungen für den Betrieb.

Minimieren Sie diese Risiken:

- Versäumnisse durch ungeregelte Zuständigkeiten
- Personalausfall von Kernkompetenzträgern
- Missbrauch von administrativen Berechtigungen
- Erleichterung von Angriffen
- Störung des Betriebs
- Fehlende Aufklärungsmöglichkeiten für Vorfälle

Priorisierung	R1
Hinweis zum besseren Verständnis	Die fortlaufende Administration von IT-Systemen und -Komponenten ist für jeden Handwerksbetrieb mittlerweile grundlegend. Ziel dieses Bausteins ist aufzuzeigen, wie mit einer ordnungsgemäßen IT-Administration die Sicherheitsanforderungen von IT-Anwendungen, IT-Systemen und Netzen erfüllt werden können. Mit der Umsetzung dieses Bausteins sorgt das Handwerksunternehmen dafür, dass die für die Sicherheit der Informations- und Kommunikationstechnik erforderlichen Tätigkeiten in der Systemadministration ordnungsgemäß und systematisch durchgeführt werden.
Anforderungen	OPS.1.1.2.A1 – A6; empfohlen A7 – A19

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Vertretungsregelungen und Notfallvorsorge
Zu OPS.1.1.2.A2:
Die Vertretungsregelung ist ein großes Problem bei kleinen Unternehmen und sollten dringend gefunden und umgesetzt werden.

Geregelte Einstellung von IT-Administratoren
Zu OPS.1.1.2.A3:
Aufgaben und Zuständigkeiten müssen schriftlich festgelegt werden, z. B. in einer Stellenbeschreibung (Aufgaben und Kompetenzen). Können die Aufgaben nicht im Betrieb verteilt werden, sollte eine externe Firma beauftragt werden.

Beendigung der Tätigkeit als IT-Administrator
Zu OPS.1.1.2.A4:
Bitte beachten: Auch bei Betriebsaufgabe bzw. -übergabe müssen alle notwendigen Unterlagen, Materialien und Beschreibungen mit den entspr. Rechten bezüglich der IT an die Nachfolger bzw. Nachfolgerinnen übergeben werden.

Administrationskennungen
Zu OPS.1.1.2.A5:
Hier die Bausteine ISMS.1. und ORP.2 beachten

Schutz administrativer Kennungen
Zu OPS.1.1.2.A6:
Bitte beachten: Geeignete Authentisierungsmechanismen einführen, siehe Datensicherung und Datenarchivierung

OPS.1.1.3 Patch- und Änderungsmanagement.

Lieber lückenlos! Schwachstellen in Büroanwendungen und anderen Programmen sind nach wie vor eines der Haupteinfallstore für Cyber-Angriffe. Diese Sicherheitslücken lassen sich schließen, indem die von den Herstellern bereitgestellten Sicherheitsupdates, auch „Patches“ genannt, so rasch wie möglich eingespielt werden.

Minimieren Sie diese Risiken:

- Mangelhaft festgelegte Verantwortlichkeiten
- Mangelhafte Kommunikation beim Änderungsmanagement
- Mangelhafte Berücksichtigung von Geschäftsprozessen
- Unzureichende Ressourcen beim Patch- und Änderungsmanagement
- Probleme bei der automatisierten Verteilung von Patches und Änderungen
- Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement
- Mangelhafte Berücksichtigung von mobilen Endgeräten
- Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement
- Fehleinschätzung der Relevanz von Patches und Änderungen
- Manipulation von Daten und Werkzeugen beim Änderungsmanagement

Priorisierung	R1
Hinweis zum besseren Verständnis	In diesem Baustein wird aufgezeigt, wie ein funktionierendes Patch- und Änderungsmanagement in einem KMU aufgebaut und wie der entsprechende Prozess kontrolliert und optimiert werden kann. Aufgabe des Änderungsmanagements ist es, verändernde Eingriffe in Anwendungen (Branchensoftware etc.), Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt schnell zu Sicherheitslücken in den einzelnen Komponenten und damit zu möglichen Angriffspunkten in der IT-Infrastruktur.
Anforderungen	OPS.1.1.3.A1 – A3

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Konzept für das Patch- und Änderungsmanagement
Zu OPS.1.1.3.A1:
Es sind für einen Administrator eines Handwerksunternehmens oder für einen Dienstleister eines Handwerksunternehmens unbedingt die ausführlichen Umsetzungshinweise in OPS1.1.3.M1 zu beachten. Das sollte man auch in seinem IT-Sicherheitskonzept beachten und schriftlich fixieren.

Festlegung der Verantwortlichkeiten
Zu OPS.1.1.3.A2:
Auch hier gilt wie so oft, dass der Handwerksmeister in den meisten Fällen selber verantwortlich ist. Die Umsetzungshinweise sollten an den IT-Fachmann (Fachfirma) gegeben werden.

Konfiguration von Autoupdate-Mechanismen
Zu OPS.1.1.3.A3:
In den meisten Handwerksbetrieben sind automatische Updates voreingestellt. Was zu empfehlen ist.

OPS.1.1.4 Schutz vor Schadprogrammen.

„Achtung Viren - nicht anstecken!“ Schadprogramme („Viren“) eröffnen Angreifern vielfältige Möglichkeiten von Spionage über Erpressung und Sabotage bis zur Zerstörung von Geräten. Sorgsam ausgewählte Viren-Schutzprogramme minimieren die Gefährdungen. In diesem Baustein gibt es eine gute Übersicht zu den verschiedenen Angriffsmethoden (siehe unter Gefährdungslage).

Minimieren Sie diese Risiken:

- Softwareschwachstellen und Drive-by-Downloads (automatisierte Ausnutzung von Sicherheitslücken)
- Erpressung durch Ransomware
- Gezielte Angriffe und Social Engineering
- Infektionen durch mobile Datenträger und andere USB-Geräte
- Botnetze
- Infektion von Produktionssystemen und IoT-Geräten

Priorisierung	R1
Hinweis zum besseren Verständnis	Dieser Baustein beschreibt die Vorgehensweise, einen Schutz gegen Schadprogramme zu erstellen und umzusetzen, um einen Handwerksbetrieb effektiv gegen Schadprogramme zu schützen. Standardmäßig ist hier die Rede vom Gebrauch einer Firewall im IT System und die Verwendung von aktuellen Virenscannern.
Anforderungen	OPS.1.1.4.A1 – A7

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erstellung eines Konzepts für den Schutz vor Schadprogrammen
Zu OPS.1.1.4.A1:
Wichtig für jedes Unternehmen. In der Regel sind es aber nur normale Antivirenprogramme.
Auch wichtig für das IT-Sicherheitskonzept nach DSGVO

Nutzung systemspezifischer Schutzmechanismen
Zu OPS.1.1.4.A2:
Wichtig für die IT des Unternehmens im Handwerk sind: Wie oben – Anwendung von Virensoftware und Firewall-Einstellungen. Nicht zu vernachlässigen sind die WLAN-Anwendung im Unternehmen

Auswahl eines Viren-Schutzprogrammes für Gateways und IT-Systeme zum Datenaustausch
Zu OPS.1.1.4.A4:
Beachtung WLAN!

Betrieb von Viren-Schutzprogrammen
Zu OPS.1.1.4.A5:
Der Handwerksbetrieb sollte immer auf die Aktualität der Viren-Schutzprogramme achten, aber auch alle seine Beschäftigten, welche mit eigenen autarken IT-Systemen arbeiten. Das bedarf genauer Unterweisung bzw. Anweisung

OPS.1.1.5 Protokollierung.

Protokolle für mehr Kontrolle - In einer Vielzahl von IT-Systemen und Anwendungen werden Protokollierungsdaten generiert. Sie sind wichtig für das Erkennen von Hard- und Softwareproblemen, Ressourcenengpässen, Sicherheitsproblemen und Angriffen. Im Falle eines Vorfalls: Nach einem Angriff auf IT-Systeme lassen sich durch forensische Untersuchungen mit Hilfe von Protokollierungsdaten Beweise sichern.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Protokollierung
- Fehlerhafte Auswahl von relevanten Protokollierungsdaten
- Fehlende Zeitsynchronisation bei der Protokollierung
- Fehlplanung bei der Protokollierung
- Vertraulichkeits- und Integritätsverlust von Protokollierungsdaten
- Falsch konfigurierte Protokollierung
- Ausfall von Datenquellen
- Ungenügend dimensionierte Protokollierungsinfrastruktur

Priorisierung	R1
Hinweis zum besseren Verständnis	Dieser Baustein beschreibt für einen verlässlichen IT-Betrieb im Handwerksunternehmen das betriebs- und sicherheitsrelevante protokollieren von Ereignissen für bestimmte IT-Systeme und Software-Anwendungen. Eine Protokollierung sollte im Handwerksunternehmen eingesetzt werden, um Hard- und Softwareprobleme sowie Ressourcenengpässe zeitnah entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Dienste können anhand von Protokollierungsdaten nachvollzogen werden. Der Baustein enthält ebenfalls Anforderungen, mit denen die Protokollierung möglichst aller sicherheitsrelevanten Ereignisse umgesetzt werden kann. Ziel ist es, alle hierfür relevanten Daten sicher zu erheben, zu speichern und geeignet für die Auswertung bereitzustellen sowie deren ordnungsgemäße Entsorgung sicherzustellen.
Anforderungen	OPS.1.1.5.A1 – A5

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Konfiguration der Protokollierung auf System- und Netzebene
Zu OPS.1.1.5.A3:
Es sind dabei die Pflichten nach DSGVO nicht zu vernachlässigen!

OPS

OPS.1.1.6 Software-Tests und -Freigaben.

Vertrauen ist gut, testen ist besser - Nur eine fehlerfreie Software kann für eine ausreichende Informationssicherheit im Betrieb sorgen.

Minimieren Sie diese Risiken:

- Unvollständige Umsetzung von Anforderungen des Auftraggebers
- Unzureichende Schulung der Entwickler und Software-Tester
- Software-Test mit Produktivdaten
- Fehlendes oder unzureichendes Testverfahren
- Fehlendes oder unzureichendes Freigabeverfahren
- Fehlende oder unzureichende Dokumentation der Tests und Testergebnisse
- Fehlende oder unzureichende Dokumentation der Freigabekriterien

Priorisierung	R1
Hinweis zum besseren Verständnis	Mit der Umsetzung dieses Bausteins sorgt das Handwerksunternehmen dafür, dass eingesetzte Software den technischen und organisatorischen Anforderungen sowie dem vorliegenden Schutzbedarf des gesamten Unternehmens oder einzelner Abteilungen/Filialen entspricht. Ein wesentlicher Teilaspekt ist dabei, dass sicherheitskritische Software auf bestehende Schwachstellen systematisch und methodisch überprüft wird.
Anforderungen	OPS.1.1.6.A1 – A5

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Durchführung nicht-funktionaler Software-Tests
Zu OPS.1.1.6.A5:
Es sollten funktionale Tests durchgeführt werden. Es ist in der Regel der Knackpunkt im Handwerksunternehmen, dass einige Funktionen nicht so funktionieren, wie sie vorher beschrieben wurden. Auch im Sinne der DSGVO müssen die Software-Programme angepasst werden, sowohl dem ISMS entsprechen als auch dem Datenschutz und dessen Dokumentationspflicht/ Rechenschaftspflicht.

OPS

OPS.1.2.3 Informations- und Datenträgeraustausch.

Sichere Kommunikation – analog wie digital – ist die Basis für gute Beziehungen mit Kunden, Kundinnen, Lieferanten und Dienstleistern. Das Einhalten von Regeln sorgt für Informationssicherheit bei persönlichen Treffen, im Umgang mit Datenträgern (z. B. Aktenordner oder USB-Sticks) als Transportmedien, aber auch für den Informationsaustausch bei oder über IT-Netze.

Minimieren Sie diese Risiken:

- Defekte Datenträger
- Nicht fristgerecht verfügbare Datenträger
- Ungeregelte Weitergabe von Informationen oder Datenträgern
- Unzureichendes Schlüsselmanagement bei Verschlüsselung
- Verlust von Datenträgern beim Versand
- Weitergabe falscher oder interner Informationen
- Diebstahl, Manipulation oder Zerstörung von Datenträgern
- Schadprogramme in übertragenen Dateien oder auf Datenträgern
- Unberechtigtes Kopieren von Informationen oder der Datenträger

Priorisierung	R3
Hinweis zum besseren Verständnis	Dieser Baustein ist bei jedem elektronischen oder verbalen Austausch sowie dem Austausch von Informationen in Papierform, einmal heranzuziehen. Hierzu zählen Angebote, Zeichnungen, Leistungsverzeichnisse von Architekten und Ausschreibungsplattformen sowie der Datenaustausch im Rahmen von Building Information Modelling (BIM). Der Baustein ist ebenso bei der Nutzung mobiler Datenträger zu berücksichtigen (auch bei USB-Messegeschenken) und NAS-Systemen zur Datensicherung.
Anforderungen	OPS.1.2.3.A1 – A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Festlegung zulässiger Kommunikationspartner
Zu OPS.1.2.3.A1:
Verteiler und berechtigte Empfänger müssen festgelegt werden. Beim E-Mail und Faxversand ist besonders auf den Empfängerkreis und die Optionen An:, CC: und BCC: zu achten.

Regelung des Informationsaustausches
Zu OPS.1.2.3.A2:
Interne Informationen (Projektplanungen, Ideenskizzen auf Papier etc.) sind angemessen zu schützen und dürfen nicht in öffentlichen Verkehrsmitteln oder im Restaurant diskutiert werden. Vor dem Versand müssen Firmenzugehörigkeit, Post-, E-Mail-Adressen oder Faxnummern überprüft werden. Nach Klärung des Schutzbedarfs dürfen Daten/Informationen nur zu dem Zwecke genutzt werden, für den sie empfangen oder weitergeben wurden (DSGVO). Dazu müssen Beschäftigte z. B. im Rahmen einer Betriebsversammlung ausreichend sensibilisiert werden.

Unterweisung des Personals zum Informationsaustausch
Zu OPS.1.2.3.A3:
Personen müssen sensibilisiert werden, welche Informationen wann, wo und wie weitergegeben werden dürfen. Zum Schutz vor Schadprogrammen in E-Mail-Anhängen sollte beim Absender nachgefragt werden, ob dieser die Daten wirklich verschickt hat. Dies empfiehlt sich insbesondere, wenn vom Absender keine E-Mail erwartet wird oder Zweifel an der Authentizität der E-Mail besteht.

Schutz vor Schadsoftware
Zu OPS.1.2.3.A4:
Digitale Daten wie z. B. E-Mail-Anhänge und Daten auf Datenträgern (USB-Stick, CD/DVDs) müssen vom Absender und Empfänger auf Schadsoftware überprüft werden.

Verlustmeldung
Zu OPS.1.2.3.A5:
Bei Verlust oder Manipulationsverdacht ist der IT-Verantwortliche umgehend zu informieren.

OPS

OPS.1.2.4 Telearbeit.

Geräte, die außerhalb der Betriebsräume und des Betriebsgeländes im Einsatz sind, bieten für Cyber-Attacken eine zusätzliche und oft leichte Angriffsfläche. Es gilt, Risiken wie Spionage, unbefugtes Eindringen in IT-Systeme oder auch die fehlerhafte Nutzung von Geräten zu minimieren. Regeln für Telearbeit tragen zu einer reibungslosen Zusammenarbeit trotz räumlicher Distanz bei.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Regelungen für den Telearbeitsplatz
- Fehlende oder unzureichende Schulung der Beschäftigten in Telearbeit
- Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners
- Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Beschäftigten in Telearbeit
- Mangelhafte Einbindung Beschäftigten in Telearbeit in den Informationsfluss
- Unzureichende Vertretungsregelungen für Telearbeit
- Nichtbeachtung von Sicherheitsmaßnahmen

Priorisierung	R2
Hinweis zum besseren Verständnis	Der Baustein OPS.1.2.4 Telearbeit ist auf jeden Heimarbeitsplatz (z. B. Home-Office des Inhabers) bzw. auf alle mobilen Geräte (Laptop, iPad, Smartphone) mit Zugriff auf das Unternehmensnetz oder die Cloud-Lösung von außerhalb der Geschäftsräume und Gebäude des Betriebs anzuwenden.
Anforderungen	OPS.1.2.4.A1 – A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Regelungen für Telearbeit
Zu OPS.1.2.4.A1:
Betriebsvereinbarungen sind eine Grundvoraussetzung für den Zugriff auf das Unternehmensnetz von außerhalb der Geschäftsräume und Gebäude des Betriebs. Dies ist vor allem wichtig, um im Streitfall (bei Diebstahl oder Beschädigung) entsprechende Ansprüche geltend machen zu können. Eine private Nutzung mobiler Geräte sollte unzulässig sein, um das Unternehmen vor unbefugtem Zugriff und anderen Sicherheitsrisiken zu schützen.

Ist sichergestellt, dass in einem unsicheren Einsatzfeld (Kunde, Familie) nicht auf die mobilen Geräte zugegriffen werden kann?

Sicherheitstechnische Anforderungen an den Telearbeitsrechner
Zu OPS.1.2.4.A2:
Die Anforderungen schreiben die notwendigen technischen, organisatorischen Maßnahmen (Zugangs- und Zugriffsmöglichkeiten) für den externen Zugriff auf das Unternehmensnetz und evtl. Cloudlösungen vor. Es muss sichergestellt werden, dass das mobile Gerät nur von autorisierten Personen für autorisierte Zwecke verwendet werden darf.

Sicherheitstechnische Anforderungen an die Kommunikationsverbindung
Zu OPS.1.2.4.A3:
Daten auf mobilen Geräten sollten prinzipiell verschlüsselt werden und die Kommunikation sollte immer über eine gesicherte Verbindung (https-, VPN-Verbindung) erfolgen.

Datensicherung bei der Telearbeit
Zu OPS.1.2.4.A4:
Diese Anforderung kann entfallen, wenn Daten immer auf dem Unternehmensserver bzw. der Cloudlösung zu bearbeiten und von diesem automatisch zu sichern sind. Auf dem Heimarbeitsplatz oder mobilen Gerät sollten keine Unternehmensdaten gespeichert werden.

Sensibilisierung und Schulung der Telearbeiter
Zu OPS.1.2.4.A5:
Die mindestens halbjährige Schulung und Sensibilisierung der Beschäftigten sollte durch ein Merkblatt über IT-Gefahren ergänzt werden. Bei Verlust sollte unverzüglich eine Meldung an eine festgelegte Ansprechperson erfolgen. Besonders ist auf die Nutzung von Zugriffssperren hinzuweisen.

OPS

OPS.2.1
Outsourcing für Kunden.

Outsourcing, also die Zusammenarbeit mit externen Dienstleistungsunternehmen, darf nicht zu unkontrollierbaren Risiken führen. Es ist wichtig, Aspekte der Informationssicherheit von Anfang an zu berücksichtigen. Tipp für den Umgang mit dem IT-Dienstleister: Die Berücksichtigung aller Aspekte dieses „Routenplaners“ wird Bestandteil des Vertrages mit dem IT-(Sicherheits-)Dienstleister.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Regelungen zur Informationssicherheit
- Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten
- Fehlendes oder unzureichendes Test- und Freigabeverfahren
- Unzulängliche vertragliche Regelungen mit einem Outsourcing-Dienstleister
- Unzulängliche Regelungen für das Ende eines Outsourcings
- Abhängigkeit von einem Outsourcing-Dienstleister
- Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
- Mangelhafte Informationssicherheit in der Outsourcing-Einführungsphase
- Ausfall der Systeme eines Outsourcing-Dienstleisters
- Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
- Fehlende Mandantenfähigkeit beim Outsourcing-Dienstleister

Priorisierung	R2
Hinweis zum besseren Verständnis	Dieser Baustein ist nur zu beachten, wenn Dienstleistungen (z. B. Branchenlösung, Webserver oder Terminkalender in die Cloud) ausgelagert werden. Beispiele sind: APP.3.1 Webanwendungen, App.3.2 Webserver und die IT-Systeme, SYS.1.1 Allgemeine Server, SYS 1.2.2 Windows Server 2012 Der Baustein ist für jede Outsourcing-Dienstleistung separat anzuwenden. Die vertragliche Regelung (Berechtigungen und Pflichten, Vereinbarungen zur Dienstgüte [SLAs]) sind zu überprüfen. Besonderer Wert ist auf die Herausgabe und Löschung der Daten bei Vertragsende zu legen.
Anforderungen	OPS.2.1.A1

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben
Zu OPS.2.1 A1:
Der Outsourcing-Dienstleister muss sich auf die Einhaltung des IT-Grundschutzes verpflichten und entsprechende technisch organisatorische Maßnahmen zur IT-Sicherheit und zum Datenschutz umgesetzt haben. Er sollte dies durch ein Zertifikat nachweisen.

OPS.2.2
Cloud-Nutzung.

Planvoll und sicher in die Cloud! Cloud-Services können attraktive Lösungen für Unternehmen sein: Sie reduzieren den Wartungsaufwand für die eigene IT-Infrastruktur und erhöhen die weltweite Verfügbarkeit von Daten. Gleichzeitig ergeben sich neue Risiken, die aufgrund der Auslagerung nicht mehr im Einflussbereich des Unternehmens liegen. Strategisches und systematisches Risikomanagement ist hier zielführend. Informationssicherheit sollte ein wichtiges Kriterium bei der Auswahl des Cloudanbieters sein.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Strategie für die Cloud-Nutzung
- Abhängigkeit von einem Cloud-Diensteanbieter (Kontrollverlust)
- Mangelhaftes Anforderungsmanagement bei Cloud-Nutzung
- Verstoß gegen rechtliche Vorgaben
- Fehlende Mandantenfähigkeit beim Cloud-Diensteanbieter
- Unzulängliche vertragliche Regelungen mit einem Cloud-Diensteanbieter
- Mangelnde Planung der Migration zu Cloud-Diensten
- Unzureichende Einbindung von Cloud-Diensten in die eigene IT
- Unzureichende Regelungen für das Ende eines Cloud-Nutzungs-Vorhabens
- Unzureichendes Administrationsmodell für die Cloud-Nutzung
- Unzureichendes Notfallvorsorgekonzept
- Ausfall der IT-Systeme eines Cloud-Diensteanbieters

Priorisierung	R1
Hinweis zum besseren Verständnis	Dieser Baustein ist nur zu beachten, wenn Dienstleistungen (z. B. Branchenlösung, Telefonanlage oder Terminkalender in die Cloud) ausgelagert oder Webserver betrieben werden. Dann ist er für jede Outsourcing-Dienstleistung separat anzuwenden. Die vertragliche Regelung (Berechtigungen und Pflichten, Vereinbarungen zur Dienstgüte [SLAs]) sind zu überprüfen. Besonderer Wert ist auf die Herausgabe und Löschung der Daten bei Vertragsende zu legen.
Anforderungen	OPS.2.2.A1 – A4

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erstellung einer Cloud-Nutzungs-Strategie
Zu OPS.2.2.A1:
Welche Dienste für eine Cloud-Lösung und welches Bereitstellungsmodell in Frage kommen, ist festzulegen. Bereitstellungsmodelle sind die Public-Cloud (viele Kunden teilen sich eine Infrastruktur: Branchensoftware, Microsoft Office 365, Apple iCloud), Private-Cloud (in einer Firma oder einem Rechenzentrum: z. B. VMWare, Webserver) und die Hybrid-Cloud (wenn sowohl Public- als auch Hybrid-Cloud-Lösungen in einer Firma genutzt werden).
Dabei ist zu beachten, dass eine Verarbeitung und Nutzung der Daten nicht möglich ist, wenn diese Dienste (z. B. bei mangelnder Leistungsfähigkeit oder Störung der Internetanbindung) nicht genutzt werden können.
Grundlegende technisch-organisatorische Sicherheitsaspekte sowie wirtschaftliche und rechtliche Rahmenbedingungen (Vorgaben der DSGVO oder von Vertragspartnern) sind zu beachten.
Daten sind verschlüsselt zu übertragen und verschlüsselt in der Cloud abzulegen.
Die Verpflichtung des Outsourcing-Dienstleisters auf die Einhaltung des IT-Grundschutzes und Umsetzung entsprechender technisch-organisatorischer Maßnahmen zur IT-Sicherheit und zum Datenschutz, sollte der Outsourcing-Dienstleister durch ein Zertifikat nachweisen.

Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung
Zu OPS.2.2.A2:
Informationen, die in der Cloud gespeichert werden, sollen nach ihrem Schutzbedarf und unter Berücksichtigung der DSVGO klassifiziert werden. Hierauf ist besonders bei international agierenden Cloud-Diensteanbietern zu achten.

Service-Definition für Cloud-Dienste durch den Anwender
OPS.2.2.A3:
Mit dem Cloud-Anbieter sind Service-Parameter wie feste Reaktionszeiten und Ansprechpartner festzulegen. Auf die Durchführung einer Datensicherung ist besonders zu achten.

Festlegung von Verantwortungsbereichen und Schnittstellen
Zu OPS.2.2.A4:
Inkompatibilitäten der Client-Software, mit der vorhanden IT-Infrastruktur und die Einbindung zusätzlicher Laufwerke, sind zu prüfen.

Leitfragen:

Verfügen die für den Datenaustausch mit der Cloud vorgesehenen Geräte (PC, Smartphone, Tablet) über einen ausreichenden Basisschutz, inklusive Viren-Schutz und Personal Firewall?

Gibt es im Unternehmen Richtlinien zur Klassifizierung vertraulicher Daten?

Wurden mit der Klassifizierung vertraulicher Daten Speicherorte für diese Daten festgelegt?

Werden die Serverstandorte des Cloud-Service Anbieters (Land, Region), an denen die Daten gespeichert und verarbeitet werden, offengelegt?

Ist die Netzwerksicherheit (Sicherheitsmaßnahmen gegen Malware, DDoS, verschlüsselte Kommunikation zw. Cloud-Computing-Standorten mit Drittanbietern) vom Anbieter gewährleistet?

Sind notwendige Kriterien für einen gewollten Service (Service Level Agreements, SLA) vorhanden und haben die Kunden die Möglichkeit messbare Größen, wie im SLA vereinbart, zu überwachen?

Werden regelmäßig lokale Backups der ausgelagerten Daten angelegt?

OPS.2.4 Fernwartung.

Service versus Sicherheit – Der Zugriff auf IT-Systeme und Anwendungen von außen bzw. durch Dritte muss geregelt sein, um das Gefahrenpotenzial gering zu halten.

Minimieren Sie diese Risiken:

- Unzureichende Kenntnisse über Regelungen der Fernwartung
- Fehlende oder unzureichende Planung und Regelung der Fernwartung
- Unerlaubtes Ausüben von Rechten bei der Fernwartung
- Ungeeignete Nutzung von Authentisierung bei der Fernwartung
- Unsicherer und unkontrollierter Aufbau von Kommunikationsverbindungen
- Fehlerhafte Fernwartung
- Verwendung unsicherer Protokolle in der Fernwartung
- Ungeeigneter Umgang mit Authentisierungsverfahren bei der Fernwartung
- Unsichere kryptografische Algorithmen bei der Fernwartung
- Unsichere und unkontrollierte Fremdnutzung der Fernwartungszugänge
- Nutzung von Online-Diensten für die Fernwartung

Priorisierung	R3
Hinweis zum besseren Verständnis	Dieser Baustein ist zu beachten, wenn Zugriffsmöglichkeiten (z. B. von IT-Dienstleistern oder Anbietern von Branchensoftware) von außerhalb auf das interne Netz und die darin verarbeiteten Daten bestehen. Diese können z. B. für Konfigurations-, Wartungs- und Update-Zwecke (Patch- und Änderungsmanagement) im Rahmen von Wartungsverträgen notwendig sein. Der Baustein ist ebenso zu beachten, wenn das Unternehmen selbst Fernwartungen z. B. bei Gebäudeleitsystemen, Heizungsanlagen, Smart-Home-Lösungen, Alarmanlagen etc. durchführt.
Anforderungen	OPS.2.4.A1 – A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Planung des Einsatzes der Fernwartung
Zu OPS.2.4.A1:
Erfolgt die Fernwartung durch Dienstleister, ist die Maßnahme OPS.2.4.M18 (Fernwartung durch Dritte) zu beachten und der Zugriff ist vertraglich zu regeln.

Sicherer Verbindungsaufbau bei der Fernwartung
Zu OPS.2.4.A2:
Bei diesem Baustein ist darauf zu achten, dass der Fernwartungszugriff immer aus dem Unternehmen heraus und nach Beendigung ein „Zwangs-Logout“ erfolgen muss.

Absicherung der Kommunikationsverbindungen bei der Fernwartung
Zu OPS. 2.4.A3:
Die Fernwartungsverbindung muss immer verschlüsselt sein. Der Personenkreis ist nach dem Minimalprinzip einzuschränken.

Einsatz von Online-Diensten
Zu OPS.2.4.A5:
Der Einsatz von Online-Diensten, wie TeamViewer, sollte auf Notfälle beschränkt werden, da nicht erkennbar ist, was mit diesen Informationen beim Diensteanbieter passiert. Ein automatischer Verbindungsaufbau der Clients zum Server sollte untersagt werden. Für jede Verbindung sind neue Zugangsdaten zu generieren.

DER.1 Detektion von sicherheitsrelevanten Ereignissen.

Cyber-Angriffe zu erkennen, ist notwendig, um den Schaden für den Betrieb zu minimieren. Erkenntnisse aus der Detektion tragen dazu bei, passende Maßnahmen zu ergreifen, um angemessen auf Angriffe zu reagieren.

Minimieren Sie diese Risiken:

- Missachtung von gesetzlichen Vorschriften und betrieblichen Mitbestimmungsrechten
- Unzureichende Qualifikation der Verantwortlichen
- Fehlende oder unzureichende Protokollierung
- Fehlerhafte Administration der eingesetzten Detektionssysteme
- Fehlende Informationen über das zu schützende Gesamtsystem
- Unzureichende Nutzung von Detektionssystemen
- Unzureichende personelle Ressourcen

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	DER.1.A1 – A5

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

DER.2.1 Behandlung von Sicherheitsvorfällen.

Für den Ernstfall gut gerüstet! Um Schäden zu begrenzen und weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren.

Minimieren Sie diese Risiken:

- Ungeeigneter Umgang mit Sicherheitsvorfällen
- Nicht erkannte Sicherheitsvorfälle
- Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

Priorisierung	R2
Hinweis zum besseren Verständnis	Für den Handwerksbetrieb ist es von zentraler Bedeutung, dass IT-basierte Sicherheitsvorfälle von Beschäftigten frühzeitig erkannt werden, die zuständigen Ansprechpersonen informiert werden und diese die richtigen Maßnahmen in die Wege leiten, um auf diese Sicherheitsvorfälle zu reagieren. Die schnelle Wiederherstellung der betroffenen Betriebsumgebung ist das Ziel, um wirtschaftliche Schäden zu verhindern.
Anforderungen	DER.2.1.A1 – A6

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Definition eines Sicherheitsvorfalls
Zu DER.2.1.A1:
Eine mögliche Definition eines Sicherheitsvorfalls könnte z. B. lauten: "Als Sicherheitsvorfall wird in unserem Unternehmen ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität unserer Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen derart beeinträchtigt, dass ein großer Schaden für unser Unternehmen, unsere Kunden oder Geschäftspartner entstehen kann."

Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
Zu DER.2.1.A2:
Die Richtlinie soll für die Benutzer von IT-Systemen die Basis dafür sein, dass z. B. die Infektion durch Schadprogramme schnell erkannt werden, ein richtiges Verhalten bei Verdacht eines Angriffs folgt und die verantwortlichen Ansprechpartner (i.d.R. Leitung des Handwerksunternehmens, IT-Verantwortlicher) und weitere Bearbeiter des Sicherheitsvorfalls, einen Maßnahmenkatalog für den sachgerechten Umgang mit dem Vorfall verfügbar haben.

Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen
Zu DER.2.1.A3:
Allen IT-Nutzern und -Nutzerinnen kommt die sehr wichtige Verantwortung zu, bei sicherheitsrelevanten Unregelmäßigkeiten, bestimmte Verhaltensregeln einzuhalten und den Sachverhalt i.d.R. direkt der Unternehmensleitung zu melden oder dem nächsten Vorgesetzten. Dieser wiederum informiert die Leitung oder die IT-Verantwortlichen bzw. externen Dienstleister.

Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
Zu DER.2.1.A4:
Die Unternehmensleitung eines Handwerksbetriebs sollte immer über alle IT-basierten Sicherheitsvorfälle informiert sein. Sie muss gegebenenfalls auch darüber entscheiden, ob externe Unterstützung und Strafverfolgungsbehörden eingeschaltet werden müssen.

Behebung von Sicherheitsvorfällen
Zu DER.2.1.A5:
Der IT-Verantwortliche, der bei einem Handwerksbetrieb auch der externe IT-Dienstleister sein kann, muss das Problem eingrenzen und die Ursache finden. In Absprache mit der Unternehmensleitung müssen Maßnahmen ausgewählt und umgesetzt werden. Eine Liste mit den externen IT-Dienstleistern, die als Experten bei bestimmten Themenbereichen in Frage kommen, muss vorhanden sein.

Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen
Zu DER.2.1.A6:
Der Datensicherung kommt bei dieser Anforderung eine entscheidende Bedeutung zu. Beim Auffinden einer Schadsoftware ist es entscheidend zu prüfen, ob auch Sicherungen betroffen sind.

DER

DER.2.2 Vorsorge für die IT-Forensik.

Spuren sichern nach einem Vorfall: IT-Sicherheitsvorfälle forensisch zu untersuchen, ist immer dann notwendig, wenn eingetretene Schäden bestimmt, Angriffe abgewehrt und künftig vermieden sowie Angreifer identifiziert werden sollen.

Minimieren Sie diese Risiken:

- Verstoß gegen rechtliche Rahmenbedingungen
- Verlust von Beweismitteln durch fehlerhafte oder unvollständige Beweissicherung

Priorisierung	R3
Hinweis zum besseren Verständnis	Der Baustein dient zur Vorbereitung auf potentielle IT-Sicherheitsvorfälle. Er soll helfen, eingetretene Schäden zu bestimmen, Angriffe abzuwehren und künftig zu vermeiden. Der Baustein zeigt auf, wie die Spurensicherung vorbereitet und durchgeführt werden kann.
Anforderungen	DER.2.2.A1 – A3

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit
Zu DER.2.2.A1:
Bei der Erfassung und Speicherung von Daten, die der späteren Auswertung dienen sollen, muss sichergestellt sein, dass alle Betriebs- und Mitarbeitervereinbarungen sowie die Vorschriften der DSGVO eingehalten werden.

Erstellung eines Leitfadens für Erstmaßnahmen bei einem Sicherheitsvorfall
Zu DER.2.2.A2:
Es empfiehlt sich, eine ausführliche Dokumentation der IT-Anlage. Dazu zählt auch ein Netzplan sowie die Softwareausstattung der einzelnen IT-Komponenten.

Vorauswahl von Forensik-Dienstleistern
Zu DER.2.2.A3:
Es sollte geklärt werden, ob der eigene IT-Dienstleister eine forensische Untersuchung durchführen kann. Ist dies nicht der Fall, so ist es immens wichtig im Vorfeld bereits die relevanten Kontakte für den Notfall geknüpft zu haben.

DER.3.1
Audits und Revisionen.

Sind die Schutzmaßnahmen wirksam, vollständig, angemessen und noch aktuell? Informationssicherheit ist ein Prozess. In regelmäßigen Abständen ist es notwendig, den Gesamtzustand der Informationssicherheit im Unternehmen systematisch zu überprüfen, um auf Dauer ein angemessenen Sicherheitsniveau aufrechtzuerhalten.

Minimieren Sie diese Risiken:

- Unzureichende oder nicht planmäßige Umsetzung von Sicherheitsmaßnahmen
- Wirkungslose oder nicht wirtschaftliche Umsetzung von Sicherheitsmaßnahmen
- Unzureichende Umsetzung des Informationssicherheits-Managementsystems (ISMS)
- Unzureichende Qualifikation des Prüfers bzw. der Prüferin
- Fehlende langfristige Planung
- Fehlende Planung und Abstimmung bei der Durchführung eines Audits
- Fehlende Abstimmung mit der Personalvertretung
- Absichtliches Verschweigen von Abweichungen

Priorisierung	R3
Hinweis zum besseren Verständnis	–
Anforderungen	DER.3.1.A1 - A4

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

DER.4 Notfallmanagement.

Für den Notfall: Eine optimale Notfallvorsorge und Notfallbewältigung ist nur möglich, wenn geplant und organisiert vorgegangen wird. Ein professionelles Notfallmanagement reduziert den Schaden und sichert somit den Betrieb und seinen Fortbestand.

Minimieren Sie diese Risiken:

- Personalausfall
- Ausfall von IT-Systemen
- Ausfall eines Weitverkehrsnetzes (WAN)
- Ausfall eines Gebäudes
- Ausfall eines Lieferanten oder Dienstleisters

Priorisierung	R3
Hinweis zum besseren Verständnis	Die Entscheidung, ob ein Notfall an sich vorliegt, wird in DER.2.1 behandelt. Es gibt fünf Arten von Ausfällen (mit Beispiel), die zu Notfällen führen können: Personalausfall (Kennwörter für Server/Tresor-PIN nicht verfügbar, Projektwissen nicht zugänglich), IT-System-Ausfall (Handbuch zum Neustart auf System selbst), Ausfall eines Weitverkehrsnetzes kurz WAN (kein Telefon/Internet), Gebäudeausfall (Feuer/Wasserschaden), Ausfall eines Lieferanten/Dienstleisters. Die Anforderungen bieten sich für jedes Handwerksunternehmen an, sollten aber im Umfang an die Unternehmensgröße angepasst werden.
Anforderungen	Empfohlen: DER.4.A1 – A2

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erstellung eines Notfallhandbuchs
Zu DER.4.A1:
Das Notfallhandbuch wie vom BSI empfohlen ist erst ab ca. 20 Personen im Betrieb sinnvoll. Es empfiehlt sich ein kleines „Notfalltestament“ bzw. ein IT-Notfallplan mit den wichtigsten Passwörtern, Zugriffsberechtigungen und Vollmachten. Auch sollten alle Lizenzen und die dazugehörigen Backup-Lösungen an einem zentralen Ort sicher aufbewahrt werden.

Vorab sind folgende Fragen zu klären:
- **Welche Auswirkungen hat der Ausfall eines bestimmten IT-Systems bzw. einer Person?**
- **Welche Ausfallzeiten sind zu verkraften?**
- **Was ist zu tun, um die Funktion der Systeme oder des Prozesses wiederherzustellen?**
- **Wer ist bei Problemen zu informieren?**
- **Wie sind Personen oder Firmen zu erreichen?**

Hieraus werden dann für den Notfallplan die Abläufe, Verzeichnisse mit relevanten Dokumenten und Informationen, Checklisten, Kontaktlisten mit alternativen Dienstleistern/Lieferanten und Vertretungsregeln abgeleitet. Diese sollten in regelmäßigen Abständen überprüft und aktualisiert werden.

Der Tod als extremster Personenausfall und damit der Verlust des kompletten Wissens sollte immer mit berücksichtigt werden.

DER

APP.1.1
Office-Produkte.

Office-Produkte gehören für die meisten Betriebe zur notwendigen IT-Grundausstattung. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen sowie Zeichenprogramme und einfache Datenbanksysteme. Aufgrund ihrer Verbreitung bieten Office-Anwendungen eine attraktive Angriffsfläche für Cyber-Attacken.

Minimieren Sie diese Risiken:

- Fehlende Anpassung der Office-Produkte an den Bedarf des Betriebs
- Fehlendes oder unzureichendes Test- und Freigabeverfahren bei Office-Produkten
- Schützenswerte Daten in Restinformationen in Office-Dokumenten
- Bezug von Office-Produkten und Updates aus unzuverlässiger Quelle
- Manipulation von Office-Dokumenten
- Mangelnde Verbindlichkeit von Office-Dokumenten
- Integritätsverlust von Office-Dokumenten
- Software-Schwachstellen in Office-Produkten
- Einsatz von unlizenzierten Office-Produkten
- Datenverlust durch Passwortschutz von Office-Dokumenten
- Unerlaubtes Ausüben von Rechten bei Office-Produkten

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	APP.1.1.A1 – A4

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

APP

APP.1.2
Web-Browser.

Web-Browser sind Anwendungsprogramme, die Dokumente, Bilder, Video-, Audio- und andere Datenformate aus dem Internet verarbeiten. Ihre Komplexität bietet ein hohes Potenzial für Schwachstellen und erhöht damit die Gefahren für Angriffe. Hinzu kommen Programmier- und Bedienungsfehler. Die Risiken für die Vertraulichkeit und Integrität von Daten sind erheblich. Auch die Verfügbarkeit des gesamten IT-Systems ist bedroht.

Minimieren Sie diese Risiken:

- Ausführung von Schadcode durch Web-Browser
- Angriff durch Exploit Kits (Werkzeuge für Cyber-Angriffe)
- Mitlesen der Internetkommunikation
- Integritätsverlust in Web-Browsern
- Verlust der Privatsphäre
- Fehler bei Administration und Betrieb

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	APP.1.2.A1 – A4

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

APP.1.4
Mobile Anwendungen.

Anwendungen (Apps) auf mobilen Endgeräten wie Smartphone und Tablet bieten unzählige Angriffsmöglichkeiten. Es kommt auf die Auswahl und die sichere Nutzung an, um die Risiken für Unternehmensdaten einzudämmen.

Minimieren Sie diese Risiken:

- Ungeeignete Auswahl von Apps
- Mangelnde Ressourcen und Kompetenzen
- Mangelnde Kontrolle und Auswertungsmöglichkeiten
- Zu weitreichende Berechtigungen
- Ungewollte Funktionen in Apps
- Software-Schwachstellen und Fehler in Apps
- Unsichere Speicherung lokaler Anwendungsdaten
- Metadaten und Inferenz vertraulicher Informationen
- Abfluss von vertraulichen Daten
- Unsichere Kommunikation mit Backend-Systemen
- Wechselwirkungen mit anderen Apps
- Kommunikationswege außerhalb der Infrastruktur der Institution
- Nicht verwaltete Apps und nicht verwaltete Endgeräte
- Abhängigkeit von Backend- oder externen Systemen und Diensten

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	APP.1.4.A1 – A8

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

APP.5.1
Allgemeine Groupware.

„Informationen effektiv und sicher teilen“ - Mithilfe von Groupware-Systemen können Anwender und Anwenderinnen miteinander kooperieren, Termine abstimmen, Dokumente und Dateien gleichzeitig bearbeiten und vieles mehr. Umso wichtiger, die geteilten Informationen angemessen zu schützen.

Minimieren Sie diese Risiken:

- Unzureichende Planung der Groupware
- Fehlerhafte Einstellung der Groupware
- Missbrauch selbst entwickelter Makros und Programmierschnittstellen bei Groupware-Diensten
- Fehlerhafte Vergabe von Zugangs- und Zugriffsrechten auf Groupware-Dienste
- Unzureichendes Wissen der Administratoren von Groupware-Systemen
- Datenverlust bei Groupware-Anwendungen
- Angriffe auf Groupware-Systeme und -Anwendungen
- Unzuverlässigkeit von Groupware

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	APP.5.1.A1 – A4

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

APP.5.2 Microsoft Exchange und Outlook.

Microsoft Exchange ist eine Groupware-Lösung mit typischen Anwendungen, wie E-Mail, Newsgroups, Kalender und Aufgabenlisten etc. Aufgrund ihrer Verbreitung zeigen sich immer wieder typische Gefahren und Risiken, denen Unternehmen z. B. mit einer sicheren Konfiguration begegnen sollten.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Regelungen für Microsoft Exchange und Outlook
- Fehlerhafte Migration von Microsoft Exchange
- Unzulässiger Browserzugriff auf Microsoft Exchange
- Unerlaubte Anbindung anderer Systeme an Microsoft Exchange
- Fehlerhafte Administration von Zugangs- und Zugriffsrechten unter Microsoft Exchange und Outlook
- Fehlerhafte Konfiguration von Microsoft Exchange
- Fehlerhafte Konfiguration von Outlook
- Fehlfunktionen und Missbrauch selbst entwickelter Makros sowie Programmierschnittstellen unter Microsoft Outlook

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	APP.5.2.A1 – A5

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

SYS.2.1
Allgemeiner Client.

Ein "Allgemeiner Client" ist ein IT-System, das die Trennung von Benutzern zulässt und beispielsweise auf einem PC mit bzw. ohne Festplatte oder einem mobilen Gerät betrieben wird. Er wird direkt von den Benutzern bedient und ist somit oft das Einfallstor für Schadsoftware.

Minimieren Sie diese Risiken:

- Schadprogramme
- Unstrukturierte lokale Datenhaltung
- Datenverlust
- Hardware-Defekte durch Fehlbedienung
- Software-Schwachstellen oder -Fehler
- Unberechtigte IT-Nutzung
- Bereitstellung nicht benötigter Betriebssystemkomponenten und Applikationen
- Abhören von Räumen mittels Mikrofon und Kamera

Priorisierung	R2
Hinweis zum besseren Verständnis	In diesem Baustein wird ein IT-System mit einem beliebigen Betriebssystem (Einzel-PC oder Server-Netz; allgemeiner Client) und die Basisanforderungen für den IT-Grundschutz betrachtet.
Anforderungen	SYS.2.1.A1 – A8

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Benutzerauthentisierung
Zu SYS.2.1.A1:
Benutzerauthentisierung, Anmeldungen am IT-System müssen durch geeignete Verfahren, wie z. B. sichere Passwörter erfolgen. Wertvolle Hinweise dazu finden Sie in den Umsetzungshinweisen.

Aktivieren von Autoupdate-Mechanismen
Zu SYS.2.1.A3:
Das größte Einfallstor für Viren, Trojaner und Co. sind veraltete Softwareversionen auf dem IT-System. Durch Updates werden gefundene Lücken geschlossen und somit das IT-System softwareseitig sicherer gemacht. Softwareupdates sollten daher am besten automatisch erfolgen oder zumindest regelmäßig manuell installiert werden.

Bildschirmsperre
Zu SYS.2.1.A5:
Nicht nur im Hinblick auf IT-Grundschutz notwendig, um unberechtigten Benutzern den Zugriff auf Daten zu erschweren. Sondern auch im Hinblick auf Schutz von personenbezogenen Daten eine Grundmaßnahme der technisch organisatorischen Maßnahmen gem. DSGVO!

Einsatz von Viren-Schutzprogrammen
Zu SYS.2.1.A6:
Um ausreichend vor Schadprogrammen geschützt zu sein, muss ein aktuelles (Siehe auch Sys.2.1. A3) Programm im Einsatz sein.

Absicherung des Boot-Vorgangs
Zu SYS.2.1.A8:
Verhinderung des Booten von anderen Medien als über das System. Der Bootvorgang über andere Medien darf nur durch den Administrator erfolgen. Hinweis für Einzel-PC: Absicherung des BIOS durch separates Passwort, ansonsten kann hier die Bootreihenfolge eingestellt werden!

SYS

SYS.2.2.2
Clients unter Windows 8.1.

Zusammen mit dem Baustein SYS.2.1 Allgemeiner Client ist dieser Baustein für den Schutz von Informationen, die durch und auf Clients unter Windows 8.1 verarbeitet werden, vorgesehen.

Minimieren Sie diese Risiken:

- Auf Windows ausgerichtete Schadprogramme
- Software-Schwachstellen oder -Fehler
- Integrierte Cloud-Funktionalitäten
- Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme
- Fehlerhafte Administration oder Nutzung von Geräten und Systemen

Priorisierung	R2
Hinweis zum besseren Verständnis	Bei der Nutzung eines Clients unter Windows 8.1 ist darauf zu achten, dass mindestens die 64-Bit-Version wegen der erweiterten Sicherheitsmöglichkeiten zum Einsatz kommt.
Anforderungen	SYS.2.2.2.A1 – A3

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Festlegung eines Anmeldeverfahrens
Zu SYS.2.2.2.A1:
Geeignete Auswahl einer Windows 8.1-Version.
Es SOLLTEN bevorzugt 64-Bit-Versionen eingesetzt werden, die erweiterte Sicherheitsfeatures enthalten!

Festlegung eines Anmeldeverfahrens
Zu SYS.2.2.2.A2:
Siehe dazu auch SYS.2.1.A2.

Einsatz von Viren-Schutzprogrammen
Zu SYS.2.2.2.A3:
Siehe dazu auch SYS.2.1.A6.
Wenn die Anforderung aus SYS.2.1. bereits erfüllt werden muss, dann ist diese in diesem Baustein bereits erfüllt und muss nicht mehr betrachtet werden!

SYS.2.2.3
Clients unter Windows 10.

Zusammen mit dem Baustein SYS.2.1 Allgemeiner Client ist dieser Baustein für den Schutz von Informationen, die durch und auf Windows10-Clients verarbeitet werden, vorgesehen.

Minimieren Sie diese Risiken:

- Schadprogramme unter Windows 10
- Software-Schwachstellen in Windows 10
- Integrierte Cloud-Funktionalitäten
- Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme
- Fehlerhafte Administration oder Nutzung von Windows 10

Priorisierung	R2
Hinweis zum besseren Verständnis	Bei der Nutzung eines Clients unter Windows 10 ist wegen der möglichen Übertragung von Daten zu Microsoft in die USA aus Gründen der DSGVO darauf zu achten, dass diese Übertragung ohne personenbezogene Daten erfolgt!
Anforderungen	SYS.2.2.3.A1 – A6

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Planung des Einsatzes von Cloud-Diensten
Zu SYS.2.2.3.A1:
Aufgrund der Verzahnung des Betriebssystem mit Cloud-Diensten (z. B. OneDrive oder auch Office365) von Microsoft ist festzulegen, welche Cloud-Dienste in welchem Umfang genutzt werden sollen bzw. dürfen. Besonders bei der Nutzung von vertraulichen Informationen oder personenbezogenen Daten ist diese Entscheidung von elementarer Bedeutung!

Geeignete Auswahl einer Windows 10-Version und Beschaffung
Zu SYS.2.2.3.A2:
Der Funktionsumfang und die Versorgung mit funktionalen Änderungen einer Windows 10-Version müssen unter Berücksichtigung des ermittelten Schutzbedürfnisses und des Einsatzzwecks ausgewählt und die Umsetzbarkeit der erforderlichen Absicherungsmaßnahmen geprüft werden.

Geeignetes Patch- und Änderungsmanagement
Zu SYS.2.2.3.A3:
Wer seine Einzelrechner bzw. „kleines“ Netzwerk nicht eigenständig in Bezug auf Sicherheitsupdates managen möchte, kann diese Aufgabe an einen IT-Dienstleister übergeben.

Telemetrie und Datenschutzeinstellungen
Zu SYS.2.2.3.A4:
Die Telemetriedienste, also die Diagnose- und Nutzungsdaten, die Microsoft zur Identifizierung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Personalisierung des Systems mit eindeutigen Identifizierungsmerkmalen verknüpft in die USA überträgt, können im Betriebssystem nicht vollständig abgeschaltet werden.

Schutz vor Schadsoftware
Zu SYS.2.2.3.A5:
Dieses Thema ist bereits in SYS.2.1. A6 beschrieben! Hier sind die Besonderheit von Windows 10 zu beachten.

Integration von Online-Konten in das Betriebssystem
Zu SYS.2.2.3.A6:
Die Anmeldung am System und der Domäne darf nur mit dem Konto eines selbst betriebenen Verzeichnisdienstes möglich sein. Anmeldungen mit lokalen Konten sollten Administratoren vorbehalten sein. Online-Konten zur Anmeldung, etwa ein Microsoft-Konto oder Konten anderer Anbieter von Identitätsmanagementsystemen, dürfen nicht verwendet werden, da hier personenbezogene Daten an die Systeme des Herstellers übertragen werden.

SYS.3.1
Laptops.

Ob Diebstahl, wechselnde Benutzer, fehlende Synchronisation – Laptops und Notebooks bergen vielfältige Risiken. Klare Regelungen für die Nutzung tragen dazu bei, die Risiken für das Unternehmen zu verringern.

Minimieren Sie diese Risiken:

- Beeinträchtigung durch wechselnde Einsatzumgebung
- Diebstahl
- Ungeordneter Benutzerwechsel bei Laptops
- Fehler bei der Synchronisation
- Datenverlust bei mobilem Einsatz
- Datendiebstahl mithilfe von Laptops

Priorisierung	R2
Hinweis zum besseren Verständnis	Aufgrund des mobilen Einsatzes sind Laptops naturgemäß einem höheren Diebstahlrisiko ausgesetzt. Wird ein Laptop gestohlen, entstehen Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes. Ebenso könnten dadurch aber auch Unbefugten schützenswerte Daten offengelegt werden, wodurch es zu weiteren Schäden kommen kann. Diese wiegen in vielen Fällen deutlich schwerer als der rein materielle Verlust des Gerätes.
Anforderungen	SYS.3.1.A1 – A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Regelungen zur mobilen Nutzung von Laptops
Zu SYS.3.1.A1:
Es MUSS klar geregelt werden, was Beschäftigte beachten sollen, wenn sie Laptops mitnehmen. Es MUSS insbesondere festgelegt werden, welche Laptops außer Haus mitgenommen werden dürfen, wer sie mitnehmen darf und welche grundlegenden Sicherheitsmaßnahmen dabei zu beachten sind. Die Benutzer MÜSSEN auf die Regelungen hingewiesen werden.

Zugriffsschutz am Laptop
Zu SYS.3.1.A2:
Auf allen Laptops MUSS ein angemessener Zugriffsschutz vorhanden sein, der verhindert, dass das Gerät unberechtigt benutzt werden kann.

Einsatz von Personal Firewalls
Zu SYS.3.1.A3:
Auf Laptops MUSS eine Personal Firewall aktiv sein. Die Filterregeln der Firewall MÜSSEN so restriktiv wie möglich sein. Sie MÜSSEN regelmäßig getestet werden. Die Personal Firewall MUSS so konfiguriert werden, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.

Einsatz von Antivirenprogrammen
Zu SYS.3.1.A4:
Abhängig vom installierten Betriebssystem und anderen vorhandenen Schutzmechanismen MUSS auf allen Laptops der Institution ein Antivirenprogramm installiert und aktiviert sein. Es MUSS sichergestellt werden, dass sowohl das Scan-Programm als auch die Signaturen stets auf dem aktuellsten Stand sind. Die Benutzer MÜSSEN mit der Antivirensoftware vertraut gemacht werden, besonders auch mit On-Demand-Scans.
Der gesamte Datenbestand der Laptops MUSS regelmäßig auf Schadprogramme geprüft werden. Wenn der Rechner infiziert ist, MUSS im Offlinebetrieb untersucht werden, ob das gefundene Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder einen Code aus dem Internet nachgeladen hat.
Das Antivirenprogramm MUSS zudem nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden. Auch MÜSSEN alle auf dem Laptop benutzten Internet-Dienste (HTTP, FTP) sowie verschlüsselte Daten ausreichend vor Schadprogrammen geschützt werden.
Außerdem MUSS sichergestellt werden, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können.

SYS.3.2.1 Allgemeine Smartphones und Tablets.

Mobilgeräte sind ständig online und ermöglichen damit jederzeit Zugriff auf digitale Informationen – auch die des Betriebs. Die „mobilen Tausendsassa“ potenzieren die Gefährdungen in Bezug auf die Informationssicherheit. Denn Smartphones vereinen oft Mobiltelefone, Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten verschiedene Anwendungen und Funktionen, wie z. B. Web-Browser, E-Mail-Client oder GPS. Das kleine Einmal-Eins der Schutzmaßnahmen muss hier dringend zur Anwendung kommen.

Minimieren Sie diese Risiken:

- Verlust des mobilen Geräts
- Fehlende Betriebssystem-Updates
- Software-Schwachstellen in Anwendungen (Apps)
- Manipulation von mobilen Endgeräten
- Schadprogramme
- Webbasierte Angriffe auf mobile Browser
- Missbrauch von Fitness- oder Ortungsdaten
- Missbrauch sensitiver Daten im Sperrbildschirm
- Gefahren durch private Nutzung mobiler Geräte
- Gefahren durch Bring Your Own Device (BYOD)

Priorisierung	R2
Hinweis zum besseren Verständnis	Die Nutzung von mobilen Endgeräten ist aus heutiger Sicht notwendig für die Arbeit als Handwerker. Sie sind allerdings auch ein enormes Datenschutzrisiko für das Unternehmen. Bei der Nutzung von privaten Smartphones oder Tablets sollte der Verantwortliche (Inhaber/Geschäftsführer) trotzdem auf die Einhaltung des Basisschutzes achten, da ein Verlust von personenbezogenen Daten der Kunden in seine Verantwortung fällt. Eine Nutzung von firmeneigenen Smartphones und Tablets ist in Verbindung mit einem MDM (Baustein: SYS.3.2.2) eine weitaus bessere Alternative.
Anforderungen	SYS.3.2.1.A1 – A8

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Verhaltensregeln bei Sicherheitsvorfällen
Zu SYS.3.2.1.A7:
Eine sofortige Verlustmeldung ist auf Grund der EU-Datenschutzgrundverordnung aus dem Jahre 2018 dringend notwendig, da im Handwerk in den meisten Fällen personenbezogene Daten von Kunden auf dem Handy verarbeitet bzw. gespeichert werden. Ein Verlust macht eine Meldung beim jeweiligen Landesdatenschutzbeauftragten innerhalb von 72 Stunden notwendig.

SYS

SYS.3.2.3 iOS (for Enterprise).

Zusammen mit dem Baustein SYS.3.2.1 Allgemeine Smartphones und Tablets ist dieser Baustein für den Schutz von Informationen auf iOS (for Enterprise) betriebenen Geräten vorgesehen.

Minimieren Sie diese Risiken:

- Fehlende oder schlechte Qualität des Zugriffsschutzes
- Jailbreak (Unterlaufen von Sicherheitsmechanismen des mobilen Betriebssystems iOS)
- Risikokonzentration durch ein Benutzerkonto (Apple ID) für alle Apple-Dienste
- Fehlende Betriebssystem-Updates bei alten Geräten
- Software-Schwachstellen in Apps
- Tiefere Integration für vorinstallierte Apps und deren Funktionalitäten
- Missbrauch biometrischer Authentisierung
- Missbrauch von Fitness-, Gesundheits- oder Ortungsdaten unter iOS
- Missbrauch sensitiver Daten im gesperrten Zustand
- Missbrauch in iOS-basierten Geräten gespeicherter Daten
- Missbräuchlicher Zugriff auf ausgelagerte Daten
- Webbasierte Angriffe auf Browser
- Unzureichende Vorgaben zum Lizenz-Management

Priorisierung	R2
Hinweis zum besseren Verständnis	Nur für Benutzer von Apple-Geräten notwendig! Sollte eine kleine Anzahl von Apple-Geräten eingesetzt werden, ist nur dieser Baustein anwendbar. Sollten eine Vielzahl (ca. >10) Apple-Geräte eingesetzt werden, wird die Nutzung eines MDM vorausgesetzt. Somit müssten zwingend die Basis-Anforderungen von SYS. 3.2.1 erfüllt werden.
Anforderungen	SYS.3.2.3.A1 – A3

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

SYS

SYS.3.2.4 Android.

Zusammen mit dem Baustein SYS.3.2.1 Allgemeine Smartphones und Tablets ist dieser Baustein für den Schutz von Informationen auf Android-basierten Geräten vorgesehen.

Minimieren Sie diese Risiken:

- Rooten des Gerätes
- Schadsoftware für das Android-Betriebssystem
- Fehlende Updates für das Android-Betriebssystem
- Risikokonzentration durch ein Benutzerkonto (Google-ID) für alle Google-Dienste
- Vorinstallierte Apps und integrierte Funktionalitäten bei Android-basierten Geräten

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	SYS.3.2.4.A1

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

SYS.3.3 Mobiltelefon.

Mobil telefonieren, aber sicher! Die in diesem Baustein betrachteten Mobiltelefone besitzen zwar weniger Eigenschaften als ein Smartphone, bieten aber mehr als nur die reine Telefonfunktion. Um typischen Gefahren vorzubeugen, helfen klare definierte Nutzungsregeln und die regelmäßige Schulung der Beschäftigten.

Minimieren Sie diese Risiken:

- Unzureichende Planung bei der Anschaffung von Mobiltelefonen
- Verlust des Mobiltelefons
- Sorglosigkeit im Umgang mit Informationen
- Unerlaubte private Nutzung des dienstlichen Mobiltelefons
- Ausfall des Mobiltelefons
- Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
- Abhören von Raumgesprächen über Mobiltelefonen
- Einsatz veralteter Mobiltelefone

Priorisierung	R2
Hinweis zum besseren Verständnis	Abarbeitung des Bausteins nur sinnvoll, wenn im Unternehmen noch reine Mobiltelefone eingesetzt werden.
Anforderungen	SYS.3.3.A1 – A4

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und Speicherkarten
Zu SYS.3.3.A4:
SIM-Karten enthalten in den meisten Fällen personenbezogenen Daten in den Kontakten bzw. Adressbüchern. Hier ist die Umsetzung der Datenschutzrichtlinie im Unternehmen erforderlich, da sonst Bußgelder drohen.

SYS.3.4
Mobile Datenträger.

Immer unterwegs und Daten sicher transportieren, speichern oder nutzen – dabei unterstützen mobile Datenträger wie externe Festplatten, CD-ROMs, DVDs, Speicherkarten, Magnetbänder und USB-Sticks. Wer die Risiken im Umgang mit ihnen reduzieren möchte, schult die Kompetenzen der Anwender und Anwenderinnen.

Minimieren Sie diese Risiken:

- Sorglosigkeit im Umgang mit Informationen
- Unzureichende Kenntnis über Regelungen
- Datenverlust bei mobilem Einsatz
- Defekte Datenträger
- Diebstahl
- Beeinträchtigung durch wechselnde Einsatzumgebung
- Verbreitung von Schadprogrammen
- Datendiebstahl mit mobilen Datenträgern

Priorisierung	R2
Hinweis zum besseren Verständnis	Mobile Geräte (Datenträger, Smartphones, Tablets etc.) sind stets der Verlustgefahr ausgesetzt. Da auf diesen Geräten des Öfteren personenbezogene Daten der Kunden bzw. Mitarbeiter gespeichert sind, muss hier auch der Datenschutz und dessen Regelungen im Unternehmen umgesetzt und überwacht werden. Werden auf den mobilen Datenträgern personenbezogene Daten gespeichert MÜSSEN auch die Standard-Anforderungen A4-A7 auf Grund des Datenschutzes umgesetzt werden.
Anforderungen	SYS.3.4.A1 – A3; empfohlen: A4 – A7

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

SYS.3.4.A3 Sicherungskopie der übermittelten Daten
Zu SYS.3.4.M3:
Sollte die Sicherungskopie personenbezogene Daten beinhalten, muss auch diese Kopie bei Wegfalls des Zwecks zur Bearbeitung dieser personenbezogenen Daten gelöscht werden. Eine Beschreibung der übermittelten Daten wäre hier ratsam, da die Beschreibung zur schnelleren Erstellung einer Kopie der abhandengekommener Daten führt, aber gleichzeitig nicht gelöscht werden muss, da sie keine personenbezogene Daten beinhaltet.

SYS

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte.

Für viele Aufgaben im Betrieb wird immer noch Papier als Informationsträger genutzt. Drucker, Kopierer, Multifunktionsgeräte und Scanner sind damit wichtige Komponenten in der IT-Infrastruktur. Fallen die Geräte aus, kann sich das mitunter auf kritische Prozesse auswirken und zu erheblichen wirtschaftlichen Schäden führen. Drucker und Multifunktionsgeräte sind oft „kleine" Server mit eigenem Betriebssystem. Da die Geräte häufig vertrauliche Informationen verarbeiten, müssen sie bzw. die gesamte Druck- und Scan-Infrastruktur entsprechend geschützt werden.

Minimieren Sie diese Risiken:

- Unerlaubte Einsicht in ausgedruckte Dokumente
- Sichtbarkeit von Metadaten
- Ungenügender Schutz gespeicherter Informationen
- Unverschlüsselte Kommunikation
- Unberechtigter Versand von Informationen
- Unberechtigtes Kopieren und Scannen von Informationen
- Fehlende Netztrennung
- Mangelhafter Zugriffsschutz zur Geräteadministration
- Manipulation des Betriebssystems

Priorisierung	R2
Hinweis zum besseren Verständnis	Alle Ausgabegeräte wie Drucker, Kopierer und Multifunktionsgeräte, die im betrieblichen Netzwerk eingerichtet werden, bedürfen einer sicherheitsrelevanten Einordnung und Konfiguration im Rahmen eines Einsatz- und Sicherheitskonzeptes (siehe dazu SYS.4.1.A4).
Anforderungen	SYS.4.1.A1 – A3; empfohlen: A12

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erstellung eines Basis-Konzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten
Zu SYS.4.1.A1:
Das Basis-Konzept regelt den zulässigen (sicheren) Standort, den Zugriff auf das Gerät und die Art der Absicherung vor der Beschaffung. (IT-Leitung/Geschäftsführung)
Beispiel: MFG-XYZ; Standort: Hinter Empfangstheke; Zentraler Fax-Empfang und -Versand mit Ausdruck, Dokumentenscanner für Eingangspost mit drei Ablage-Speicherplätzen im Netzwerk für Vertrieb, Techn. Büro, Buchhaltung; Zugriff auf MFG-XYZ: Empfangs-MA Abel und Brem sowie Administration mit Passwort.

Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte
Zu SYS.4.1.A2:
Aufstellung, Konfiguration und Zugriffssystem stellen sicher, dass nur berechtigte Personen die Geräte benutzen, darauf zugreifen und sie administrieren können. Im Falle des Fernwartung, sind die Hinweise OPS.2.4.A1 – A5 zu berücksichtigen.

Regelmäßige Aktualisierung von Druckern, Kopieren und Multifunktionsgeräten
Zu SYS.4.1.A3:
Das Einspielen von Patches und Updates aus sicheren Quellen stellt sicher, dass Sicherheitslücken geschlossen bzw. die Sicherheitskonzepte (siehe auch SYS.4.1.A4) weiterhin greifen.

Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln
Zu SYS.4.1.A12:
Vor Rücknahme oder Entsorgung der Geräte sind alle Speichermedien der Geräte sicher zu löschen oder die Löschung der Speicher durch Dienstleister vertraglich sicher zu stellen.

Bei kleinen Handwerksbetrieben stellt die Geschäftsleitung die Handhabung nach den Anforderungen sicher. Mit Dienstleistern sind entsprechende Verträge zum Geräte-, Datenschutz und der IT-Sicherheit abzuschließen (siehe Datenschutz-Grundverordnung, EU-DSGVO).

SYS.4.4
Allgemeines IoT-Gerät.

Das Internet der Dinge/Internet of Things (IoT) ist ein wichtiger Faktor in der Digitalisierung. „Smarte“ IoT-Geräte sind in der Regel an Datennetze angeschlossen, häufig drahtlos, und können auf das Internet zugreifen oder sind darüber erreichbar. Das hat Auswirkungen auf die Informationssicherheit im Unternehmen. Ziel ist es, einen unautorisierten Datenabfluss sowie eine Manipulation der Geräte zu verhindern.

Minimieren Sie diese Risiken:

- Ausspähung über IoT-Geräte
- Verwendung von UPnP
- Schäden Dritter
- Spionageangriffe mittels Hintertüren in IoT-Geräten

Priorisierung	R2
Hinweis zum besseren Verständnis	Alle IoT-Geräte, die im betrieblichen Netzwerk als eigenständige Einheit eingerichtet werden, bedürfen einer sicherheitsrelevanten Einordnung und Konfiguration im Rahmen eines Einsatz- und Sicherheitskonzeptes. Dabei ist zu beachten, dass folgende Funktionen bei jedem Gerät verfügbar sind: Zugriff nur mit Authentifizierung, Updatefähigkeit und ein Hersteller-Update-Prozess, veränderbare Standard-Passwörter. Immer wichtiger wird bei komplexen Systemen eine Lifetime-Betrachtung, d.h. Dokumentation aller System-Elemente mit den Kenndaten, Daten zur Inbetriebnahme, den Updates, Austausch von Elementen und vorhersehbaren Umwelteinflüssen. Nur dann kann eine Bewertung der IT-Sicherheit mit IoT-Geräten erfolgen und sichergestellt werden.
Anforderungen	SYS.4.4.A1 – A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Einsatzkriterien für IoT-Geräte
Zu SYS.4.4.A1:
Die Einsatzkriterien definieren den zulässigen Standort, den Zugriff auf das Gerät, die Art der Absicherung und vorhersehbare Umwelteinflüsse vor der Beschaffung.

Authentisierung
Zu SYS.4.4.A2:
Die Absicherung bzw. Authentisierung stellen sicher, dass nur berechtigte Personen die Geräte benutzen, darauf zugreifen und sie administrieren können.

Regelmäßige Aktualisierung
Zu SYS.4.4.A3:
Das Einspielen von Patches und Updates aus sicheren Quellen stellt sicher, dass Sicherheitslücken geschlossen bzw. die Sicherheitskonzepte weiterhin greifen.

Aktivieren von Autoupdate-Mechanismen
Zu SYS.4.4.A4:
Auto-Update-Mechanismen sichern die Aktualität der Funktionalität von IoT-Geräten. Alternativen sind zyklische manuelle Wartungen oder Softwareverteilsysteme.

Einschränkung des Netzzugriffs
Zu SYS.4.4.A5:
Einschränkung des Netzverkehrs von IoT-Geräten erreicht man am einfachsten durch Einrichtung von Virtuellen Privaten Netzwerken (VPN), die über die eingesetzte Router oder Switch-Technik konfiguriert werden. Innerhalb dieser VPN bleiben die IoT-Geräte separiert.

IND.2.1
Allgemeine ICS-Komponente.

Industrielle Steuerungssysteme (engl.: Industrial Control System, ICS) sind vielfältigen Gefährdungen ausgesetzt: Sie reichen von physikalischen Schäden über unsichere Konfigurationen sowie Schadprogramme bis zu gezielter Spionage und Sabotage. ICS-Komponenten sind umfassend zu sichern.

Minimieren Sie diese Risiken:

- Beeinträchtigung durch schädliche Umgebungseinflüsse
- Unvollständige Dokumentation
- Unsichere Systemkonfiguration
- Unzureichendes Benutzer- und Berechtigungsmanagement
- Unzureichende Protokollierung
- Manipulation und Sabotage einer ICS-Komponente
- Einsatz unsicherer Protokolle
- Denial-of-Service-(DoS)-Angriffe (Angriffe gegen die Verfügbarkeit von Systemen)
- Schadprogramme
- Ausspionieren von Informationen
- Unzureichende Sicherheitsanforderungen bei der Beschaffung
- Manipulierte Firmware

Priorisierung	R2
Hinweis zum besseren Verständnis	Auf diesem Baustein basieren die Bausteine IND 2.2, 2.3 und 2.4.
Anforderungen	IND.2.1.A1 – A6

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

IND

IND.2.2 Speicherprogrammierbare Steuerung (SPS).

Eine speicherprogrammierbare Steuerung (SPS) ist eine elektronische Komponente, die Steuerungs- und Regelaufgaben in der Betriebstechnik übernimmt. Eine besondere Herausforderung besteht darin, dass die Dokumentation zu den Steuerungen häufig unvollständig ist. Das erschwert die Gefährdungsanalyse, da Schnittstellen, Funktionen sowie sicherheitsrelevante Mechanismen übersehen werden.

Minimieren Sie diese Risiken:

- Unvollständige Dokumentation

Priorisierung	R2
Hinweis zum besseren Verständnis	Alle SPS-Systeme mit direkten und indirekten Zugangssystemen, bedürfen einer sicherheitsrelevanten Einordnung und Konfiguration im Rahmen eines Einsatz- und Sicherheitskonzeptes.
Anforderungen	Empfohlen: IND.2.2.A1 – A3

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erweiterte Systemdokumentation für speicherprogrammierbare Steuerungen
Zu IND.2.2.A1:
Die Systemdokumentation sollte jede Veränderung versionieren und dokumentieren.

Benutzerkontenkontrolle und restriktive Rechtevergabe
Zu IND.2.2.A2:
Die Pflege und Aktualisierung des Berechtigungssystems stellt sicher, dass nur berechtigte Personen die Geräte und Programme benutzen, darauf zugreifen und verändern können. Beachtet werden muss dabei die Passwort-Änderung bei Personalfluktuation.

Zeitsynchronisation
Zu IND.2.2.A3:
Die automatisierte, zentrale Zeitsynchronisation stellt das zeitgemäße Funktionieren der einzelnen Programmteile und der Programmteile zueinander sicher.

Zu Beachten sind bei allen elektronischen Steuerungen die aktuellen Normen zum Überspannungsschutz und zum Brandschutz. Der Überspannungsschutz wurde zuletzt 12/2018 für Eigenheime und kleine Gewerbebauten erweitert. DIN VDE 0100-443 und DIN VDE 0100-534.

Bei kleinen Handwerksbetrieben stellt die Geschäftsführung die Handhabung nach den Anforderungen sicher. Mit Dienstleistern sind entsprechende Verträge zum Geräte-, Datenschutz und zur IT-Sicherheit abzuschließen (siehe auch DSGVO).

IND.2.3
Sensoren und Aktoren.

„Wehret den Anfängen…“: Schon bei der Beschaffung von Sensoren muss Informationssicherheit berücksichtigt werden, da sie schwerwiegende Schwachstellen enthalten können, die sich später nur sehr aufwändig beheben lassen. Sensoren für industrielle Komponenten sind häufig besonderen Bedingungen extreme Wärme, Kälte, Feuchtigkeit, Staub, Vibration ausgesetzt, die den sicheren Betrieb beeinträchtigen können. Dadurch können die Sensoren schneller verschleißen und früher ausfallen oder fehlerhafte Werte messen.

Minimieren Sie diese Risiken:

- Unzureichende Sicherheitsanforderungen bei der Beschaffung

Priorisierung	R2
Hinweis zum besseren Verständnis	Alle Sensoren und Aktoren, die als eigenständige Einheit oder Teil einer Einheit eingerichtet werden, bedürfen einer sicherheitsrelevanten Einordnung und Konfiguration im Rahmen eines Einsatz- und Sicherheitskonzeptes. Dabei sollte Berücksichtigung finden: Produktsicherheit, Schnittstellen-Auswahl und Absicherung bzw. Authentisierung, Robustheit entsprechend dem eingesetzten Zweck und der Umgebung.
Anforderungen	IND.2.3.A1

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Installation von Sensoren
Zu IND.2.3.A1:
Alle Sensoren und Aktoren stellen im System auch einen Angriffspunkt dar, so dass bei der Auswahl der Schnittstelle und dem Zugriffsverfahren dem Einsatz- und Sicherheitskonzept zu entsprechen ist. Der Zugriffsschutz ist mit sicheren Passwörtern zu realisieren. Immer schwieriger wird die systematische Aufrechterhaltung der IT-Sicherheit bei Systemveränderungen und beim Austausch bzw. Ersatz von defekten Bauteilen über die gesamte Lebenszeit. Eine detaillierte System-Dokumentation hilft bei der Aufrechterhaltung der IT-Sicherheit.

Bei kleinen Handwerksbetrieben stellt die Geschäftsleitung die Handhabung nach den Anforderungen sicher. Mit Dienstleistern sind entsprechende Verträge zum Geräte-, Datenschutz und IT-Sicherheit abzuschließen (siehe EU-DSGVO).

IND.2.4 Maschine.

Ungenügende Wartung oder gezielte Manipulation – Der Ausfall einer Maschine bedeutet für den Betrieb ein hohes Risiko. Es gilt, elektronisch gesteuerte, halb- oder vollautomatische Maschinen (z. B. CNC-Maschinen) mit geeigneten Maßnahmen abzusichern.

Minimieren Sie diese Risiken:

- Ausfall oder Störung durch ungenügende Wartung
- Gezielte Manipulationen

Priorisierung	R2
Hinweis zum besseren Verständnis	Alle Maschinen, die im betrieblichen Netzwerk konfiguriert sind, bedürfen einer sicherheitsrelevanten Einordnung und Konfiguration im Rahmen eines Einsatz- und Sicherheitskonzeptes. Entsprechend sind auch Wartungsplanung und -ausführung, Fernwartungszugang, weitere Schnittstellen der Maschinen sowie deren Zugriff bzw. Nutzung zu dokumentieren.
Anforderungen	IND.2.4.A1 – A2

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Fernwartung durch Maschinen- und Anlagenbauer
Zu IND.2.4.A1:
Der Fernwartungszugang wie auch weitere Schnittstellen müssen durch ein sicheres Zugriffsverfahren (s. auch OPS.2.4, ORB.4) geschützt, sowie jeder Zugriff protokolliert werden.

Betrieb nach Ende der Gewährleistung
Zu IND.2.4.A2:
Für den Betrieb der Maschinen nach der Gewährleistungsfrist ist durch eine vorsorgende Wartungsplanung und -überwachung der funktionierende Betrieb sicherzustellen.

Bei kleinen Handwerksbetrieben stellt die Geschäftsführung die Handhabung nach den Anforderungen sicher. Mit Dienstleistern sind entsprechende Verträge zum Geräte-, Datenschutz und der IT-Sicherheit abzuschließen. Alles weitere Regeln die Umsetzungshinweise zu den STANDARD-Anforderungen IND.2.4.A3.

NET.1.1
Netzarchitektur und -design.

„Mit Netz und doppeltem Boden“: Die meisten Betriebe benötigen heute für ihren Geschäftsbetrieb Rechnernetze, die herkömmliche sowie mobile Endgeräte und IoT-Geräte („Internet der Dinge“), Cloud-Dienste miteinander verbinden. Aber durch die vielen Endgeräte und Dienste steigen auch die Risiken. Eine sichere Netzarchitektur ist die Basis für die Informationssicherheit im Unternehmen.

Minimieren Sie diese Risiken:

- Ausfall oder unzureichende Performance von Kommunikationsverbindungen
- Ungenügend abgesicherte Netzzugänge
- Unsachgemäßer Aufbau von Netzen

Priorisierung	R2
Hinweis zum besseren Verständnis	Ein sicheres Netzwerk ist wesentlicher Bestandteil zum Schutz der Daten, IT-Systeme und Maschinen. Netzwerkarchitektur – und -design im Handwerksbetrieb müssen daher gut geplant, zeitnah aufgebaut und sicher betrieben werden. Ein sicheres und durchdachtes Netzwerkkonzept sollte daher schon am Anfang, bei der Entwicklung eines IT-Sicherheitskonzeptes, für den Handwerksbetrieb entwickelt und umgesetzt werden. Es bildet die Basis für viele weitere technische IT-Sicherheitsmaßnahmen.
Anforderungen	NET.1.1.A1 – A15

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Sicherheitsrichtlinie für das Netz
Zu NET.1.1.A1:
Diese Richtlinie definiert die Anforderungen und Vorgaben für das sichere Netzwerk im Handwerksbetrieb. Sie ist als Ergänzung zur allgemeinen Sicherheitsrichtlinie des Handwerksbetriebs (IS-Leitlinie) zu sehen.

Wann werden Sicherheitszonen segmentiert?

Wann werden Benutzergruppen bzw. Mandanten logisch oder sogar physisch getrennt?

Welche Kommunikationsbeziehungen und welche Netz- und Anwendungsprotokolle sind jeweils zugelassen?

Wie wird der Datenverkehr für Administration und Überwachung netztechnisch getrennt?

Welche firmeninterne und standortübergreifende Kommunikation (WAN, Funknetze) ist erlaubt?

Welche Verschlüsselung im WAN, LAN oder auf Funkstrecken ist erforderlich?

Welche firmenübergreifende Kommunikation ist zugelassen?

Die Sicherheitsrichtlinie für das Netz ist zu dokumentieren und regelmäßig auf korrekte Umsetzung zu prüfen.

Diese Richtlinie sollte gemeinsam mit NET.1.1.A3, NET.1.1.A13, NET.1.1.A14, NET.1.1.A16 und NET.1.1.A17 betrachtet und bearbeitet werden.

Dokumentation des Netzes
Zu NET.1.1.A2:
Zwei Dokumentationen sind erforderlich. Logische (Netzwerkplan) und physikalische (Raumplan) Dokumentation des Netzes. Der Netzwerkplan und der Raumplan sollten aktuell und vollständig sein. Änderungen müssen aufgeführt sein.

Anforderungsspezifikation für das Netz
Zu NET.1.1.A3:
Wird basierend auf die Sicherheitsrichtlinie für das Netz (NET.1.1.A1) erstellt. Hieraus MÜSSEN sich dann alle wesentlichen Elemente für Netzarchitektur und -design ableiten.

Netztrennung in Sicherheitszonen
Zu NET.1.1.A4:
Das Firmennetz MUSS in Sicherheitszonen unterteilt werden. Es sind mindestens drei Sicherheitszonen erforderlich: internes Netz, Demilitarisierte Zone (DMZ) und WAN (für Internetzugang). Weitere Zonen: Smart Home Produkte, IoT, VoIP etc. Die Zonenübergänge müssen durch eine Firewall abgesichert werden.

Client-Server-Segmentierung
Zu NET.1.1.A5:
Endgeräte (stationäre und mobile) und Server-Systeme MÜSSEN sich in unterschiedlichen Netzwerksegmenten befinden.

Endgeräte-Segmentierung im internen Netz
Zu NET.1.1.A6:
Es dürfen nur Endgeräte in einem Sicherheitssegment positioniert werden, die einem ähnlichen Sicherheitsniveau entsprechen.

Absicherung von schützenswerten Informationen
Zu NET.1.1.A7:
Schützenswerte Informationen (Daten) sollten bei der „Bestandsaufnahme“ ermittelt werden. Eine sichere Datenübertragung dieser Informationen im Netzwerk ist durch technische Maßnahmen, wie HTTPS-Transfer oder VPN-Techniken, zu realisieren.

Grundlegende Absicherung des Internetzugangs
Zu NET.1.1.A8:
Hierfür eignet sich ein Sicherheitsgateway.

Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen
Zu NET.1.1.A9:
Spielt z. B. eine Rolle, wenn Cloud-Dienste genutzt werden.

DMZ-Segmentierung für Zugriffe aus dem Internet
Zu NET.1.1.A10:
Die Demilitarisierte Zone (DMZ) enthält IT-Systeme, auf die aus dem Internet zugegriffen werden kann. Dazu zählen z. B. VPN-Server, E-Mail-Server, eigener Web-Server. Über Firewall-Regeln muss sichergestellt sein, dass Systeme in der DMZ nie selbst auf das firmeninterne Netz zugreifen können.

Absicherung eingehender Kommunikation vom Internet in das interne Netz
Zu NET.1.1.A11:
Hier kommen VPN-Lösungen, aber auch herstellerspezifische Lösungen zum Einsatz. Sicherheitsgateways stellen auch hierfür eine ideale Lösung dar.

Absicherung ausgehender interner Kommunikation zum Internet
Zu NET.1.1.A12:
Die Anforderungen werden durch ein richtig konfiguriertes Sicherheitsgateway mit Proxy-Funktion erfüllt.

Regelmäßiger Soll-Ist-Vergleich
Zu NET.1.1.A15:
Spätestens alle zwei Jahre sollte das bestehende Netzwerk auf Aktualität hin überprüft werden.

NET.2.1 WLAN-Betrieb.

„Kann ich Ihr WLAN nutzen?“ Ob als lokales Netz im Betrieb oder temporär auf einer Messe oder Veranstaltung – drahtlose Netze gehören zum betrieblichen Alltag. Der sichere Aufbau und Betrieb eines WLAN ist notwendig dafür, dass auch die angebundenen Geräte vor Cyber-Risiken geschützt sind.

Minimieren Sie diese Risiken:

- Ausfall oder Störung eines Funknetzes
- Fehlende oder unzureichende Planung des WLAN-Einsatzes
- Fehlende oder unzureichende Regelungen zum WLAN-Einsatz
- Ungeeignete Auswahl von Authentisierungsverfahren
- Fehlerhafte Konfiguration der WLAN-Infrastruktur
- Unzureichende oder fehlende WLAN-Sicherheitsmechanismen
- Abhören der WLAN-Kommunikation
- Vortäuschung eines gültigen Access Points (Rogue Access Point)
- Ungeschützter LAN-Zugang am Access Point
- Hardware-Schäden
- Diebstahl eines Access Points

Priorisierung	R2
Hinweis zum besseren Verständnis	Der Baustein NET.2.1 WLAN-Betrieb enthält grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn im Handwerksbetrieb WLAN aufgebaut und betrieben werden. Die Anforderungen für eine sichere Nutzung von WLAN wird im Baustein NET.2.2 WLAN-Nutzung behandelt. Beide Bausteine MÜSSEN somit im Handwerksbetrieb umgesetzt werden.
Anforderungen	NET.2.1.A1 – A8; empfohlen A9 – A14

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Aufgrund des Stands der Technik SOLLTEN die Basis- und die Standard-Anforderungen umgesetzt werden. Für die planerischen Anforderungen dieses Bausteins ist die Unterstützung durch den IT-Sicherheitsberater des Handwerkbetriebs erforderlich. Die technische Umsetzung SOLLTE nur durch autorisierte Personen erfolgen, damit zusätzliche Gefahren z. B. durch eine fehlerhafte Konfiguration vermieden werden.

Auswahl eines geeigneten WLAN-Standards
Zu NET.2.1.A2:
WLANs können im 2,4 und/oder 5 GHz-Band betrieben werden. Die höchste Übertragungsrate wird dabei im 5 GHz-Band erreicht. Für die Reichweite gibt es mehrere Einflussfaktoren (Störquellen), die berücksichtigt werden müssen. Die Sicherheits-Standards für WLANs sind zu bewerten.

Auswahl geeigneter Kryptoverfahren für WLAN
Zu NET.2.1.A3:
WPA2 gilt seit Oktober 2017 als nicht mehr sicher. Daher sollte zukünftig auf WPA-3-Produkte gesetzt werden. Hier sollten sich die Verantwortlichen über die aktuelle Sicherheitslage informieren und die Gefahrenlage für ihren Betrieb bewerten (Risikoabschätzung).

Sichere Basis-Konfiguration der WLAN-Clients
Zu NET.2.1.A6:
Geeignete Anforderungen für eine sichere Konfiguration von Clients sind bereits in den Bausteinen SYS.2.1 Allgemeiner Client und NET.2.2 WLAN-Nutzung zu finden.
Zusätzliche Anforderungen werden hier definiert.

Geeignete Auswahl von WLAN-Komponenten
Zu NET.2.1.A11:
In regelmäßigen Abständen werden in IT-Fachzeitschriften WLAN-Komponenten diverser Hersteller vorgestellt und verglichen. Dadurch lässt sich schnell ein aktueller Produktüberblick gewinnen.

NET

NET.2.2 WLAN-Nutzung.

WLANs bieten einen Gewinn an Komfort und Mobilität. Allerdings birgt die Nutzung eines drahtlosen Netzes ein zusätzliches Gefährdungspotenzial für die Sicherheit der Informationen. Daher ist es unabdingbar, dass neben den IT-Verantwortlichen auch die Benutzer und Benutzerinnen zu möglichen Gefahren sensibilisiert sind, die entstehen können, wenn WLANs unsachgemäß verwendet werden.

Minimieren Sie diese Risiken:

- Unzureichende Kenntnis über Regelungen
- Nichtbeachtung von Sicherheitsmaßnahmen
- Abhören der WLAN-Kommunikation
- Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation
- Vortäuschung eines gültigen Access Points (Rogue Access Point)

Priorisierung	R2
Hinweis zum besseren Verständnis	WLAN-Nutzung ist ein wichtiger Baustein bei firmeninternen WLANs bzw. auch für die Nutzung von externen WLANs, sei es als Gastzugang in fremden Firmen oder bei öffentlichen Hotspots. Für die Informationssicherheit spielt vor allem das Verhalten des WLAN-Benutzers eine entscheidende Rolle.
Anforderungen	NET.2.2.A1 – A3

NET

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erstellung einer Benutzerrichtlinie für WLAN
Zu NET.2.2.A1:
Bevor WLANs betrieben und benutzt werden, ist eine sorgfältige Planung notwendig. Für die Zielgruppe WLAN-Benutzer sollte eine spezielle WLAN-Richtlinie erstellt werden.

Die Benutzerrichtlinie für WLAN gilt als Ergänzung der allgemeinen Sicherheitsrichtlinie des Handwerksbetriebes (IS-Leitlinie). In der Benutzerrichtlinie ist zum Beispiel auch beschrieben, ob und wie Hotspots von den Beschäftigten genutzt werden dürfen.

Die Benutzerrichtlinie beschreibt u. a. ...
Die Besonderheiten bei der WLAN-Nutzung
- Mit welchen internen und externen Netzen die WLAN-Clients verbunden werden dürfen
- Unter welchen Rahmenbedingungen sie sich an internen oder externen WLANs anmelden dürfen
- Ob und wie Hotspots genutzt werden dürfen
- Dass der Ad-hoc-Modus abzuschalten ist, damit kein anderer Client direkt auf die WLAN-Clients zugreifen kann
- Welche Schritte bei (vermuteter) Kompromittierung der WLAN-Clients zu unternehmen sind
- Wer zu benachrichtigen ist

Beschreibt auch, wie mit clientseitigen Sicherheitslösungen umzugehen ist. Dazu gehört z. B., dass
- Keine sicherheitsrelevanten Konfigurationen verändert werden dürfen
- Eine vorhandene Firewall nicht abgeschaltet werden darf
- Alle Freigaben von Verzeichnissen oder Diensten deaktiviert oder zumindest durch gute Passwörter geschützt sind
- Für die Nutzung externer WLANs nach Möglichkeit nur spezielle Benutzerkonten mit restriktiver Rechtevergabe verwendet werden sollten
- Enthält ein klares Verbot, ungenehmigt WLAN Access Points an das Firmennetz anzuschließen.
- Den Umgang mit der WLAN-Schnittstelle
- Welche Daten in WLANs genutzt und übertragen werden dürfen

Sensibilisierung und Schulung der WLAN-Benutzer
Zu NET.2.2.A2:
Ziele: Um die Sicherheitsanforderungen des Handwerksbetriebs in der täglichen Nutzung von WLANs zu erfüllen, müssen die Benutzer mit eingebunden werden.

Alle Benutzer, inklusive der Leitung des Handwerksbetriebes, MÜSSEN über WLAN-Grundlagen informiert und zu möglichen Gefahren sensibilisiert sein, die entstehen können, wenn WLANs unsachgemäß verwendet werden. Sie MÜSSEN über die erforderlichen Kenntnisse verfügen, um Sicherheitsmaßnahmen richtig verstehen und anwenden zu können. Allen Benutzern MUSS bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in bestimmten Situationen bei der Nutzung von WLANs reagieren sollten. Alle Benutzer sollten öffentliche Hotspots grundsätzlich meiden und wenn dennoch erforderlich, nur Virtual Private Network (VPN) nutzen.

Absicherung der WLAN-Nutzung in unsicheren Umgebungen
Zu NET.2.2.A3:
Allgemeines: Hotspots sollten immer als unsicheres Netz betrachtet werden. Es ist daher zu empfehlen, die Nutzung von Hotspots durch die WLAN-Sicherheitsrichtlinie (NET.2.2.A1) vollständig zu verbieten.

Dürfen externe Hotspots verwendet werden, dann müssen die Beschäftigten gezielt hinsichtlich der Hotspot-Nutzung geschult werden und entsprechende Maßnahmen umsetzen, die in NET.2.2.A3 Absicherung der WLAN-Nutzung in unsicheren Umgebungen beschrieben werden. Über fremde WLANs (z. B. bereitgestellte Gastzugänge fremder Firmen, öffentliche Hotspots) dürfen die Benutzer nur über VPN auf interne Ressourcen im Unternehmen zugreifen. Weitere Informationen hierzu sind im Baustein NET.3.2 VPN zu finden.

NET

NET.3.1
Router und Switches.

Router und Switches bilden das Rückgrat moderner IT-Netze. Ein Ausfall eines oder mehrerer dieser Geräte kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Sie müssen daher besonders abgesichert werden.

Minimieren Sie diese Risiken:

- Distributed Denial of Service - DdoS (Angriffe gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen)
- Manipulation
- Software-Schwachstellen oder -Fehler
- Fehlerhafte Konfiguration eines Routers oder Switches
- Fehlerhafte Planung und Konzeption
- Inkompatible aktive Netzkomponenten
- MAC-Flooding (Angriff mit wechslenden Quell-Mac-Adressen)
- Spanning-Tree-Angriffe (Bösartiger Switch als Root Bridge)
- GARP-Attacken (Angriff mit dem Ziel des Mitschnitts oder der Manipulation von Kommunikation)

Priorisierung	R2
Hinweis zum besseren Verständnis	Für den sicheren Einsatz von Router und Switches müssen auch andere Bausteine aus den Schichten NET Netzkomponenten und INF Infrastruktur berücksichtigt werden. Die Entwicklung und Umsetzung der Bausteine sollten vom IT-Sicherheitsberater unterstützt und nur durch autorisierte Personen erfolgen.
Anforderungen	NET.3.1.A1 – A9; empfohlen A10 – A23

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erstellung einer Sicherheitsrichtlinie
Zu NET.3.1.A10:
Die Sicherheitsrichtlinie für Router und Switches dient als Ergänzung der IS-Leitlinie des Handwerksbetriebes.

Beschaffung eines Routers oder Switches
Zu NET.3.1.A11:
Vor der Beschaffung sollten ein Anforderungskatalog erstellt werden. Damit kann über einschlägige IT-Fachzeitschriften ein Produktvergleich durchgeführt werden.

Erstellung einer Konfigurations-Checkliste für Router und Switches
Zu NET.3.1.A12:
Die sichere Konfiguration der Router und Switches ist stark vom Einsatzzweck abhängig. Dies beeinflusst die Anforderungen.

Administration über ein gesondertes Managementnetz
Zu NET.3.1.A13:
Diese Anforderung gilt ebenso für Firewalls und Sicherheitsgateways. Es gilt für den Handwerksbetrieb zu überlegen, den Baustein NET.1.2 Netzmanagement auch mit zu berücksichtigen.

Sicherung von Switch-Ports
Zu NET.3.1.A19:
Die Ports sind vor unbefugten, nicht berechtigten Anschlüssen bzw. Zugriffen zu schützen. Hierauf sollte stets geachtet werden.

Sicherheitsaspekte von Routing-Protokollen
Zu NET.3.1.A20:
Diese Anforderung betrifft in erster Linie größere Handwerksbetriebe mit mehreren gerouteten Netzsegmenten und mehreren einzelnen Routern. Bei herkömmlichen Netzen sind die Routingeigenschaften in einem Sicherheitsgateway integriert und dabei spielen die genannten Aspekte von Routing-Protokollen keine so große Rolle.

Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur
Zu NET.3.1.A21:
Hierzu siehe auch ORP.4 Identitäts- und Berechtigungsmanagement.

Notfallvorsorge bei Routern und Switches
Zu NET.3.1.A22:
Da es sich bei Routern und Switches um wichtige IT-Systeme im Netzwerk handelt, müssen sie im Notfallmanagement bedacht werden. Sie sind also genau so zu betrachten, wie z. B. Firewalls und Sicherheitsgateways. Idealerweise existiert hierzu im Handwerksbetrieb ein Notfallordner, indem alles dokumentiert ist. Router und Switches bilden somit ein Kapitel im Notfallordner.

Revision und Penetrationstests
Zu NET.3.1.A23:
Router und Switches sollten genauso wie andere IT-Systeme gepflegt werden. Dazu zählen unter anderem Revision und Penetrationstests.

NET

NET.3.2 Firewall.

„Mit Sicherheit verbunden“ - dafür sorgt die Firewall, ein System aus soft- und hardwaretechnischen Komponenten, das ausschließlich die erwünschten Zugriffe oder Datenströme zwischen verschiedenen Netzen zulassen soll.

Minimieren Sie diese Risiken:

- Distributed Denial of Service - DdoS (Angriffe gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen)
- Manipulation
- Software-Schwachstellen oder -Fehler
- Umgehung der Firewall-Regeln
- Fehlerhafte Konfiguration und Bedienungsfehler einer Firewall

Priorisierung	R2
Hinweis zum besseren Verständnis	Die Planung einer Firewall-Struktur, die Auswahl von Firewall-Systemen sowie das Einrichten und der Betrieb von Firewalls sind ein sehr komplexes Thema. Daher sollte sich der Handwerksbetrieb sehr früh nach einem kompetenten Dienstleister umschauen. Viele kleinere IT-Dienstleister sind damit heute noch, mangels Fachwissen, überfordert. Der IT-Sicherheitsberater des Handwerksbetriebs muss hierbei unterstützen.
Anforderungen	NET.3.2.A1 – A15; empfohlen A16 – A24

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Erstellung einer Sicherheitsrichtlinie
Zu NET.3.2.A1:
Die Sicherheitsrichtlinie für Firewalls ist eine Ergänzung der allgemeinen Sicherheitsrichtlinie (IS-Leitlinie) des Handwerkbetriebes. Für die Sicherheitsrichtlinie ist der Informationssicherheitsbeauftragte (ISB) des Unternehmens verantwortlich. Da diese Funktion meist in einem Handwerksbetrieb nicht besetzt ist, wird externe Unterstützung benötigt.

Festlegen der Firewall-Regeln
Zu NET.3.2.A2:
Firewall-Regeln werden vom Handwerksbetrieb und dem IT-Sicherheitsberater und optional IT-Dienstleister gemeinsam entwickelt.

Einrichten geeigneter Filterregeln am Paketfilter
Zu NET.3.2.A3:
Die Paketfilter-Firewall MUSS weitere Kriterien erfüllen, die bei der Produktauswahl in NET.2.2.A15 Beschaffung einer Firewall berücksichtigt werden MÜSSEN.

Sichere Konfiguration der Firewall
Zu NET.3.2.A4:
Für die sichere Konfiguration der Firewall gilt das KISS-Prinzip (Keep it small and simple).

Restriktive Rechtevergabe
Zu NET.3.2.A5:
Dazu dürfen nur so wenig Rechte wie erforderlich (Need to know-Prinzip) vergeben werden.

Schutz der Administrationsoberflächen
Zu NET.3.2.A6:
Die aufgeführten Anforderungen sind bei der Planung des Firmen-Netzwerkes zu berücksichtigen.

Notfallzugriff auf die Firewall
Zu NET.3.2.A6:
Es MUSS immer möglich sein, direkt auf die Firewall zugreifen zu können, sodass weiterhin lokal gearbeitet werden kann, auch wenn das lokale Netz ausfällt.

Unterbindung von dynamischem Routing
Zu NET.3.2.A8:
Dieser Parameter MUSS bei der Produktauswahl mit berücksichtigt werden (NET.3.2.A15 Beschaffung einer Firewall). Die Einstellung erfolgt durch den IT-Spezialisten.

Protokollierung
Zu NET.3.2.A9:
Logging und Monitoring ist wichtig um Engpässe zu erkennen, sich ein aktuelles Bild über die „Sicherheitslage im Netzwerk“ zu verschaffen oder später auch Angriffe rekonstruieren zu können.

Abwehr von Fragmentierungsangriffen am Paketfilter
Zu NET.3.2.A10:
Dieser Schutzmechanismus MUSS bei Produktauswahl mit berücksichtigt werden und ist im Gerät zu aktivieren. Dieses Feature ist in vielen Geräten heutzutage automatisch aktiviert.

Einspielen von Updates und Patches
Zu NET.3.2.A11:
In OPS.1.1.3 Patch- und Änderungsmanagement sind Verfahren für das Einspielen von Updates und Patches definiert. Hier greifen die gleichen Gesetze für die Verantwortlichen.

Vorgehen bei Sicherheitsvorfällen
Zu NET.3.2.A12:
Notfallvorsorge MUSS auch für Firewalls getroffen werden. Näheres ist unter DER.2.1 Behandlung von Sicherheitsvorfällen und DER.4 Notfallmanagement geregelt.

Regelmäßige Datensicherung
Zu NET.3.2.A13:
Die regelmäßige Datensicherung ist zwingend. Automatisierte Abläufe werden von den meisten Produkten heutzutage unterstützt und müssen nur konfiguriert werden.

Betriebsdokumentation
Zu NET.3.2.A14:
Die Einrichtung der Firewalls sowie Konfigurationsänderungen MÜSSEN protokolliert und dokumentiert werden.

Beschaffung einer Firewall
Zu NET.3.2.A15:
Es gibt unterschiedliche Firewall-Realisierungen und Firewalltypen, die abhängig vom Anforderungsprofil verwendet werden können. Aufgrund der Komplexität sollte die Beschaffung der Firewalls, genauso wie die Netzwerkarchitektur und -design (NET.1.1) zusammen mit dem IT-Spezialisten erfolgen.

Aufbau einer „P-A-P“-Struktur
Zu NET.3.2.A16:
Die Anforderungen zum Aufbau einer P-A-P-Struktur werden entweder über separate Firewall-Komponenten aber auch für KMUs über ein Sicherheitsgateway gelöst.

Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter
Zu NET.3.2.A19:
Diese Anforderung MUSS bei der Produktauswahl (NET.3.2.A15) berücksichtigt werden.

Revision und Penetrationstests
Zu NET.3.2.A24:
Die Firewall SOLLTE regelmäßig auf bekannte Schwachstellen (Sicherheitsprobleme) hin überprüft werden.

NET

NET.3.3 VPN.

Wie ein Tunnel zum Schutz von Daten: Mithilfe von Virtuellen Privaten Netzen (VPNs) können Sicherheitsmaßnahmen realisiert werden, um schutzbedürftige Daten über nicht-vertrauenswürdige Netze wie das Internet zu übertragen. Ein VPN ist ein Netz, das physisch innerhalb eines anderen Netzes, wie beispielsweise des Internets, betrieben wird, jedoch logisch von diesem Netz getrennt ist.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Planung und Reglementierung des VPN-Einsatzes
- Unsichere VPN-Dienstleister
- Probleme bei der lokalen Speicherung der Authentisierungsdaten für VPNs
- Unsichere Konfiguration der VPN-Clients für den Fernzugriff
- Unsichere Standard-Einstellungen auf VPN-Komponenten
- Diebstahl von mobilen Endgeräten mit VPN-Client

Priorisierung	R2
Hinweis zum besseren Verständnis	Handwerksbetriebe können mithilfe von Virtuellen Privaten Netzen (VPN) einen sicheren Zugang über nicht-vertrauenswürdige Netze, wie das Internet, ins Firmennetzwerk bewerkstelligen.
Anforderungen	NET3.3.A1 – A5

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Planung des VPN Einsatzes
Zu NET.3.3.A1:
Vor der Einführung eines VPN muss geplant werden, wer verantwortlich für den VPN-Betrieb ist, welche VPN Benutzergruppen welche Berechtigungen haben sollen, und wie Änderungen der Zugriffsberechtigungen zu dokumentieren sind.

Auswahl eines VPN-Dienstleisters
Zu NET.3.3.A2:
Mit einem VPN-Dienstleister muss eine Vereinbarung über den Leistungsumfang (Service Level Agreements – SLAs) angeschlossen und schriftlich dokumentiert werden.

Sichere Installation von VPN-Endgeräten
Zu NET.3.3.A3:
Von einem VPN-Dienstleister muss von qualifiziertem Personal eine sicher VPN-Plattform installiert und vor Inbetriebnahme geprüft werden

Sichere Konfiguration eines VPN
Zu NET.3.3.A4:
Für VPN-Clients, VPN-Server und VPN-Verbindungen muss eine sichere Konfiguration festgelegt und geeignet dokumentiert werden. Der zuständige Administrator muss dies regelmäßig kontrollieren.

Sperrung nicht mehr benötigter VPN-Zugänge
Zu NET.3.3.A5:
Der VPN-Zugriff muss auf die Benutzungszeiten beschränkt und nicht mehr benötigte VPN-Zugänge zeitnah deaktiviert werden.

NET

NET.4.1 TK-Anlagen.

„Sind unsere Telefone sicher?“ Was wie ein Satz aus einem veralteten Spionage-Film klingt, ist dennoch eine berechtigte Frage. Denn Abhören und Gebührenbetrug sind nach wie vor typische Gefahren von Telefon-Anlagen (TK-Anlagen). Deshalb sind einige Sicherheitsaspekte zu berücksichtigen.

Minimieren Sie diese Risiken:

- Abhören von TK-Anlagen
- Abhören von Räumen über TK-Anlagen
- Gebührenbetrug
- Missbrauch frei zugänglicher Telefonanschlüsse

Priorisierung	R2
Hinweis zum besseren Verständnis	In Handwerksbetrieben können Telekommunikationsanlagen (TK-Anlagen) nicht nur zur Sprachtelefonie eingesetzt werden, sondern abhängig vom Endgerät auch Daten, Texte, Grafiken und Bewegtbilder übertragen werden.
Anforderungen	NET.4.1.A1 – A5

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Anforderungsanalyse und Planung für TK-Anlagen
Zu NET.4.1.A1:
Vor der Anschaffung/Erweiterung einer TK-Anlage müssen die Anforderungen geklärt, die Anlage geplant, die Sicherheitsanforderungen abgestimmt und dokumentiert werden. Evtl. werden entsprechende Supportverträge notwendig.

Auswahl von TK-Diensteanbietern
Zu NET.4.1.A2:
Bei der Auswahl eines Anbieters müssen finanzielle und Sicherheitsaspekte berücksichtigt und die Vereinbarungen schriftlich festgehalten werden.

Änderung voreingestellter Passwörter
Zu NET.4.1.A3:
Vor Inbetriebnahme müssen Standardpasswörter durch ausreichend starke Passwörter ersetzt werden.

Absicherung von Remote-Zugängen
Zu NET.4.1.A4:
Externe Zugänge sollten auf das Notwendigste beschränkt sein und müssen vor unberechtigtem Zugang geschützt sein.

Protokollierung bei TK-Anlagen
Zu NET.4.1.A5:
Administrationsarbeiten und systemtechnische Eingriffe müssen protokolliert und regelmäßig kontrolliert werden.

NET

NET.4.2 VoIP.

Voice over IP (VoIP) bezeichnet das Telefonieren über Datennetze, insbesondere über das Internet. Durch die Nutzung des Internets steigen die Ansprüche an die Informationssicherheit. Das erfordert geeignete Schutzmaßnahmen.

Minimieren Sie diese Risiken:

- Fehlerhafte Konfiguration der VoIP-Middleware
- Fehlerhafte Konfiguration der VoIP-Komponenten
- Abhören von Telefongesprächen
- Missbrauch frei zugänglicher Telefonanschlüsse

Priorisierung	R2
Hinweis zum besseren Verständnis	In Handwerksbetrieben kommen heute vermehrt internetbasierte VoIP Anlagen zum Einsatz.
Anforderungen	NET.4.2.A1 – A6

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Planung des VoIP-Einsatzes
Zu NET.4.2.A1:
Vor der Anschaffung einer VoIP Lösung müssen die Anforderungen geklärt und die Anlage und Anbindung ans öffentliche Netz geplant werden. Entsprechende Zeit für die Umstellung ist notwendig.

Sichere Administration der VoIP-Middleware
Zu NET.4.2.A2:
Administrationskonzept mit verschiedenen Rollen und regelmäßigen Updates ist zu erstellen.

Sichere Administration und Konfiguration von VoIP-Endgeräten
Zu NET.4.2.A3:
Sicherheitseinstellungen sind vor Inbetriebnahme zu testen, Konfigurationseinstellungen dürfen nicht verändert und die Softwarekomponenten sollten durch regelmäßige Updates aktualisiert werden.

Einschränkung der Erreichbarkeit über VoIP
Zu NET.4.2.A4:
Externe Zugänge sollten auf das Notwendigste beschränkt sein.
IT-Systeme aus unsicheren Netzen dürfen keine direkten Datenverbindungen auf die VoIP-Komponenten der Institution aufbauen können.

Sichere Konfiguration der VoIP-Middleware
Zu NET.4.2.A5:
Die Konfiguration muss den Sicherheitsanforderungen entsprechen. Die Installation und Konfiguration sind zu dokumentieren und alle nicht benötigten Dienste der VoIP-Middleware müssen deaktiviert werden.

Protokollierung bei VoIP
Zu NET.4.2.A6:
Sicherheitsrelevante Systemereignisse müssen protokolliert werden. Es ist zu entscheiden, welche Informationen dokumentiert werden und wer Zugriff bekommt.

NET.4.3
Faxgeräte und Faxserver.

In vielen Betrieben spielen Faxe immer noch eine wichtige Rolle.
Um die Vertraulichkeit und Integrität der übermittelten Daten zu schützen,
ist es wichtig Maßnahmen gegen den Zugriff bzw. die Manipulation durch
Unbefugte zu implementieren.

Minimieren Sie diese Risiken:

- Unzureichende oder falsche Versorgung mit Verbrauchsgütern
- Fehlerhafte Faxübertragung
- Manipulation von Adressbüchern und Verteilerlisten
- Unbefugtes Lesen von Faxsendungen
- Auswertung von Restinformationen in Faxgeräten und Faxservern
- Vortäuschen eines falschen Absenders bei Faxsendungen

Priorisierung	R2
Hinweis zum besseren Verständnis	In Handwerksbetrieben sind Stand-Alone-Faxgeräte/Faxserver immer noch fester Bestandteil der Standardausstattung der IT im Büroumfeld. Vertrauenswürdige Informationen und Inhalte können per Fax versendet werden, dadurch können Faxgeräte auch als Angriffsweg genutzt werden. Daher sollte für einen sicheren Einsatz von Faxgeräten, dem Schutzbedarf entsprechend angemessene Maßnahmen zur Sicherheit geplant und umgesetzt werden.
Anforderungen	NET.4.3.A1

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Geeignete Aufstellung eines Faxgerätes
Zu NET.4.3.A1:
Ein Faxgerät muss so aufgestellt werden, dass eingegangene Faxsendungen nicht von Unberechtigten eingesehen oder entnommen werden können. Daher sollte es in einem Bereich aufgestellt werden, der nicht frei öffentlich zugänglich ist.

Informationen für alle Mitarbeiter über die Faxnutzung
Zu NET.4.3.A2:
Alle Beschäftigten sind auf die Besonderheiten der Informationsübermittlung per Fax hinzuweisen. Eine verständliche Bedienungsanleitung muss am Faxgerät zur Verfügung stehen und eine Kurzeinweisung erfolgen.

Sicherer Betrieb eines Faxservers
Zu NET.4.3.A3:
Nach der Beschaffung einer Faxlösung ist diese umfangreich zu testen. Für die Verwendung (eingehende/ausgehende Faxe) sind Berechtigungen zu vergeben und die Speicherdauer im Gerät zu definieren. Die sichere Anordnung des Faxservers ist abhängig vom LAN und der Firewall.

INF.1
Allgemeines Gebäude.

Ein Gebäude ist mehr als nur ein Bauwerk mit Wänden, Fenstern, Türen etc. Es umfasst auch Infrastruktur- und Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung und Kühlung. Das sind alles wichtige Aspekte, die es zu berücksichtigen gilt, um die Informationssicherheit im Unternehmen von allen Seiten zu gewährleisten. Das Ideal: Es wird eine optimale Umgebung für die im Gebäude tätigen Menschen sichergestellt. Unberechtigte erhalten dort keinen Zutritt, wo sie die Sicherheit beeinträchtigen könnten, und die im Gebäude stationierte Technik wird sicher und effizient betrieben.

Minimieren Sie diese Risiken:

- Feuer
- Blitz
- Wasser
- Elementarschäden und Naturkatastrophen
- Umfeld-Gefährdungen
- Unbefugter Zutritt
- Verstoß gegen Gesetze oder Regelungen
- Unzureichende Brandschottungen
- Ausfall der Stromversorgung

Priorisierung	R2
Hinweis zum besseren Verständnis	Handwerksbetriebe können Mieter oder Eigentümer von Gebäuden und Werkstätten sein. Die Umsetzung der Maßnahmen muss daher ggf. mit dem Vermieter abgesprochen werden. Es gibt Handwerksbetriebe mit und ohne Kundenkontakt/ Ladengeschäft an der Betriebsstätte. Besonders Ladengeschäfte sollten die Punkte A6 und A7 priorisieren.
Anforderungen	INF.1.A1 – A8

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Planung der Gebäudeabsicherung
Zu INF.1.A1:
Sicherheitsanforderungen verschiedener Bereiche wie Werkstatt, Lager und Verkauf müssen miteinander abgestimmt werden. Bewährte Vorgehensweise ist eine Zonierung (s. INF.1.M23)

Angepasste Aufteilung der Stromkreise
Zu INF.1.A2:
Hierbei ist vor allem auf gleichmäßige Auslastung der drei Außenleiter zu achten sowie auf regelmäßige Anpassung an IST-Situation.

Einhaltung von Brandschutzvorschriften
Zu INF.1.A3:
Für IT-Räume sollten besondere Schutzmaßnahmen (z. B. Brandschutztür) getroffen werden. Eine verantwortliche Person für den Brandschutz sollte benannt werden. Fluchtwege und Löschwasserzugänge sollen gut ausgeschildert sein.

Branderkennung in Gebäuden
Zu INF.1.A4:
Mindestanforderung sind hier Rauchmelder in allen Räumen. Bei Entlüftungsanlagen sollten auch die Luftkanäle überwacht werden. Fluchtwege müssen frei passierbar sein (s. Technische Richtlinie für Arbeitsstätten ASR).

Geschlossene Fenster und Türen
Zu INF.1.A6:
In nicht besetzten Räumen sollen Türen und Fenster geschlossen bleiben. Brandschutztüren sollen immer geschlossen sein (s. INF.1.M3). Ein Kontrollgang bei Feierabend hilft eventuelle Sicherheitslücken zu schließen (s. INF.1.M22).

Zutrittsregelung und -kontrolle
Zu INF.1.A7:
Schutzbedürftige Räume bzw. Gebäudeteile müssen ebenso definiert werden (s. siehe INF.1.M23) wie die Personen, die dort Zutritt erhalten sollen (s. siehe ORP.4). Hierbei gilt: so wenig Personen wie möglich sollten eine Zugangsmöglichkeit erhalten. Wichtig ist eine Dokumentation der Schlüsselverwaltung (s. siehe INF.1.M12). Die Zutrittsregelungen müssen regelmäßig überprüft und angepasst werden, um der aktuellen Betriebssituation gerecht zu werden. (Weitere Hinweise in Baustein ORP.4)

Rauchverbot
Zu INF.1.A8:
Rauchen kann empfindliche IT-Geräte schädigen und ist eine Gefahrenquelle für Brände. Hier sollte darauf geachtet werden, dass auch für Raucherbereiche die Maßnahmen aus INF.1.M7 umgesetzt werden.

INF.2 Rechenzentrum und Serverraum.

An diesem Ort läuft vieles zusammen: Im Serverraum befindet sich die Hardware, die der Bereitstellung von Diensten und Daten im Betrieb dient. Demgemäß ist der Zutritt zu regeln und die Umgebung für die einzelnen Komponenten so zu gestalten, dass die Technik optimal und sicher laufen kann. Hinweis Serverraum: Soll ein Serverraum abgesichert werden, können die Anforderungen dieses Bausteins entsprechend reduziert werden. Es sind mindestens die Basisanforderungen umzusetzen.

Minimieren Sie diese Risiken:

- Fehlerhafte Planung
- Unberechtigter Zutritt
- Unzureichende Überwachung
- Unzureichende Klimatisierung im Rechenzentrum
- Feuer
- Wasser
- Fehlender oder unzureichender Einbruchsschutz
- Ausfall der Stromversorgung
- Verschmutzung
- Unzureichende Trassendimensionierung

Priorisierung	R2
Hinweis zum besseren Verständnis	–
Anforderungen	INF.2.A1 – A11

Online-Material.

Baustein

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

INF

INF.3
Elektronische Verkabelung.

„Nicht stören!“ - Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb.

Minimieren Sie diese Risiken:

- Kabelbrand
- Unzureichende Dimensionierung der elektrotechnischen Verkabelung
- Unzureichende Dokumentation der Verkabelung
- Unzureichende geschützte Verteiler
- Leitungsbeschädigungen
- Spannungsschwankungen und Über- bzw. Unterspannung
- Verwendung unzureichender Steckdosenleisten

Priorisierung	R2
Hinweis zum besseren Verständnis	Handwerksbetriebe können Mieter oder Eigentümer von Gebäuden und Werkstätten sein. Die Umsetzung der Maßnahmen muss daher ggf. mit dem Vermieter abgesprochen werden.
Anforderungen	INF.3.A1 – A3

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Auswahl geeigneter Kabeltypen
Zu INF.3.A1:
Kabel müssen die Sicherheitsanforderungen für die übertragungstechnischen Notwendigkeiten und die Umgebungsbedingungen erfüllen.

Planung der Kabelführung
Zu INF.3.A2:
Die Kabelverlegung sollte Gefahrenquellen grundsätzlich umgehen. Besondere Herausforderungen stellen hier Tiefgaragen, gemeinsam mit Dritten genutzte Räumlichkeiten, Räume mit besonders hoher Brandgefahr (u. a. Produktionsräume) mit hohen induktiven Lasten dar. Eine regelmäßige Aktualisierung an den IST-Stand ist notwendig. Wenn hohe Verfügbarkeit des IT-Systems notwendig ist, ist die Versorgung über zwei unabhängige Netze wichtig. IT-Verkabelung ist generell getrennt zu verlegen.

Fachgerechte Installation
Zu INF.3.A3:
Für die fachgerechte Ausführung ist der Auftraggeber (i. d. R. der Chef/ Vermieter) in der Prüfpflicht.

INF.4
IT-Verkabelung.

Bloß kein Kabelsalat! Die IT-Verkabelung umfasst alle Kommunikationskabel sowie passiven Komponenten und ist somit die physikalische Grundlage der internen Kommunikationsnetze im Betrieb. Ziel ist es, sie so zu schützen, dass die Kommunikation über diese Verbindungen weder mitgehört noch manipuliert noch gestört werden kann.

Minimieren Sie diese Risiken:

- Kabelbrand
- Unzureichende Netzdimensionierung
- Unzureichende Dokumentation der Verkabelung
- Unzulässige Kabelverbindungen
- Leitungsbeschädigungen
- Leitungsbeeinträchtigung
- Abhören und Manipulation von Leitungen

Priorisierung	R2
Hinweis zum besseren Verständnis	Handwerksbetriebe können Mieter oder Eigentümer von Gebäuden und Werkstätten sein. Die Umsetzung der Maßnahmen muss daher ggf. mit dem Vermieter abgesprochen werden.
Anforderungen	INF.4.A1 – A3

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Auswahl geeigneter Kabeltypen
Zu INF.4.A1:
Prinzipiell gilt es hier zu entscheiden, wo Kupfer- oder Lichtwellenkabel zum Einsatz kommen sollen und wie sicher deren Abschirmung gestaltet werden muss.

Fachgerechte Installation
Zu INF.4.A3:
Es sind die Normen EN 50173-1 bis EN 50173-3 zu beachten.

Weitere Hinweise zu den Anforderungen ergeben sich auch aus dem Baustein INF.3.

INF.7
Büroarbeitsplatz.

Informationen vor neugierigen Blicken Unbefugter schützen – das gilt insbesondere in Büroräumen, in denen Besucherinnen und Besucher ein und aus gehen. Schon scheinbar selbstverständliche Maßnahmen zeigen eine große Wirkung.

Minimieren Sie diese Risiken:

- Unbefugter Zutritt
- Beeinträchtigung durch ungünstige Arbeitsbedingungen
- Reinigungs- und Fremdpersonal oder Besucherinnen bzw. Besucher
- Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software im Büroraum
- Diebstahl
- Fliegende Verkabelung
- Vandalismus

Priorisierung	R2
Hinweis zum besseren Verständnis	Handwerksbetriebe können Mieter oder Eigentümer von Gebäuden und Werkstätten sein. Die Umsetzung der Maßnahmen muss daher ggf. mit dem Vermieter abgesprochen werden.
Anforderungen	INF.7.A1 – A11

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

INF

INF.8
Häuslicher Arbeitsplatz.

Arbeiten im Home-Office hat viele Vorteile, birgt aber auch Risiken bei der Verarbeitung von betriebseigenen Informationen. Denn an einem häuslichen Arbeitsplatz kann nicht das gleiche Sicherheitsniveau vorausgesetzt werden wie in den Büroräumen des Betriebs. So ist beispielsweise oft der Arbeitsplatz auch für Dritte oder Familienangehörige zugänglich. Das erfordert also einen besonders intensiven Blick auf geeignete Schutzmaßnahmen.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Regelungen für den häuslichen Arbeitsplatz
- Unbefugter Zutritt zu schutzbedürftigen Räumen des häuslichen Arbeitsplatzes
- Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen am häuslichen Arbeitsplatz
- Ungesicherter Akten- und Datenträgertransport
- Ungeeignete Entsorgung der Datenträger und Dokumente
- Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software am häuslichen Arbeitsplatz
- Gefährdung durch Reinigungs- oder Fremdpersonal
- Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

Priorisierung	R2
Hinweis zum besseren Verständnis	Dieser Baustein ist umzusetzen, wenn Mitarbeiter im Home-Office arbeiten dürfen. Mitarbeiter können Mieter oder Eigentümer von Gebäuden und Räumen sein. Die Umsetzung der Maßnahmen muss daher ggf. mit dem Vermieter abgesprochen werden.
Anforderungen	INF.8.A1 – A3

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz
Zu INF.8.A1:
Verfügbarkeit, Vertraulichkeit und Integrität von Daten muss gewährleistet bleiben. Passwortschutz und Zugangsbeschränkungen beachten!

Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz
Zu INF.8.A2:
Regelungen für den Austausch von Datenträgern und Unterlagen müssen festgelegt und an die Mitarbeiter kommuniziert werden.

Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz
Zu INF.8.A3:
Festlegung und Kommunikation von Maßnahmen an die Mitarbeiter. Insbesondere Türen und Fenster sollten während längerer Abwesenheit geschlossen sein.

Weitere Hinweise s. Baustein INF.1.M6

140

INF.9
Mobiler Arbeitsplatz.

Arbeiten von nahezu überall: Viele Beschäftigte nutzen die Möglichkeit mobil zu arbeiten – beim Kunden, auf Geschäftsreisen oder von zu Hause aus. Wechselnde Arbeitsplätze bedeuten unterschiedliche Umgebungen, z. B. im Hotelzimmer, in Zügen oder in den Geschäftsräumen eines Kunden. Das mobile Arbeiten erhöht damit die Anforderungen an die Informationssicherheit, da in mobilen Arbeitsplatz-Umgebungen keine sichere IT-Infrastruktur, wie sie in einer Büroumgebung anzutreffen ist, vorausgesetzt werden kann. Die Herausforderung: Die dabei verarbeiteten Informationen müssen angemessen geschützt werden.

Minimieren Sie diese Risiken:

- Fehlende oder unzureichende Regelungen für mobile Arbeitsplätze
- Beeinträchtigung durch wechselnde Einsatzumgebung
- Manipulation oder Zerstörung von IT-Systemen, Zubehör, Informationen und Software am mobilen Arbeitsplatz
- Verzögerungen durch temporär eingeschränkte Erreichbarkeit
- Ungesicherter Akten- und Datenträgertransport
- Ungeeignete Entsorgung der Datenträger und Dokumente
- Vertraulichkeitsverlust schützenswerter Informationen
- Diebstahl oder Verlust von Datenträgern oder Dokumenten
- Fehlendes Sicherheitsbewusstsein und Sorglosigkeit im Umgang mit Informationen

Priorisierung	R2
Hinweis zum besseren Verständnis	Dieser Baustein ist umzusetzen, wenn Beschäftigte von unterwegs aus arbeiten dürfen.
Anforderungen	INF.9.A1 – A4

Online-Material.

Baustein

Umsetzungshinweise

Arbeitshilfen

Empfehlungen für einzelne Anforderungen.

Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
Zu INF.9.A1:
Entscheidung zu mobilem Arbeiten anhand folgender Kriterien:
Bestehendes Verbot, Netzanschluss vorhanden, Bearbeitung vertraulicher Informationen, Einsichtnahme Dritter

Weitere Hinweise
s. Baustein INF.9.M2

Regelungen für mobile Arbeitsplätze
Zu INF.9.A2:
Festlegungen, welche Daten außerhalb des Unternehmens genutzt werden dürfen, müssen getroffen werden. Verschlüsselungen müssen eingerichtet und Zugriffe von außen entsprechend geschützt werden. Eine stichprobenartige Überprüfung der Einhaltung der Regeln und Sensibilisierung der Beschäftigten sollte regelmäßig erfolgen.

Hinweise zur Entsorgung mobiler Datenträger
s. INF.9.M6

Zutritts- und Zugriffsschutz
Zu INF.9.A3:

s. Hinweise aus Baustein INF.1.M6 und INF.8.M1 – INF.8.M3

Arbeiten mit fremden IT-Systemen
Zu INF.9.A4:
Da fremde Systeme beispielsweise beim Kunden genutzt werden, müssen zusätzliche Sicherheitsmaßnahmen getroffen werden.

Wie ist das fremde IT-System abgesichert?

Mögliche Maßnahmen: Eigene Regelungen einhalten, Zwischenspeicher nach beendeter Arbeit löschen, keine Auto-Vervollständigung für Zugangsdaten nutzen

INF

AdobeStock / © Wavebreak Media

Allianz für Cyber-Sicherheit.

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Aktuell gehören dem Netzwerk ca. 3.500 Unternehmen und Institutionen an – und jeden Tag kommen weitere Teilnehmer dazu. Werden Sie Teil eines starken Netzwerks!

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

- der Expertise des BSI und der Kooperations-Partner der Allianz für Cyber-Sicherheit aus Wirtschaft und Forschung
- dem vertrauensvollen Erfahrungsaustausch mit anderen Unternehmen
- den exklusiven Angeboten zum Ausbau der Sicherheitskompetenz in Ihrem Unternehmen

Die Teilnahme an der Allianz für Cyber-Sicherheit ist kostenfrei.
Registrierung unter: **www.allianz-fuer-cybersicherheit.de** – Menüpunkt: **Teilnehmer werden**

Das Kompetenzzentrum Digitales Handwerk.

Neue Potenziale erschließen.

Mit mehr als einer Million Betrieben ist das Handwerk zentraler Teil der deutschen Wirtschaft. Die ausgeprägte Kundenorientierung hat sich in der Vergangenheit als besonderes Qualitätsmerkmal erwiesen. Die Digitalisierung bietet viele Möglichkeiten, diesen Vorteil weiter auszubauen. Das Kompetenzzentrum Digitales Handwerk informiert Unternehmerinnen, Unternehmer und Führungskräfte aus dem Handwerk über die konkreten Einsatzmöglichkeiten digitaler Technologien und gibt nützliche Hilfestellung zur praktischen Umsetzung in den einzelnen Handwerksbetrieben. Nehmen Sie Kontakt mit uns auf!
Alle Angebote des Kompetenzzentrums Digitales Handwerk sind anbieterneutral und kostenfrei!

Konkrete Angebote nutzen.

Das Kompetenzzentrum bietet für jeden Handwerksbetrieb praktische Informations-, Qualifikations- und Unterstützungsangebote:

- Broschüren, Checklisten, Online-Ratgeber
- Demonstration digitaler Anwendungen
- Workshops und Fachveranstaltungen
- Webinare und Präsenzschulungen
- Entwicklung von praxisnahen Implementierungsstrategien
- Betriebsübergreifender Erfahrungsaustausch
- Begleitung von Betrieben bei der konkreten Umsetzung von digitalen Projekten

Weitere Informationen dazu finden Sie unter:
www.handwerkdigital.de

EINE FÖRDERINITIATIVE DES BMWI.

Das Kompetenzzentrum Digitales Handwerk ist Teil der Förderinitiative »Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse«, die im Rahmen des Förderschwerpunkts »Mittelstand-Digital – Strategien zur digitalen Transformation der Unternehmensprozesse« vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird.

Was ist Mittelstand-Digital?
Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.
Weitere Informationen finden Sie unter www.mittelstand-digital.de

KOMPETENZZENTRUM
DIGITALES HANDWERK

IMPRESSUM

Herausgeber
Kompetenzzentrum Digitales Handwerk
Zentralverband des Deutschen Handwerks (ZDH)
Abteilung Wirtschafts-, Energie- und Umweltpolitik
Mohrenstraße 20/21 · 10117 Berlin · www.zdh.de

Redaktion
Stephan Blank · ZDH
Frauke Greven · BSI

Gestaltung
Potsdam für Freunde

Druck Trend Point Marketing GmbH

Stand März 2019

Autorinnen und Autoren der Bausteine
Gunter Maetze · Henrik Klohs
Dr. Markus Kühn · Sven-Erik Laars
Jürgen Schüler · Andreas Spiller
Thomas Becker · Udo Kaethner
Torsten Gerlach · Dieter Opel
Werner Schmit · Anett Fritzsche

DAS HANDWERK
DIE WIRTSCHAFTSMACHT. VON NEBENAN.

www.handwerkdigital.de
facebook.com/handwerkdigital
twitter.com/HaWe_Digital

Allianz für Cyber-Sicherheit