IT-Sicherheit im Handwerk

Modularisierung IT-GRUNDSCHUTZ-PROFIL

FÜR HANDWERKSBETRIEBE – Fundament

Modularisierung
IT-Grundschutz-Profil Für Handwerksbetriebe
- Fundament
1. Auflage 2021

Herausgeber: Kompetenzzentrum IT-Sicherheit
und Qualifizierte Digitale Signatur (KOMZET)
Math. & Phys. Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz

Heinz-Piest-Institut für Handwerkstechnik
an der Leibnitz-Universität Hannover
Dipl.-Ing. Manfred Fülbier
Wilhelm-Busch-Straße 18 • 30167 Hannover

Layout und Titelgestaltung: Jürgen Schüler • Mainz

ISBN **978-3-944916-xx-x**

Verlag Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz
www.it-sicherheitsbotschafter.de

Autorenteam Templates

Hendrik Böker — **Handwerkskammer Hildesheim**

Schwerpunkte:
SYS.3.1 Laptops
SYS.3.2.1 Allgemeine Smartphones und Tablets

Manfred Fülbier — **Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover**

Schwerpunkte:
APP.5.2 Microsoft Exchange und Outlook
SYS.2.1. Allgemeiner Client
SYS.2.2.3 Clients unter Windows 10
SYS.4.5 Wechseldatenträger

Henrik Klohs — **Handwerkskammer Frankfurt (Oder) - Region Ostbrandenburg**

Schwerpunkte:
CON.2 Datenschutz
APP.1.2 Web-Browser
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
NET.4.1 WLAN-Betrieb
NET.4.2 VoIP
NET.4.3 Fax

Sven Erik Laars — **Handwerkskammer Erfurt**

Schwerpunkte:
APP.1.1 Office-Produkte
INF.1 Allgemeines Gebäude
INF.3 Elektrotechnische Verkabelung
INF.4 IT-Verkabelung

Dieter Opel — **Handwerkskammer für Oberfranken**

Schwerpunkte:
DER.2.1 Behandlung von Sicherheitsvorfällen
IND.2.4 Maschine
NET.1.1 Netzarchitektur und -design

Michael Pfister — **Handwerkskammer für Unterfranken**

Schwerpunkte:
APP.1.4 Mobile Anwendungen (Apps)
NET.2.1 WLAN-Betrieb
NET.2.2 WLAN-Nutzung
NET.3.1 Router und Switches
NET.3.2 Firewall
NET.3.3 VPN

Hacer Ritzler-Engels — **Kreishandwerkerschaft Paderborn-Lippe**

Schwerpunkt:
DER.1 Detektion von sicherheitsrelevanten Ereignissen

Jürgen Schüler — **Kompetenzzentrum IT-Sicherheit der Handwerkskammer Rheinhessen**

Kapitel 1-3, 6-9
Schwerpunkte:
ISMS.1 Sicherheitsmanagement
ORP.1 Organisation
ORP.2 Personal
ORP.3 Sensibilisierung und Schulung
ORP.4 Identitäts- und Berechtigungsmanagement
CON.3 Datensicherungskonzept
OPS.1.1.3 Patch- und Änderungsmanagement
OPS.1.1.4 Schutz vor Schadprogrammen
DER.4 Notfallmanagement
SYS.3.3 Mobiltelefon

Norbert Speier — **Handwerkskammer Münster in der Emscher-Lippe-Region**

Schwerpunkte:
INF.7 Büroarbeitsplatz
INF.8 Häuslicher Arbeitsplatz
INF.9 Mobiler Arbeitsplatz

Vorwort

Als Ergebnis einer vom HPI und dem BSI Anfang 2018 initiierten Workshop-Reihe wurde im März 2019 ein IT-Grundschutz-Profil für Handwerksbetriebe vom ZDH veröffentlicht[1].

Die Basis dieses IT-Grundschutz-Profils bilden ausgewählte Bausteine und Anforderungen aus dem IT-Grundschutz-Kompendium des BSI (Edition 2018), die von den im Workshop beteiligten Experten/innen aus Handwerksorganisationen als handwerksrelevant bewertet wurden. Durch die Umsetzung dieser Anforderungen soll das Informations-Sicherheitsniveau eines Betriebes signifikant erhöht werden.

Die Handwerkorganisationen HPI[2], KOMZET IT-Sicherheit[3] und ZDH-ZERT[4], einigten sich darauf, dass die Prüfung und Nachweisführung des IT-Grundschutzes im Handwerksbetrieb in verschiedenen Anforderungsstufen erfolgen kann (Fundament, Stufe 1: Einsteiger, Stufe 2: Fortgeschrittene und Stufe 3: Profi).

Das BSI begrüßt den zielgruppenorientierten Weg der stufenweisen Einführung des IT-Grundschutzes in Handwerksbetrieben mit dem Ziel, die Basis-Absicherung nach IT-Grundschutz zu erreichen.

Durch die aufeinander aufbauenden Stufen mit Prüfung und Nachweisführung erhalten die Handwerksbetriebe eine praktikable Möglichkeit, den IT-Grundschutz Schritt für Schritt umzusetzen und in der letzten Stufe die Basis-Absicherung nach IT-Grundschutz zu erreichen.

Zur Umsetzung dieses Stufenmodells haben die Vertreter der Handwerksorganisation den Anforderungskatalog (Bausteine und Anforderungen) Fundament auf Basis des IT-Grundschutz-Kompendiums (Edition 2020) definiert und ein Programm zur Prüfung und Nachweisführung des IT-Grundschutz-Profils für Handwerksbetriebe entworfen. Dieses Programm beinhaltet den Ablauf des Prozesses von der Anfrage eines Betriebes für eine Konformitätsbescheinigung nach dem IT-Grundschutz-Profil für Handwerksbetriebe bis hin zur Erstellung und Aufrechterhaltung des Nachweises. Die notwendigen Dokumente zur Beantragung der Konformitätsbescheinigung sind Gegenstand dieser Broschüre.

Basierend auf der Konformitätsbescheinigung kann nach Durchlaufen aller vier Stufen eine Testierung der Basisabsicherung nach IT-Grundschutz und darauf aufbauend eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz erlangt werden.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Veröffentlichung die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

---

[1] *https://www.it-sicherheit-handwerk.de/fileadmin/downloads/IT-Konzepte/Routenplaner_cyber-sicherheit_klickbar.pdf*
[2] *Heinz-Piest-Institut für Handwerkstechnik, Hannover*
[3] *Kompetenzzentrum IT-Sicherheit der Handwerkskammer Rheinhessen, Mainz*
[4] *ZDH-ZERT GmbH, Bonn*

Inhaltsverzeichnis

1 Einleitung

Hatten Sie schon einmal Probleme mit Computer-Viren?

Sind auf Ihren Rechnern vertrauliche oder personenbezogene Kundendaten gespeichert?

Sind Ihnen schon einmal Daten unwiederbringlich verloren gegangen? Haben Sie oder Ihre Mitarbeiter im Büro einen Internetzugang?

Sofern Sie eine der Fragen mit „Ja“ beantwortet haben, sollten Sie sich mit dem Thema Informationssicherheit beschäftigen. In der heutigen Informationsgesellschaft unterstützen Computer nahezu alle Arbeitsbereiche. In den Büros von Handwerksbetrieben werden Computer und weitere Informationstechnologie (abgekürzt mit IT) eingesetzt. Hierbei werden oft sehr sensible Unternehmensdaten verarbeitet, die geschützt werden müssen.

Zu den herausfordernden Aufgaben für IT-Sicherheitsverantwortliche gehört es, den Überblick über die abzusichernden Geschäftsprozesse und die zugehörige IT zu behalten und angemessene Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Mit dem IT-Grundschutz-Profil für Handwerksbetriebe bietet sich hierfür eine einfache Methode an. In diesem ist beschrieben, wie ein IT-Sicherheitsmanagement im Handwerksbetrieb aufgebaut und betrieben werden kann.

Das IT-Grundschutz-Profil für Handwerksbetriebe enthält Standards zu Gefährdungen und Sicherheitsmaßnahmen für typische Geschäftsprozesse und IT-Systeme, die nach Bedarf im eigenen Handwerksbetrieb eingesetzt werden können. Der Grundgedanke des IT-Grundschutz-Profils ist dabei, einen angemessenen Schutz für alle Informationen eines Handwerksbetriebes zu erreichen.

Diese Unterlage erklärt nicht nur, was gemacht werden sollte, sondern gibt konkrete Hinweise in Form von Templates, wie eine Umsetzung aussehen kann. Ein Vorgehen nach dieser Unterlage bietet die Möglichkeit eine Konformitätsbescheinigung zu erhalten und kommt Anforderungen der ISO-Standards nach.

Das IT-Grundschutz-Profil – Fundament vermittelt einen ersten Einstieg in die wichtigsten Basis-Sicherheits-Maßnahmen. Eine Zusammenstellung von gesetzlichen Regelungen mit Bezug zur IT-Sicherheit, ein umfangreiches Glossar mit den wichtigsten Fachbegriffen sowie Darstellung von typischen Fehlern motivieren, das Thema IT-Sicherheit systematisch anzugehen.

In diesem Dokument wird Ihnen ein Beispiel gegeben, wie Sie in Ihrem Handwerksbetrieb systematisch eine IT-Sicherheitskonzeption erstellen können. Sie werden mit konkreten Sicherheitsaspekten vertraut gemacht, die beim Umgang mit geschäftsrelevanten Informationen und beim Einsatz von Informationstechnologie in einem kleinen Handwerksbetrieb zu beachten sind. Ausgehend von einem beispielhaft dargestellten Handwerksbetrieb mit wenigen Mitarbeitern wird gezeigt, wie Sie basierend auf Referenzdokumenten eine Konformitätsbescheinigung auf Grundlage von IT-Grundschutz erhalten können.

2 Konformitätsbewertungsverfahren nach „Modularisierung IT-Grundschutz-Profil für Handwerksbetriebe - Fundament“

Für das Konformitätsbewertungsverfahren auf der Basis dieser Unterlage ist durch den antragstellenden Handwerksbetrieb eine Vielzahl von Dokumenten für Prüfzwecke bereitzustellen. Diese sind in elektronischer Form dem Auditor zu übergeben. Zur Vereinfachung wurden für Handwerksbetriebe Templates (Vgl. Abschnitt 4) erstellt. Der Antragsteller ergänzt die fehlenden Angaben in den vorgenannten Templates und leitet sie an den Auditor weiter. Die Dokumente sind im Rahmen des Konformitätsbewertungsverfahrens und der Aufrechterhaltung durch den Antragsteller fortzuschreiben.

2.1 Referenzdokumente[5]

Die folgenden Dokumente bilden die Grundlage für eine Konformitätsbescheinigung und sind dem Auditor vom Antragsteller als Arbeitsgrundlage zur Verfügung zu stellen:

- IT-Sicherheitsleitlinie Handwerk (A.0)
- IT-Strukturanalyse (A.1)
- Modellierung des Informationsverbunds (A.3)
- Ergebnis des IT-Grundschutz-Checks (A.4)

Die Dokumente:

- Schutzbedarfsfeststellung (A.2)
- Risikoanalyse (A.5)
- Realisierungsplan (A.6)

sind weder aus Sicht von Heinz-Piest-Institut (HPI) und KOMZET (Kompetenzzentrum IT-Sicherheit) noch aus Sicht des BSI zur Erfüllung der Basisanforderungen notwendig.

Der Auditor wird darüber hinaus während des Vor-Ort-Audits weitere Dokumente und Aufzeichnungen (vgl. auch Spalte Nachweis in den Checklisten) einsehen. Die Referenzdokumente sind Bestandteil des Auditberichtes. Sollten zusätzliche Dokumente erstellt worden sein, die zur Prüfung heranzuziehen sind, sind diese ebenfalls in der aktuellen Fassung dem Auditor vorzulegen und können ggf. Gegenstand des Auditberichtes werden. Soweit der Antragsteller und der Auditor der Ansicht sind, dass Maßnahmen zur Gewährleistung der Vertraulichkeit bei der Übergabe der Dokumentation erforderlich sind, sollten geeignete Schritte ergriffen werden. Der Auditor sollte durch vertragliche Vereinbarungen mit dem auditierten Handwerksbetrieb verpflichtet werden, im Rahmen des Audits gewonnene

[5] Hinweise zur Bereitstellung der Referenzdokumente im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Version 2.1 BSI

Informationen streng vertraulich zu behandeln sowie Beschäftigten und Dritten Informationen nur zu geben, soweit ihre Kenntnis unbedingt notwendig ist. Neben den Referenzdokumenten ist die Übersicht “Liste der Referenzdokumente“ einzureichen. In dieser Liste der Referenzdokumente müssen ferner relevante Änderungen (bei Überwachungsaudits und Re-Zertifizierungsverfahren) verzeichnet sein.

2.2 IT-Sicherheitsleitlinie Handwerk (A.0)

Die Leitlinie zur Informationssicherheit (vgl. Template 4.1.1) beschreibt allgemeinverständlich, was Informationssicherheit ist und welche Bedeutung sie für ihr Unternehmen hat. Das Dokument zeigt auf, wie Informationssicherheit im Unternehmen gelebt wird, indem das zu erreichende Mindest-Sicherheitsniveau beschrieben wird sowie die angestrebten Informationssicherheitsziele und die verfolgte Informationssicherheitsstrategie dargestellt werden.

Das Template in Abschnitt 4.1.1 soll Ihnen helfen, eine eigene Sicherheitsleitlinie für Ihren Handwerksbetrieb zu erstellen. Prüfen Sie die in [*kursiv*] enthaltenen Textstellen und passen Sie diese an Ihre Bedürfnisse an.

2.3 Strukturanalyse (A.1)

In der Strukturanalyse (vgl. Template 4.1.2) wird der zu untersuchende Informationsverbund dargestellt. Ausgehend von einem Netzplan werden die vorhandenen und geplanten IT-Systeme erfasst und die sie jeweils charakterisierenden Angaben zusammengestellt. Dazu zählen

- alle im Netz vorhandenen Computer (Clients und Server) , Gruppen von Computern und aktiven Netzkomponenten, Netzdrucker, aber auch
- nicht vernetzte Computer wie Internet PCs und Laptops,
- Telekommunikationskomponenten wie TK-Anlagen, Faxgeräte, Mobiltelefone und Anrufbeantworter.
- die Zuordnung der IT-Anwendungen zu den Servern, Clients, Räumen und Netz- bzw. Telekommunikationskomponenten sowie
- eine Liste der Dienstleister

Das Template in Abschnitt 4.1.2 soll Ihnen helfen, eine eigene Strukturanalyse für Ihren Handwerksbetrieb zu erstellen. Prüfen Sie die in <*kursiv*> enthaltenen Textstellen in den Tabellen und passen Sie diese an Ihre Bedürfnisse an.

2.4 Modellierung des Informationsverbunds (A.3)

Die Modellierung des Informationsverbundes legt fest, welche Bausteine des IT-Grundschutzkompendiums auf welche Zielobjekte im betrachteten Informationsverbund angewandt werden. Durch die Auswahl der Bausteine und den entsprechenden Anforderungen wird das konkrete Sicherheitsniveau des Handwerksbetriebes definiert.

Die Modellierung für die Stufe 1 entnehmen Sie der Tabelle in Abschnitt 4.1.3.

2.5 Ergebnis des IT-Grundschutz-Checks (A.4)

Ausgehend von der Modellierung in 2.4 und 4.1.3 wird im IT-Grundschutz-Check mit Hilfe einer Software[6] geprüft, inwiefern jede einzelne Anforderung umgesetzt wird. Für jede Anforderung wird konkret dargelegt, wie die aktuelle Umsetzung erfolgt.

[6] Empfohlen werden alternative IT-Grundschutz-Tools des BSI
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/AndereTools/anderetools_node.html;jsessionid=04A688B085BA56782A61519D57811C1D.2_cid502

Zur Illustration verschiedener Risiken im Umgang mit Informationssicherheit und zur Beschreibung möglicher Gegenmaßnahmen wird uns im vorliegenden Dokument beispielhaft Herr Fleißig begleiten.

Die Beispiele werden im nachfolgenden Text optisch durch einen grauen Hintergrund und eine Umrandung hervorgehoben.

Herr Fleißig führt einen kleinen Familienbetrieb mit 3 Angestellten. Zu den Angestellten zählen eine Sekretariatskraft (Ehefrau), die halbtags arbeitet und zwei Außendienstmitarbeiter (Geselle und Auszubildender), die den ganzen Tag vor Ort bei den Kunden des Familienbetriebs beschäftigt sind. Herr Fleißig selbst ist für die Akquisition der Kunden verantwortlich. Während der Ausführung der Arbeiten betreut er seine Kundschaft und kümmert sich um kleinere Details und kurzfristig von den Kunden geäußerte Sonderwünsche.

Die Kunden schätzen diesen Service und empfehlen den kleinen Betrieb gerne an Bekannte und Verwandte weiter. Ein guter Ruf ist für den Betrieb daher sehr wichtig und sichert langfristig die Kundschaft.

Herr Fleißig hat nach eigener Aussage keine Ahnung von Computern, obwohl er im Betrieb PCs und einen Laptop vielfältig einsetzt: das Führen der Kundenkartei, die Erstellung von Angeboten, das Schreiben der Rechnungen oder die elektronische Kontoführung über das Internet sind nur wenige Beispiele für den Einsatz von Computern in dem kleinen Betrieb.

Frau Fleißig hat sich in den Umgang mit PCs und Rechnernetzen etwas eingearbeitet und hierfür einen Kurs in der Handwerkskammer besucht. Sie hilft zeitweise im Betrieb. aus und übernimmt insbesondere die Wartung und Pflege der PCs.

Im vorliegenden Dokument sind Merksätze und Handlungsanweisungen enthalten. Diese sind durch einen rot umrandeten Kasten gekennzeichnet.

Referenzen auf andere Dokumente werden mit einem Kürzel in eckigen Klammern (z. B. [*GSK*]) angegeben. In Kapitel 8 findet man mit dieser Bezeichnung dann den ausführlichen Literaturhinweis.

3 Rahmenbedingungen für kleine Handwerksbetriebe

3.1 Erläuterung zum Schutzbedarf

Was sind Ihre wichtigsten Geschäftsprozesse? Wissen Sie, welche Daten innerhalb Ihres Handwerksbetriebes so bedeutend sind, dass ihr Verlust oder deren Offenbarung einen Verstoß gegen ein Gesetz, einen Vertrag oder eine Vorschrift bedeutet?

Wie wichtig sind Ihnen Ihre Kundendaten? Wie lange können Sie problemlos arbeiten, wenn Ihr Computer ausfällt, die Festplatte nicht mehr lesbar oder Ihr Internetzugang/ Telefonanschluss nicht nutzbar ist?

Wenn Sie sich mit IT-Grundschutz beschäftigen, müssen Sie diese wichtigen Fragen zunächst für sich beantworten.

Herr Fleißig hat in seiner Kundenkartei auf dem PC nicht nur alle Vorgänge von ausgeführten Aufträgen gespeichert, sondern auch vertrauliche Informationen, die ihm bei der Erstellung neuer Angebote nützlich sein können.

Herr Fleißig erhält eine unaufgeforderte Bewerbung als Worddokument per E-Mail. Diese öffnet eine Hintertür in den Computern und ermöglicht es dem Absender, über das Internet auf die Computer von Herrn Fleißig zuzugreifen. Da weder Herr Fleißig noch der IT-Dienstleister die Betriebssysteme und die vorhandenen Schutzprogramme der Computer (Virenscanner, Firewall, etc.) längere Zeit nicht aktualisiert hat, kann sich das Schadprogramm ausbreiten. Dem Angreifer wird es hierdurch ermöglicht, auf die Festplatten und somit auf die Daten von Herrn Fleißig zuzugreifen.

Unter den Daten findet der Angreifer auch die Vorbereitungsunterlagen für eine Ausschreibung. Er kann anhand der Daten die Kalkulation von Herrn Fleißig nachvollziehen und ein vergleichbares Angebot zu einem geringeren Preis anbieten. Ebenso kann er die Rechner von Herrn Fleißig verschlüsseln und Lösegeld für die Entschlüsselung fordern.

In diesem Beispiel wurde der Grundwert der „Vertraulichkeit“ verletzt, da der Angreifer auf interne Informationen von Herrn Fleißig zugreifen konnte.

Vertraulichkeit besagt, dass Informationen nur von berechtigten Personen **gelesen** werden dürfen. Zusätzlich zur Vertraulichkeit sind auch die Grundwerte „Integrität“ und „Verfügbarkeit“ von Bedeutung.

Unter **Integrität** von Daten versteht man die Tatsache, dass Daten nur von Befugten in beabsichtigter Weise verändert und z. B. von Unbefugten nicht modifiziert werden können. **Verfügbarkeit** bedeutet, dass Informationen und Systeme zur Verfügung stehen, wenn sie benötigt werden.

Bedenken Sie die Folgen, die sich ergeben, wenn Unberechtigte Zugriff auf Ihre Daten erhalten oder wenn Ihnen Systeme, die Sie im Tagesablauf nutzen möchten, nicht zur Verfügung stehen. Oder wenn Daten, die Sie bearbeiten müssen, verändert oder gelöscht wurden.

Jeder Inhaber eines Unternehmens sollte wissen, dass es für seinen Betrieb schwerwiegende Konsequenzen haben kann, wenn unberechtigte Personen Zugang zu vertraulichen Informationen erlangen. Mit der Methodik dieser Broschüre werden Sie in die Lage versetzt, die IT-Sicherheit in Ihrem Betrieb zu verbessern.

3.2 Verantwortlichkeit

In Handwerksbetrieben trägt der Inhaber/Geschäftsführer die Verantwortung bei Sicherheitsvorfällen. Er muss die folgenden Aufgaben selbst erledigen oder durch einen IT-Dienstleister erledigen lassen um seinen Betrieb abzusichern.

Der Chef muss

- eine Sicherheitsleitlinie erstellen (siehe hierzu Kapitel 2.2 und das Template für eine Sicherheitsleitlinie in Abschnitt 4.1.1),
- eine Strukturanalyse durchführen (siehe Kapitel 2.3 und das Template 4.1.2),
- relevante Sicherheitsmaßnahmen in seinem Betrieb umsetzen (Hierzu geben wir in den Templates im Abschnitt 4.2 Beispiele, die für einen kleinen Handwerksbetrieb relevant sind) und
- alle Vorgänge und Maßnahmen dokumentieren

In kleinen Handwerksbetrieben ist der Chef (Geschäftsführer oder Inhaber) für alle wichtigen Punkte selbst verantwortlich. Insbesondere beim Thema IT-Sicherheit hat der Chef eines kleinen Handwerksbetriebs wenige Möglichkeiten, Verantwortung an seine Mitarbeiter zu delegieren. Daher muss er sich mit dem Thema Sicherheit seiner Geschäftsprozesse beschäftigen.

3.3 Definition und Abgrenzung des IT-Verbundes

Zunächst muss der zu betrachtende IT-Verbund abgegrenzt werden. Als IT-Verbund wird die Gesamtheit der infrastrukturellen, organisatorischen, personellen und technischen Komponenten verstanden, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Es stellen sich die Fragen:

- Welche relevanten Geschäftsprozesse gibt es in Ihrem Betrieb?
- Welche IT-Systeme gibt es in Ihrem Unternehmen?

In diesem Abschnitt wird der IT-Verbund von kleinen Handwerksbetrieben aus Sicht des Geschäftsführers beschrieben. Ein Template für den IT-Verbund befindet sich in Kapitel 4.1.2 (Strukturanalyse).

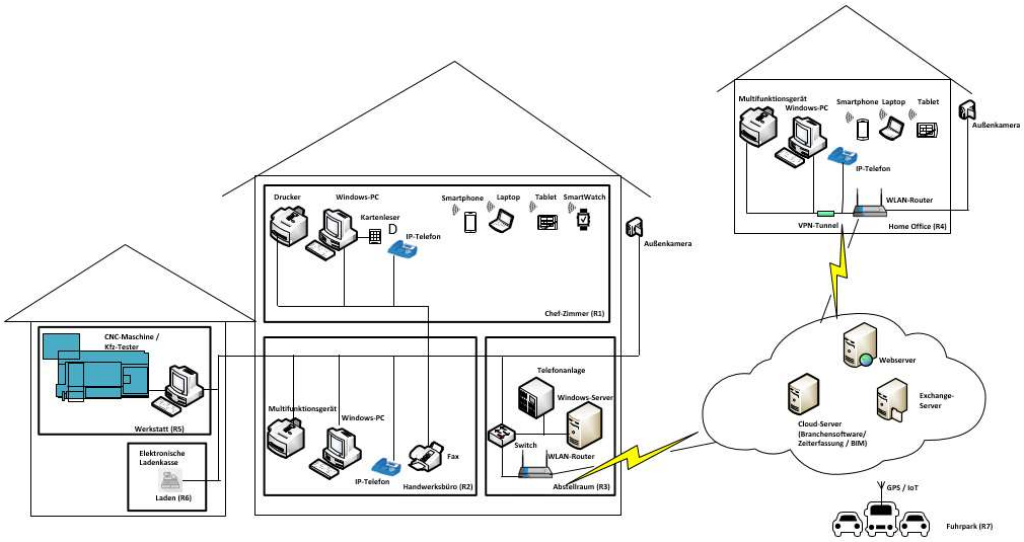

Abbildung 1: *Kleiner IT-Verbund eines Handwerksbetriebes*

Abbildung 1 zeigt Ihnen den IT-Verbund, der diesem Dokument zugrunde liegt. Die Büro-Umgebung des dargestellten Handwerksbetriebs besteht aus verschiedenen Räumlichkeiten (R1-R6). Befindet sich der Laptop in der Büro-Umgebung, so steht er im Chef-Zimmer (R1).

In welchen Räumen sind die Geräte aufgestellt?

- **Chef-Zimmer (R1):** Chef-PC, Drucker, Kartenleser, Telefon, Laptop, Tablet, Handy, SmartWatch
- **Sekretariat (R2):** Sekretariats-PC, Drucker, Telefon, Faxgerät, Anrufbeantworter.
- **Abstellraum (R3):** Telefonanlage, DSL-WLAN-Router mit Firewall, Switch, Server.
- **Werkstatt (R5):** CNC-Maschine, Maschinen-PC, KFZ-Tester.
- **Laden /R6):** Elektronische Ladenkasse.
- **Home Office:** Chef-PC, Drucker, Telefon, Laptop, Tablet, Handy, SmartWatch, Außenkamera.
- **Verbindungsräume** (z. B. Flure): Teile der Verkabelung, Außenkamera.

Das Handwerksbüro (R2) und der Laden (R6) sind öffentlich zugänglich. Die anderen Räume (R1, R3, R5) sind nur durch die Flurtüren des Betriebes erreichbar.

3.3.1 Welche IT-Systeme sind installiert?

Als nächstes wird betrachtet welche IT-Systeme (Hardware) im Unternehmen vorhanden bzw. installiert sind.

Der Arbeitsplatzrechner des Geschäftsführers (Chef-PC) und der Sekretariats-PC laufen unter Windows 10 mit ähnlicher Konfiguration und gleichen Anwendungen. Der Server läuft unter Windows Server 2012 und dient zur zentralen Datenspeicherung verschiedener Anwendungen. An der IP-Telefonanlage (TK-Anlage) sind alle Telefone,

das Faxgerät, der Anrufbeantworter sowie der DSL-Router angeschlossen. Der Laptop läuft unter Windows 10 und besitzt eine eingebaute SIM-Karte. Die Firewall des DSL-Routers besitzt ein spezielles Betriebssystem des Herstellers. Das Handy (iPhone) ist ein mobiles IT-System, welches der Geschäftsführer bei sich trägt.

3.3.2 Welche Computerprogramme werden verwendet?

Nach der Ist-Aufnahme der IT-Systeme wird betrachtet welche Softwarekomponenten installiert sind und welche Kommunikationsverbindungen genutzt werden.

Neben einer Branchensoftware, die Geschäftsprozesse des Betriebs unterstützt, wird Microsoft Office 365 eingesetzt.

Von jedem PC aus kann man auf alle Festplatten zugreifen und auf jedem Drucker ausdrucken.

Über welche (Kommunikations-)Leitungen werden Daten übertragen?

Die Kommunikationsleitungen (IT-Verbindungen) bestehen aus der internen Verkabelung und der Außenanbindung über einen Diensteanbieter (Provider) ins Internet und Telefonnetz.

Anwendung der Templates
Wie können Sie die im vorliegenden Dokument beschriebenen IT-Grundschutz-Maßnahmen für Ihren individuellen Betrieb nutzen?
Am Beispiel des in diesem Dokument beschriebenen Handwerksbetriebes wird eine vollständige IT-Sicherheitskonzeption erstellt. Das Beispiel muss nicht notwendigerweise in allen Punkten mit den Gegebenheiten Ihres Betriebes übereinstimmen. Vielmehr soll es Ihnen als Vorlage dienen, an der Sie ohne allzu großen Aufwand kleinere Änderungen vornehmen können.
Prüfen Sie, inwieweit der beschriebene IT-Verbund mit den Gegebenheiten in Ihrem Handwerksbetrieb übereinstimmt und nehmen Sie entsprechende Anpassungen vor.

3.4 Sicherheitsleitlinie und Sicherheitskonzeption

Wofür benötigen Sie die Sicherheitsleitlinie und das Sicherheitskonzept?

Eine Sicherheitsleitlinie definiert die zu erreichenden und gewünschten Sicherheitsziele für den Betrieb. Das Sicherheitskonzept beschreibt, wie diese Ziele erreicht werden sollen.

3.4.1 Sicherheitsleitlinie

Die Sicherheitsleitlinie definiert das angestrebte Sicherheitsniveau im Unternehmen. Sie enthält die angestrebten Sicherheitsziele sowie die verfolgte Sicherheitsstrategie und ist daher Anspruch und Aussage zugleich.

> Ein Template für eine Sicherheitsleitlinie eines kleinen Handwerksbetriebes finden Sie in Abschnitt 4.1.1

Bestimmen und dokumentieren Sie Ihre Sicherheitsleitlinie auf Basis des Templates in Abschnitt 4.1.1 unter Berücksichtigung der besonderen Anforderungen ihres Betriebs.

3.4.2 Sicherheitskonzeption

Eine IT-Sicherheitskonzeption gibt Antwort auf die Fragen: „Was genau muss ich schützen? Wogegen muss ich es schützen? Wie kann ich einen wirksamen Schutz erreichen?“ und gliedert sich in mehrere Teilaufgaben.

Nachdem Sie die Sicherheitsziele in der Sicherheitsleitlinie festgelegt haben, ist im Rahmen der Sicherheitskonzeption der Schutzbedarf der IT-Anwendungen und IT-Systeme festzustellen und dafür angemessene Sicherheitsmaßnahmen umzusetzen.

> Die Templates in Abschnitt 4.2 helfen Ihnen, die Vorgänge in Ihrem Betrieb zu dokumentieren und geeignete Sicherheitsmaßnahmen auszuwählen.

Legen Sie einen Ordner für die Sicherheitskonzeption an. Dokumentieren Sie, dass die Sicherheitsmaßnahmen umgesetzt sind. Ist der Ordner vollständig, haben Sie Ihr Ziel erreicht. Eine IT-Sicherheitskonzeption ist erstellt!

Nachdem Frau Fleißig die Übersicht über die IT-Systeme erstellt und die Betriebssysteme auf den neuesten Stand gebracht hat, passt sie die beispielhafte Sicherheitsleitlinie auf die Gegebenheiten ihres Unternehmens an. Sie bespricht die Leitlinie nochmals mit ihrem Mann. Herr Fleißig unterzeichnet sie und gibt sie allen Mitarbeitern zur Kenntnis und erläutert ihnen die Hintergründe. Herr Fleißig möchte, dass allen Mitarbeitern bewusst wird, dass die IT-Systeme einen kritischen Erfolgsfaktor für das Unternehmen darstellen.

3.5 Strukturanalyse

Der erste Schritt bei der Erstellung der Sicherheitskonzeption ist die Durchführung der Strukturanalyse, mit der die Fragen: „Welche geschäftsrelevanten Informationen und IT-Systeme gibt es in meinem Betrieb? Mit welchen IT-Systemen führen sie Ihre relevanten Geschäftsprozesse durch?“ beantwortet werden. Hierzu müssen Sie

zunächst für jedes IT-System folgende Informationen erfassen, um schnell alle relevanten Daten und Informationen vorliegen zu haben (z. B. im Schadensfall).

- Bezeichnung des IT-Systems
- Betriebssystem des IT-Systems
- Anwendungen/Programme auf dem IT-System
- Werden mit den Anwendungen personenbezogene Daten verarbeitet?
- In welchem Raum steht das System?

Ein Template für eine Strukturanalyse finden Sie im Abschnitt 4.1.2

3.5.1 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung gibt Antworten auf Fragen nach zu schützenden Informationen und danach, wo sich diese befinden und verarbeitet werden. In der Schutzbedarfsfeststellung wird somit versucht, die folgenden Fragen zu beantworten:

- Was ist zu schützen? Auf welchen Systemen werden sensible Daten verarbeitet?
- Welche Systeme sind für die Aufrechterhaltung Ihrer Geschäftsprozesse am wichtigsten?

Die Schutzbedarfsfeststellung dokumentiert nachvollziehbar das Sicherheitsverständnis Ihres Betriebs. Ziel der Schutzbedarfsfeststellung ist es, für jede erfasste IT-Anwendung einschließlich ihrer Daten zu entscheiden, welcher Schaden entstehen könnte, wenn die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit verletzt werden. Da eine Einschätzung des möglichen Schadens meist nicht exakt quantifizierbar ist, sollten Sie zwei Kategorien definieren, die nach einem „normalen“ oder einem „hohen“ Schutzbedarf unterscheiden.

In der Tabelle Abschnitt 4.1.3 haben wir bereits eine Schutzbedarfsfeststellung (Auswahl entsprechender Bausteine) für einen kleinen Betrieb vorgeschlagen und die Anforderungen entsprechend (Orange) gekennzeichnet. Sollten Komponenten mit „höherem“ Schutzbedarf vorhanden sei, kann es erforderlich sein, zusätzliche Maßnahmen zu ergreifen.

Herr Fleißig wird von einem potenziellen Kunden aufgefordert, schnell ein aus seiner Sicht umfangreiches Angebot abzugeben. Herr Fleißig hat dazu ein ausführliches Gespräch mit dem Kunden geführt und dabei mit seinem Laptop die wichtigsten Punkte notiert. Herr Fleißig ist sehr daran interessiert ein Angebot abzugeben, da der Umfang der durchzuführenden Arbeiten etwa 25.000 Euro betragen wird. Für das Angebot und die auszuführenden Arbeiten hat er schon während des Kundengesprächs eine Idee entwickelt, die auf einer vor einigen Jahren von seiner Firma durchgeführten Dienstleistung beruht. Auf dieser Grundlage sollte es ihm über das Wochenende möglich sein, ein fundiertes, aussagekräftiges und attraktives Angebot zu unterbreiten. Es ist ihm sehr wichtig, diesen größeren Auftrag zu erhalten.

Als Herr Fleißig am Abend im Büro sitzt, muss er feststellen, dass die Unterlagen aus den früheren Jahren nicht auf dem Server abgelegt sind. Es fällt ihm ein, dass die Festplatte vor einiger Zeit getauscht wurde. Er ruft seine Frau und sagt ihr, dass er jetzt sehr schnell diese Unterlagen benötigt, da ihm sonst ein größerer Auftrag verloren geht.

Die Schutzbedarfskategorien werden anhand von Schadenszenarien, die individuell auf die Anforderungen Ihres Handwerksbetriebes abgestimmt sind, festgelegt. Mögliche Schäden sind dabei nicht nur finanzieller Art. Betrachtet werden müssen beispielsweise auch Imageschäden sowie Verstöße gegen Gesetze, Vorschriften und Verträge.

In allen Szenarien müssen Sie entscheiden, wie wichtig Ihnen Ihre Daten sind, und darüber hinaus die individuellen Gegebenheiten Ihres Handwerksbetriebes berücksichtigen. Ein angenommener Schaden von 200.000 Euro ist z. B. gemessen am Umsatz für eine Bank eher gering, würde aber bei einem Handwerksbetrieb zum Konkurs führen.

Für Herrn Fleißig ist ein Auftrag, der für sein Unternehmen zu etwa 25.000 Euro Umsatz führt, sehr wichtig. Von daher stuft er die Verfügbarkeit seiner Daten, die er zur schnellen Erstellung des Angebots benötigt, als 'hoch' ein.

Um die Schutzbedarfskategorien für Ihren Handwerksbetrieb zu definieren, passen Sie einfach die Vorgaben der Tabellen aus Abschnitt 4.1.3 auf Ihren Betrieb an. Sind für Sie zusätzliche Schadensszenarien relevant, ergänzen Sie diese bitte.[7]

.

[7] Für Unternehmen mit höherem Schutzbedarf wird eine neue Broschüre erarbeitet

4 Templates

Wir kommen nun zum letzten Schritt bei der Erstellung einer IT-Sicherheitskonzeption, der zur Beantwortung der folgenden Frage führt:

Welche Sicherheitsmaßnahmen sind bereits umgesetzt und wo ist noch Handlungsbedarf?

Dieses Kapitel wird Ihnen dabei helfen, Defizite innerhalb Ihres Handwerksbetriebes zu erkennen, die zu einem Risiko für Ihre IT-Systeme und Daten führen können und konkrete Gegenmaßnahmen festzulegen. Hierzu werden die für den IT-Verbund identifizierten Bausteine des IT-Grundschutz-Kompendiums herangezogen. Die Maßnahmen und Gefährdungen der einzelnen Bausteine sind im IT-Grundschutz-Kompendium unter der entsprechenden Bausteinnummer beschrieben. Anhand von konkreten Beispielen einzelner Bausteine erfahren Sie, wie Sie das IT-Grundschutz-Kompendium anwenden können und wie die Anforderungen sinnvoll auf Ihren IT-Verbund angewendet werden können.

Auf den nachfolgenden Seiten sind Templates zusammengestellt, die Sie bei der Erstellung eines Sicherheitskonzepts unterstützen. Neben einer Beispiel Sicherheitsleitlinie finden Sie die vollständige Modellierung für den beispielhaften IT-Verbund im Anschluss. Sie sollten eine ähnliche Tabelle erstellen und Ihren IT-Verbund modellieren. Auch dieses Ergebnis halten Sie anschließend in Ihrem Ordner für das Sicherheitskonzept fest.

Im Kapitel 5 sowie bei jedem Template haben wir noch Checklisten für die Selbstüberprüfung beigefügt. Vergessen Sie nicht, die Checklisten regelmäßig neu auszufüllen, um Änderungen an Ihrem IT-Verbund und daraus erforderliche neue Maßnahmen zu erkennen.

4.1 Referenzdokumente

In den folgenden Abschnitten finden Sie Templates für die Referenzdokumente „IT-Sicherheitsleitlinie Handwerk“ „IT-Strukturanalyse“ und „Modulierung des Informationsverbundes“. In [eckigen Klammern] sind mögliche Lösungsansätze angegeben.

4.1.1 IT-Sicherheitsleitlinie Handwerk (A.0)

Template A.0 IT-Sicherheitsleitlinie - Handwerk

Autor:
Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 – 277
Telefax: (06131) 9992 – 8277
E-Mail: j.schueler@hwk.de
Webseite: www.it-sicherheitsbotschafter.de

Stand: Juni. 2020

1 Einleitung

Unser Unternehmen ist ein innovativer Dienstleister im Handwerk [*Geschäftszweck*]. Wir beschäftigen [*Mitarbeiter*]. [*Ort*] ist unser einziger Standort. *[Ergänzen könnte man noch Informationen über die Art der Kunden und die Bedeutung der Sicherheit für einzelne Kunden und Aufträge.]*

1.1 Die IT-Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit beschreibt allgemeinverständlich, was Informationssicherheit ist und welche Bedeutung sie für unser Unternehmen hat. Das Dokument zeigt auf, wie Informationssicherheit im Unternehmen gelebt wird, indem das zu erreichende Mindest-Sicherheitsniveau beschrieben wird sowie die angestrebten Informationssicherheitsziele und die verfolgte Informationssicherheitsstrategie dargestellt werden.

1.2 Geltungs-/Anwendungsbereich

Der Wettbewerb und Kunden verlangen neben der Produktion und Lieferung qualitativer Produkte auch den Nachweis der Qualität und Sicherheit interner Prozesse. Die vorliegende Informationssicherheitsleitlinie adressiert dieses Erfordernis im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb unseres Unternehmens. Sie gilt somit für das gesamte Unternehmen.

- Diese Leitlinie richtet sich an alle Mitglieder und Angehörige des Unternehmens. Hierzu zählen auch die Beschäftigten von beauftragten Dienstleistungsunternehmen und Geschäftspartnern.
- Jeder Beschäftigte ist verpflichtet, die IT-Sicherheitsleitlinie im Rahmen seiner Zuständigkeiten und Arbeiten einzuhalten und die Informationen und die Technik angemessen zu schützen.
- Unter den Vorgaben dieser IT-Sicherheitsleitlinie und dem IT-Grundschutz-Profil für Handwerksbetriebe werden Ziele, Anforderungen, organisatorische und technische Sicherheitsmaßnahmen in dem IT-Sicherheitskonzept detailliert geplant, dokumentiert und dann umgesetzt.

2 Definitionen und Erläuterungen

Bei der Gestaltung von Informationssicherheit orientiert sich unser Unternehmen am IT-Grundschutz-Profil für Handwerksbetriebe und den Empfehlungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2.1 Grundwerte der Informationssicherheit

Aufgabe der Informationssicherheit ist der angemessene Schutz der drei Grundwerte.

- ***Integrität***
  Mit diesem Begriff wird die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen bezeichnet. Bei intakter Integrität sind Daten vollständig und unverändert. Eventuell zugehörige Attribute wurden nicht unerlaubt manipuliert.

- ***Verfügbarkeit***
  Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- ***Vertraulichkeit***
  Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen, aber auch der Zutritt zu Räumlichkeiten dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Die Einhaltung weiterer Grundwerte wird für personenbezogene Daten durch den Datenschutz geprüft

2.2 Anforderungen, Risiken und Ziele

Das Vertrauen unserer Kunden und letztlich unser Geschäftserfolg beruhen darauf, dass wir insbesondere

- die gesetzlichen Vorgaben und hier nicht zuletzt die Datenschutzgesetze einhalten (Compliance),
- unsere Betriebsgeheimnisse schützen,
- die Vertraulichkeit der Daten unserer Kunden wahren,
- unsere Projekte und Dienstleistungen in der geplanten bzw. zugesicherten Zeit abwickeln,

Vor diesem Hintergrund ist der Geschäftserfolg unseres Unternehmens davon abhängig, dass wir bestehende Risiken für die genannten Ziele erkennen, durch geeignete Maßnahmen vermeiden bzw. mindern und verbleibende Risiken geeignet behandeln.

Zu den Risiken zählen die unvollständige bzw. nicht korrekte Einhaltung von gesetzlichen Vorgaben, die unbefugte und ggf. unbemerkte Weitergabe von Betriebsgeheimnissen, die Verletzung von Vorgaben unserer Kunden aufgrund von Systemausfall, Datenverlust sowie unbefugter Preisgabe von Informationen.

3 Bedeutungen der Informationssicherheit für das Unternehmen

3.1 Stellenwert der Informationssicherheit

Die Unternehmensleitung schätzt die strategische und operative Bedeutung der Informationstechnik folgendermaßen ein:

Die Informationstechnik dient unserem Unternehmen wesentlich zur Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung sowie für die Aufgaben der Finanz- und Lohnbuchhaltung. Insbesondere für auftragsbezogene Entscheidungen und Investitionen sind aktuelle und korrekte Unternehmensdaten erforderlich. Ein Ausfall von IT-Systemen ist bis zu einem Tag überbrückbar, darüber hinaus wären Beeinträchtigungen der Auftragsabwicklung und der Unternehmenskommunikation zwischen Verwaltung, Großhändler und Kunden riskant.

Vor dem Hintergrund der externen und internen Anforderungen, vor allem aber den Sicherheitsanforderungen unserer Kunden ist Informationssicherheit ein integraler Bestandteil unserer Unternehmenskultur.

Jeder Mitarbeiter / jede Mitarbeiterin ist sich der Notwendigkeit der Informationssicherheit bewusst und kennt die grundsätzlichen Auswirkungen von Risiken auf den Geschäftserfolg.

Neben der Abwehr dieser Angriffe auf Daten und Systeme ist die Aufrechterhaltung des Geschäftsbetriebs ein wesentliches Ziel der Informationssicherheit. Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzungen für die Einhaltung der IT-Sicherheitsziele Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.

Durch die Umsetzung von Sicherheitsmaßnahmen wird sichergestellt, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheit geboten wird, um Informationswerte und personenbezogene Daten zu schützen und die Verfügbarkeit zu gewährleisten.

Die Unternehmensleitung hat aufgrund ihrer Verantwortung für die Informationssicherheit einen IT-Sicherheitsprozess in Gang gesetzt. Dazu gehören die Entwicklung und Umsetzung dieser Leitlinie und eines IT-Sicherheitskonzepts. Die Einhaltung der Leitlinie sowie Aktualität und Angemessenheit des Sicherheitskonzepts werden regelmäßig überprüft.

3.2 Leitsätze der Informationssicherheit (Mindestsicherheitsniveau)

In Abwägung der Gefährdungen, der Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für IT-Sicherheit, hat die Unternehmensleitung bestimmt, dass ein **grundlegendes IT-Sicherheitsniveau** angestrebt werden soll. Das Unternehmen orientiert sich an den folgenden Leitsätzen:

- Das Unternehmen orientiert sich bei der Ausgestaltung ihres Informationssicherheitsprozesses am IT-Grundschutz-Profil für Handwerksbetriebe.
- Der Erfolg von Informationssicherheit kann nur gewährleistet werden, wenn im ganzen Unternehmen einheitliche und angemessene Sicherheitsstandards im Sinne eines Mindeststandards definiert und etabliert werden:
- Die Etablierung eines umfassenden Informationssicherheitsprozesses wird durch die Unternehmensleitung initiiert und aktiv unterstützt.
- Aufwand (finanziell wie personell) und Ziele von Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen.
- Ziel von Informationssicherheit im Unternehmen ist es, einen Zustand zu erreichen bzw. zu erhalten, in dem die Grundwerte der Informationssicherheit entsprechend der Vorgaben der Unternehmensleitung und bestehender rechtlicher Auflagen gewahrt werden und die potentiellen Bedrohungen nur so wirksam werden können, dass die verbleibenden Risiken tragbar sind. Der Fokus liegt dabei auf Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit des jeweiligen Zielobjekts. Das bedeutet, dass auch im Umgang mit elektronischen Dokumenten und Daten Geheimhaltungsanweisungen strikt Folge zu leisten ist.
- Die für das Unternehmen relevanten Gesetze und Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen müssen eingehalten werden.

- Ziel ist, die Sicherheit der IT (gleichwertig neben Leistungsfähigkeit und Funktionalität) im Unternehmen aufrechtzuerhalten, so dass die Geschäftsinformationen bei Bedarf verfügbar sind. Ausfälle der IT haben Beeinträchtigungen des Unternehmens zur Folge. Lang andauernde Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag führen, sind nicht tolerierbar.
- Durch Sicherheitsmängel im Umgang mit IT verursachte Ersatzansprüche, Schadensregulierungen und Image-Schäden müssen verhindert werden. [Kleinere Fehler können toleriert werden.]
- Im Unternehmen sollen für die Zugangskontrolle sowohl physikalische als auch logische Sicherheitsmaßnahmen angewandt werden.
- Bereits betriebene und geplante Informationstechnik soll nach der Vorgehensweise des IT-Grundschutz-Profils für Handwerksbetriebe in einem IT-Sicherheitskonzept erfasst, im Schutzbedarf eingeschätzt, modelliert und auf Sicherheitsmaßnahmen überprüft werden. Sicherheit der IT soll u. a. auch durch Anwenden von Normen und Standards und durch den Einsatz zertifizierter Systeme erreicht werden.
- Informationssicherheit ist eine Gemeinschaftsaufgabe, die von allen Nutzerinnen/Nutzern der IT-Infrastruktur wahrgenommen werden muss. Eine erfolgreiche Umsetzung ist nur durch eine offene Kommunikation und Sensibilisierung der Nutzerinnen/Nutzer sowie durch Einhaltung der Sicherheitsrichtlinien möglich
- Informationssicherheit soll mit Sicherheitsbewusstsein der Beschäftigten bezüglich möglicher Gefährdungen und mit ihrem persönlich-verantwortlichen Verhalten praktiziert und mit organisatorischen und technischen Maßnahmen unterstützt werden. Dafür sollen regelmäßige Fortbildungsmaßnahmen zur IT-Sicherheit durchgeführt werden.
- Die Mitarbeiter/innen unseres Unternehmens erhalten bei Bedarf für den jeweiligen Arbeitsplatz spezielle Sicherheitsregeln, die insbesondere eine Meldepflicht bei Sicherheitsvorkommnissen beinhalten.
- Alle Mitarbeiter/innen haben regelmäßig an den angebotenen Sicherheitsschulungen teilzunehmen
- Jeder Mitarbeiter / jede Mitarbeiterin ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten.
- Die vorliegende Sicherheitsleitlinie ist grundsätzlich nur unternehmensintern zu halten. Bei Bedarf wird die Leitung darüber befinden, ob sie an Dritte (z. B. Kunden, Vertragspartner, Lieferanten) weitergegeben werden kann.

Informationssicherheit ist kein einmaliges Projekt. Informationssicherheit ist ein Prozess, der die Überwachung und Weiterentwicklung der Sicherheitsstandards erfordert. Zur Erfüllung ist die Einführung von Qualitätssicherungsmaßnahmen notwendig. Hierzu werden seitens der Unternehmensleitung alle erforderlichen Maßnahmen getroffen.

4 Informationssicherheitsleitlinie

4.1 Angestrebte Informationssicherheitsziele

Das Unternehmen verfolgt mit Fokus auf Bewahrung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität die folgenden allgemeingültigen Informationssicherheitsziele:

- Zuverlässige Unterstützung des Geschäftsbetriebs und der Geschäftsprozesse durch den IT-Beauftragten/-Dienstleister
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb des Unternehmens
- Schutz von Daten und Informationen unter Berücksichtigung ihrer spezifischen Anforderungen (personenbezogene Daten, Angebots-, Abrechnungsdaten usw.)
- Schutz der Infrastruktur gegen Missbrauch von innen und außen
- Einhaltung gesetzlicher Vorgaben zum Umgang mit Informationen und Systemen
- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der IT-gestützten Verarbeitung personenbezogener Daten
- Aufrechterhaltung der positiven Außendarstellung.

4.2 Sicherheitsniveau

Ziel von Informationssicherheit des Unternehmens ist es, mindestens ein Sicherheitsniveau zu erreichen, das für den grundlegenden Schutzbedarf der Informationen angemessen und ausreichend ist. Die hierzu umzusetzenden Maßnahmen liefern einen soliden grundlegenden Schutz für alle Daten und die verbundenen Komponenten.

4.3 Verfolgte Informationssicherheitsstrategie

Die Informationssicherheitsstrategie wird durch die Geschäftsleitung festgelegt. Das Unternehmen orientiert sich bei der Gestaltung von Informationssicherheit am IT-Grundschutz-Profil für Handwerksbetriebe. Eine Zertifizierung wird zurzeit nicht angestrebt.

Um das definierte Sicherheitsniveau des Unternehmens aufrecht zu erhalten, ist eine fortlaufende Kontrolle und Verbesserung der implementierten Sicherheitsmaßnahmen, Dokumente und des festgelegten Informationssicherheitsprozesses zwingend erforderlich. Dazu wird die Leitlinie zur Informationssicherheit mindestens alle zwei Jahre überprüft und aktualisiert.

4.4 Informationssicherheitsorganisation

4.4.1 Verantwortung

- Der Inhaber ist für die Einschätzung der geschäftlichen Bedeutung (der Information, Technik), für die sichere Nutzung und Kontrolle, inklusive der Einhaltung von Sicherheitsgrundsätzen, Standards und Richtlinien verantwortlich. Die „Inhaber“, auch als Informationseigentümer bezeichnet definieren die erforderliche Zugänglichkeit (der Information, Technik) sowie Art und Umfang der Autorisierung.

Er ist für die Verwaltung der zustehenden Zugriffsrechte der Benutzer verantwortlich und rechenschaftspflichtig.

- Ein IT-Dienstleister, der z. B. aufgrund eines Serviceauftrags für das Unternehmen Leistungen erbringt, hat Vorgaben des „Informationseigentümers“ und diese IT Sicherheitsleitlinie einzuhalten. Damit ist er verantwortlich für die Einhaltung der IT Sicherheitsziele (Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Rechenschaftspflicht und Verbindlichkeit der Informationen). Bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen hat er den „Informationseigentümer“ zu informieren.
- Jeder Mitarbeiter soll im Rahmen seines Umgangs mit IT (als Benutzer, Berater, Geschäftspartner) die erforderliche Integrität und Vertraulichkeit von Informationen sowie Verbindlichkeit und Beweisbarkeit von Geschäftskommunikation gewährleisten und die Richtlinien des Unternehmens einhalten. Unterstützt durch sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten, Sicherheitsvorfälle von innen und außen vermeiden. Erkannte Fehler sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.
- Das Sicherheitsmanagement, bestehend aus Inhaber, IT-Beauftragtem und IT-Dienstleister, ist gemäß den Sicherheitsvorgaben verantwortlich für die Sicherheit im Umgang mit der IT und den Schutz der Geschäftsinformationen, einschließlich der Kunden- und Managementdaten. Ebenso ist es zuständig für die Weiterentwicklung des IT-Sicherheitsniveaus, des IT-Sicherheitskonzepts und für seine Umsetzung und Aufrechterhaltung von Sicherheit im Betrieb.
- Für die Überprüfung der IT-Sicherheit bei der Bearbeitung, Nutzung und Kontrolle von Informationen werden jeweils unabhängige Verantwortliche eingesetzt, die z. B. Zugriffsmöglichkeiten und zugehörige Sicherheitsmaßnahmen kontrollieren.

4.4.2 Verstöße und Folgen

- Beabsichtigte oder grob fahrlässige Handlungen, die die Sicherheit von Daten, Informationen, Anwendungen, IT-Systemen oder des Netzes gefährden, werden als Verstöße verfolgt. Dazu gehören beispielsweise:
  - der Missbrauch von Daten, der finanziellen Verlust verursachen kann, unberechtigte Zugriff auf Informationen bzw. ihre Änderung und unbefugte Übermittlung,
  - die illegale Nutzung von Informationen aus dem Unternehmen,
  - die Gefährdung der IT-Sicherheit der Mitarbeiter, Geschäftspartner und des Unternehmens und
  - die Schädigung des Rufes des Unternehmens.
- Bewusste Zuwiderhandlungen gegen die IT-Sicherheitsleitlinie werden bestraft – gegebenenfalls disziplinarisch, arbeitsrechtlich oder mit zivil- und strafrechtlichen Verfahren, in denen auch Haftungsansprüche und Regressforderungen erhoben werden können.

5 Schlusswort

Funktionierende und sichere Geschäftsprozesse sind eine maßgebliche Voraussetzung für die Leistungsfähigkeit des Unternehmens. Wenn die Grundregeln im Umgang mit Informationen und der IT als Werkzeug zu deren Verarbeitung eingehalten werden, werden damit der Bestand des Unternehmens, aber auch die Arbeitsplätze Mitarbeiter gesichert. Die Unternehmensleitung ist sich ihrer Verantwortung für die Informationssicherheit bewusst und unterstützt daher nachdrücklich jegliche Bemühungen. Das wertvollste Glied in dieser Kette ist jedoch der gesunde Menschenverstand jeder einzelnen Nutzerin, jedes einzelnen Nutzers und Ihre persönliche Bereitschaft, einen Beitrag zur Informationssicherheit leisten.

6 In-Kraft-Treten

Diese Leitlinie tritt mit sofortiger Wirkung in Kraft.

4.1.2 Strukturanalyse (A.1)

Template A.1 Strukturanalyse

Autor:
Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 – 277
Telefax: (06131) 9992 – 8277
E-Mail: j.schueler@hwk.de
Webseite: www.it-sicherheitsbotschafter.de

Stand: Juni. 2020

1 Netzplanerhebung und Komplexitätsreduktion durch Gruppenbildung

1.1 Erhebung

Ausgangspunkt für die IT-Strukturanalyse ist der folgende Netzplan. Um die Übersichtlichkeit zu bewahren, wurde darauf verzichtet, Geräte und Informationen in den Netzplan einzutragen, die bei den nachfolgenden Beschreibungen nicht weiter benötigt werden.

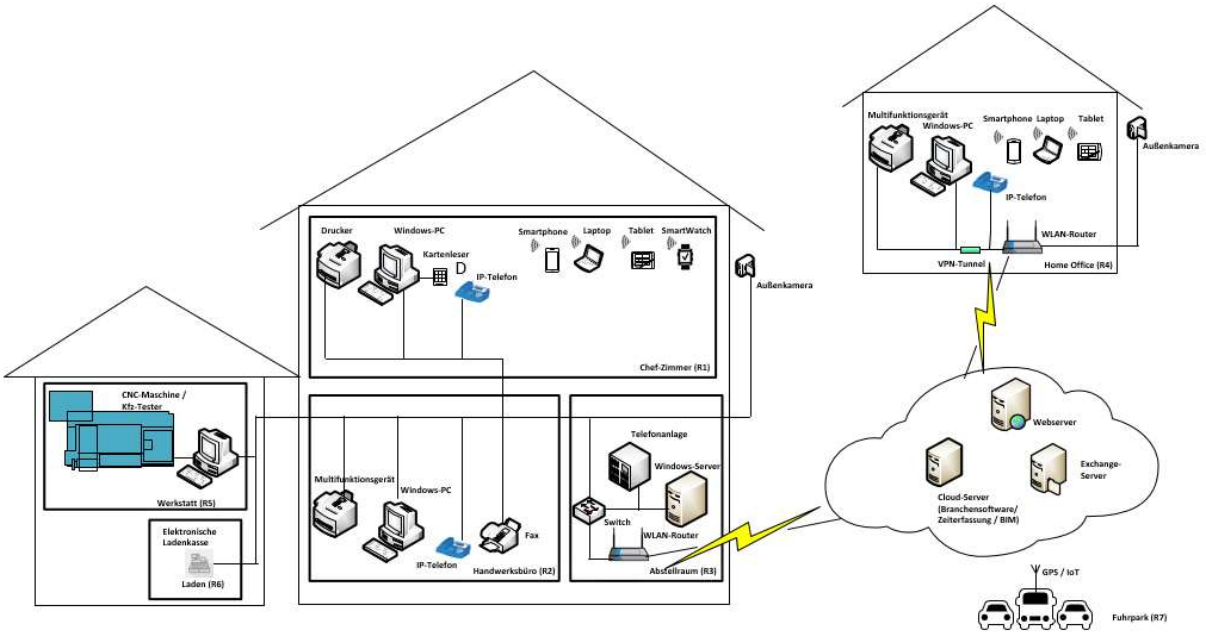

Abb. Möglicher Netzplan eines Unternehmens

1.2 Bereinigung

Nicht alle Informationen des vorliegenden Netzplans sind für die nachfolgenden Schritte beim Vorgehen gemäß IT-Grundschutz-Profil für das Handwerk tatsächlich erforderlich. Zu einer Gruppe zusammengefasst wurden, die Komponenten, die

- vom gleichen Typ sind,
- gleich oder nahezu gleich konfiguriert sind,
- gleich oder nahezu gleich in das Netz eingebunden sind,
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen und
- die gleichen Anwendungen bedienen.

Im bereinigten Netzplan sind Gruppen gebildet worden:

- Die Clients die grundsätzlich gleich ausgestattet sind und mit denen auf weitgehend identische Datenbestände zugegriffen werden kann.
- Büros, die sich durch eine einheitliche IT-Ausstattung auszeichnen, übereinstimmende Aufgaben und Regelungen sowie einer identischen Zugangsmöglichkeit zum Firmennetz haben. Sie lassen sich in gewisser Weise mit häuslichen Telearbeitsplätzen vergleichen. Sie wurden deswegen zu einer Gruppe zusammengefasst.
- Die nicht vernetzten Komponenten Laptops und Faxgeräte wurden Standort übergreifend zu jeweils einer Gruppe zusammengefasst, da für den Umgang mit diesen Geräten übereinstimmende organisatorische Regelungen gelten.

Folgende Clients sollten nicht zusammengefasst werden:

- Bei den Rechnern der Geschäftsführung kann man von einem höheren Schutzbedarf ausgehen (z. B. könnte auf ihnen besonders vertrauliche Korrespondenz gespeichert sein).
- Die größere Sensibilität der Daten ist auch ein Grund dafür, die Rechner der Entwicklungsabteilung/Produktion gesondert zu erfassen. Auf ihnen befinden sich Konstruktionspläne und unter Umständen kundenspezifische Entwicklungen und Verfahrensbeschreibungen, die z. B. vor Wirtschaftsspionage und damit möglichen gravierenden wirtschaftlichen Folgen für die Firma zu schützen sind.
- Eine hohe Vertraulichkeit besitzen die Daten der Finanz- und Lohnbuchhaltung.

2 Erfassungen der IT-Systeme

Bei der Erhebung der IT-Systeme geht es darum, die vorhandenen und geplanten IT-Systeme und die sie jeweils charakterisierenden Angaben zusammenzustellen. Dazu zählen

- alle im Netz vorhandenen Computer (Clients und Server), Gruppen von Computern und aktiven Netzkomponenten, Netzdrucker, aber auch
- nicht vernetzte Computer wie Internet PCs und Laptops,
- Telekommunikationskomponenten wie TK-Anlagen, Faxgeräte, Mobiltelefone und Anrufbeantworter.

Aufgrund der damit verbundenen besseren Übersichtlichkeit empfiehlt sich die folgende tabellarische Darstellung:

2.1 Übersicht Clients

Kürzel	Name	Erläuterung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform
C001	**Clients Handwerksbüro Branchensoftware/ Buchhaltung**	Bei den Clients handelt es sich um handelsübliche Clients.	Kalkulation / Faktura/ Buchhaltung	1	Betrieb	Windows 10
C002	**Client Chefzimmer**	Bei dem Client handelt es sich um einen handelsüblichen Client.	Geschäftsführung	1	Betrieb	Windows 10
C003	**Clients der Produktion**	Bei den Clients handelt es sich um handelsübliche Clients.	Produktion	1	Betrieb	Windows 10
C004	**Client Home Office**	Bei dem Client handelt es sich um einen handelsüblichen Client.	Geschäftsführung	1	Betrieb	Windows 10

2.2 Übersicht Laptops/ Mobile Geräte

Kürzel	Name	Erläuterung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform
L001	**Laptops der Geschäftsführung**	Bei den Laptops handelt es sich um handelsübliche Laptops. Die Geschäftsführung nutzt die Laptops ausschließlich für Kundenbesuche	Geschäftsführung	1	Betrieb	Windows 10
L002	**Laptops Kundendienst**	Bei den Laptops handelt es sich um handelsübliche Laptops.	Mitarbeiter	1	Betrieb	Windows 10
M001	**Smartphone(iPhone)**	Geschäftsführer und Mitarbeiter, haben ein Diensthandy für die Kommunikation bei Terminen, sowie den Zugriff auf Mails.	Geschäftsführung, Mitarbeiter bei Kundenaufträgen	5	Betrieb	IOS
M002	**Tablet (iPad)**	Die GF hat ein iPad.	Geschäftsführung	1	Betrieb	IOS

2.3 Übersicht über die Internet of Things-Systeme (IoT)

Kürzel	Name	Erläuterung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform
O001	**Video-Überwachung**	Die Videoüberwachung dient zur Überwachung der Eingänge, sowie kritischer Bereiche in den Gebäuden	IT-Betrieb, Geschäftsführung	1	Betrieb	Video-Überwachung
O003	**Alarmanlage**	Alarmanlagen für Firmengebäude	Alle Mitarbeiter	2	Betrieb	Alarmanlage
O002	**VoIP Anlage**	Telefonanlagen für Firmengebäude mit VoIP Telefonen	Alle Mitarbeiter	1	Betrieb	TK-Anlage
O004	**Fax-Gerät**	Das Fax-Gerät dient dem versenden von Faxen an Großhändler und Kunden	Alle Mitarbeiter	1	Betrieb	Fax-Gerät
O005	**Kartenleser**	Der Leser dient dem Generieren rechtsverbindlicher Unterschriften	Geschäftsführung	1	Betrieb	Windows PC
O006	**CNC-Maschine**	Produktion von Komponenten	Mitarbeiter	1	Betrieb	CNC-Maschine

2.4 Übersicht Server

Kürzel	Name	Erläuterung	Mitarbeiter/Benutzer	Anzahl	Status	Plattform
S001	**Domänen-Controller**	Der Domänen-Controller regelt die Authentifizierung von Computern und Benutzern (AD, DNS)	Alle Mitarbeiter	1	Betrieb	Windows Server 2012
S002	**Dateiserver**	Der Dateiserver dient zur Dokumentenablage	Alle Mitarbeiter		Betrieb	
S003	**Druckserver**	Der Druckserver stellt die Prozesse und Ressourcen für die Druckservices zur Verfügung.	Alle Mitarbeiter		Betrieb	
S004	**Kommunikationsserver**	Server für die interne und externe Mail-Kommunikation	Alle Mitarbeiter		Betrieb	

2.5 Übersicht Drucker

Kürzel	Name	Erläuterung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform
D001	**Multifunktionsdrucker**	Bei dem Multifunktionsgerät handelt es sich um Geräte, mit den folgenden Funktionen: Kopieren, Scannen, Faxen, Kopieren.	Alle Mitarbeiter	2	Betrieb	Mutltifunktionsgerät

2.6 Übersicht Netzkomponenten

Kürzel	Name	Erläuterung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform
N001	**Router zum Internet**	Der Router ist der Knotenpunkt zum Internet.	Alle Mitarbeiter	2	Betrieb	DSL Router
N002	**Firewall**	Die Firewall dient zum Schutz zwischen dem Internet und dem internen Netz des Unternehmens sowie zur Verbindung von außerhalb mittels VPN. Die Firewall bildet eine DMZ.	Alle Mitarbeiter	2	Betrieb	Firewall
N003	**Zentrale Switche im Unternehmen und Home Office**	Die gemanagten Switche dienen zur Paketverteilung und als Layer-3-Switch auch als Paketfilter-Firewall im internen Netzwerk.	Alle Mitarbeiter	2	Betrieb	Switch

2.7 Übersicht Telekommunikationskomponenten

Kürzel	Name	Erläuterung	Mitarbeiter/ Benutzer		Status	Plattform
K001	**Internetanschluss**	Außenanschluss des Unternehmens an das Internet. Gleichzeitig Teil der Verbindung zm Home Office und den mobilen Clients.	Alle Mitarbeiter		Betrieb	
K002	**Verbindungen zwischen Netzkomponenten innerhalb des Unternehmens**	Die Netzkomponenten werden untereinander mittels CAT5 Kabel verbunden.	Alle Mitarbeiter		Betrieb	
K003	**Verbindungen zwischen Switches und Servern**	Die Switche und Server werden mittels CAT 5 Kabel verbunden	Alle Mitarbeiter		Betrieb	
K004	**Verbindungen zwischen Switches und Clients**	Die Clients und Switche werden über CAT5 Kabel verbunden.	Alle Mitarbeiter		Betrieb	
K005	**Verbindungen zwischen Switches und Produktionsmaschinen**	Die Produktionsmaschinen werden mittels CAT 5 Kabel verbunden.	IT-Betrieb, Produktion		Betrieb	
K006	**Internetanschluss des Home Office**	Außenanschluss des Home Office an das Internet.	Geschäftsführung		Betrieb	
K007	**Mobile Internetanschlüsse der Laptops**	Die Laptops können sich per WLAN in das Netzwerk einwählen.	Alle Mitarbeiter		Betrieb	

2.8 Übersicht Räume

Kürzel	Name	Erläuterung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform
GB001	**Firmengebäude**	Firmengebäude des Unternehmens XYZ.	Geschäftsführung, Kalkulation, Faktura, Disposition, Buchhaltung	1		Allgemeines Gebäude
GB002	**Home Office**	Wohnhaus der Geschäftsführung	Entwicklung, Produktion, Disposition	1		Allgemeines Gebäude
R001	**Büros Geschäftsführung**	GB001, EG 01	Geschäftsführung	1		Büroraum
R002	**Handwerksbüro**	GB001, EG 02	Kalkulation, Faktura, Disposition, Buchhaltung	1		Büroraum
R003	**Server-/Technikraum**	GB001, EG 03	IT-Betrieb	1		Serverraum
R004	**Produktionshalle**	GB001 Die Halle mit der für die Produktion relevanten Technik.	Produktion	1		Werkhalle
R005	**Besprechungsraum**	GB001 Der Raum dient für interne Besprechungen sowie Termine mit externen.	Alle Mitarbeiter	1		Besprechungsraum
R006	**Büro Geschäftsführung**	GB002 Dachgeschoss	Geschäftsführung	1		Büroraum

3 Erfassungen der IT-Anwendungen und der zugehörigen Informationen

Kürzel	Name	Beschreibung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform / Baustein
A001	**Virtualisierungssoftware**	Software, um die virtuellen Systeme bereitzustellen.	IT-Betrieb	1	Betrieb	
A002	**Active Directory**	Zu allen Benutzern der IT-Systeme werden Informationen zu Gruppenzugehörigkeit, Rechten und Authentisierungsmerkmalen verarbeitet und gespeichert. Diese Anwendung ist über beide Domain Controller verfügbar.	Alle Mitarbeiter	2	Betrieb	Active Directory
A003	**Druckservice**	Über diesen Dienst können alle Mitarbeiter den Multifunktionsdrucker benutzen.	Alle Mitarbeiter	1	Betrieb	Druckservice
A004	**Backupsoftware**	Software, welche ein regelmäßiges Backup durchführt.	IT-Betrieb	1	Betrieb	Backupsoftware
A005	**Updateverwaltung Windows**	Die Anwendung dient zur Updateverteilung an Windows-Clients.	IT-Betrieb	1	Betrieb	
A006	**Auftrags- und Kundenwerwaltung**	Angebotskalkulation, Faktura, Nachkalkulation	Geschäftsführer, Kalkulator, Buchhaltung	3	Betrieb	Branchensoftware
A007	**Textverarbeitung, Präsentation, Tabellenkalkulation**	Geschäftsbriefe, Kommunikation mit Kunden und Personal soweit nicht in der Branchensoftware, Analysen oder Präsentationen werden in einem Office-Produkt verarbeitet.	Alle Mitarbeiter	4	Betrieb	Office-Produkt
A008	**E-Mail-Client**	Diese Anwendung wird von allen Mitarbeitern für die Bearbeitung von Mailnachrichten, Terminen und Kontakten genutzt.	Alle Mitarbeiter	4	Betrieb	Office-Produkt
A009	**Web-Browser**	Auf jedem Client ist ein Web-Browser für die Internetnutzung u.a. zum Zugriff auf Großhänderdaten installiert.	Alle Mitarbeiter	4	Betrieb	Web-Browser
A010	**Finanzbuchhaltung**	Vorkontierung für den Steuerberater	Buchaltung	1	Betrieb	FiBU

Kürzel	Name	Beschreibung	Mitarbeiter/ Benutzer	Anzahl	Status	Plattform / Baustein
A011	**Voice over IP**	Die Anwendung steuert die Telekommunikation über die TK-Anlage.	Alle Mitarbeiter	1	Betrieb	VoIP
A012	**Zeiterfassung**	Zeiterfassung für Faktura und Lohnnachweis, die Anwendung wird über die Fa. XXX über eine Cloud bereitgestellt.	Human Resources, Geschäftsführung	1	Betrieb	Zeiterfassungssoftware
A013	**Webserver**	Webserver für die Webseite	Alle Mitarbeiter	1	Betrieb	Webserver
A014	**Content Management System**	Software zur Gestaltung und Pflege der Webseite.	Vertrieb	1	Betrieb	Webanwendung
A015	**CAD/CAM**	Die Anwendung dient der Simulation und Erstellung von Konstruktionsmodellen für die CNC-Bearbeitung.	Produktion	1	Betrieb	CAD/CAM
A016	**Steuerung der Produktionsanlagen**	Die Anwendung dient zur Steuerung der Produktionsanlagen.	Produktion	1	Betrieb	ICS-System
A017	**Mobile Device Management**	Anwendung zur Verwaltung der Smartphones. Die Anwendung wird über die Fa. XXX über eine Cloud bereitgestellt.	IT-Betrieb	1	Betrieb	Webanwendung

3.1 Erfassungen der Geschäftsprozesse

Die folgenden Geschäftsprozesse wurden im Hinblick auf Vertraulichkeit, Integrität und höchster Bedarf an Verfügbarkeit als wesentlich identifiziert:

Kürzel	Name	Beschreibung	Benutzer	Prozessart
GP001	**Angebotswesen**	In der Angebotsabwicklung werden die Kundenanfragen für Dienstleistungen/Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post oder Mail an den Kunden versendet. Im Angebotswesen werden Kundendaten, Lagerbestände, Anfragen und Angebote bearbeitet.	Geschäftsführer	unterstützender Prozess
GP002	**Auftragsabwicklung**	Kunden vereinbaren im Regelfall einen Vororttermin per Telefon oder E-Mail. Eine Auftragsbestätigung erhält der Kunde nur, wenn er dies ausdrücklich wünscht. Die Auftragsabwicklung verwendet Kundendaten, Lagerbestände, Aufträge und Bestellungen.	Meister	Kerngeschäft
GP003	**Disposition**	In der Disposition werden alle für den Auftrag benötigten Materialien (beschafft. Hierzu erfolgen Anfragen beim Großhändler per E-Mail oder Telefon.	Disposition, Produktion	Kerngeschäft
GP004	**Personal - Gehaltszahlung**	In der Buchhaltung wird insbesondere die monatliche Gehaltszahlung vorbereitet und durchgeführt. Die dazu genutzten Daten sind personenbezogen.	Mitarbeiter FiBU	unterstützender Prozess
GP005	**IT-Betrieb**	Die IT-Dienstleister sorgt für den störungsfreien Betrieb der IT-Infrastruktur der Server, Clients und Netze. Beim Betrieb der Produktions-IT wird sie von Mitarbeitern der Produktionsabteilung unterstützt. Es wird mit Konfigurationsdaten der IT-Systeme gearbeitet.	IT-Betrieb	unterstützender Prozess
GP006	**Produktion**	Die Produktion umfasst alle Phasen von der Materialbereitstellung bis zur Einlagerung des produzierten Materials. Es werden alle Informationen über Aufträge, Lagerbestände und Stücklisten verarbeitet.	Produktion	Kerngeschäft
GP007	**Betrieb der Webseite**	Die Webseite wird durch einen externen Dienstleister gehostet. Die Webseite enthält Neuigkeiten, Ansprechpartner und ein Kontaktformular.	Geschäftsführer	unterstützender Prozess
GP008	**Verwaltung des Mobile Device Managements**	Das Unternehmen nutzt zur Verwaltung der Smartphones und Tablets ein Mobile Device Management.	IT-Betrieb	unterstützender Prozess
GP009	**Nutzung einer Cloud-Umgebung**	Die Cloud dient zum Datenaustausch zwischen mobilem Endgerät und den Clients bzw. Notebooks.	Alle Mitarbeiter	unterstützender Prozess

In den folgenden Tabellen sind die Anwendungen den Servern, Clients, Netz- und Telekommunikationskomponenten zugeordnet, die für deren Ausführung erforderlich sind. Zusätzlich ist für jede IT-Anwendung vermerkt, ob sie personenbezogene Daten verarbeitet oder nicht.

3.1 Zuordnungen der Anwendungen zu den Servern

Kürzel	Name		
S001	**Domain-Controller**		
	Zuordnung	Kürzel	Name
	nötig für	A008	E-Mail-Client
	nötig für	A006	Auftrags- und Kundenverwaltung
	nötig für	A001	Actice Directory
	nötig für	A009	Web-Browser
S002	**Dateiserver**		
	Zuordnung	Kürzel	Name
	nötig für	A004	Backupsoftware
	nötig für	A006	Auftrags- und Kundenverwaltung
	nötig für	A007	MS-Office
	nötig für	A010	Finanzbuchhaltung
	nötig für	A012	Zeiterfassung
		A015	CAD/CAM
S003	**Druckserver**		
	Zuordnung	Kürzel	Name
	nötig für	A003	Druckservice
S004	**Kommunikationsserver**		
	Zuordnung	Kürzel	Name
	nötig für	A011	Voice over IP
	nötig für	A017	Mobile Device Management

3.2 Zuordnungen der Anwendungen zu den Clients

Die folgende Tabelle zeigt die Zuordnung von Clients und Laptops auf Anwendungen.

Kürzel	Name		
C001	**Client Handwerksbüro**		
	Zuordnung	Kürzel	Name
	nötig für	A003	Druckservice
	nötig für	A004	Backupsoftware
	nötig für	A006	Auftrags- und Kundenverwaltung
	nötig für	A007	MS-Office
	nötig für	A008	E-Mail-Client
	nötig für	A009	Web-Browser
	nötig für	A010	Finanzbuchhaltung
	nötig für	A012	Zeiterfassung
	nötig für	A017	Mobile Device Management
C002	**Client Chefzimmer (wie C001 zusätzlich)**		
	Zuordnung	Kürzel	Name
	nötig für	A015	CAD/CAM
C003	**Client Produktion**		
	Zuordnung	Kürzel	Name
	nötig für	A003	Druckservice
	nötig für	A015	CAD/CAM
	nötig für	A016	Steuerung der Produktionsanlage
C003	**PC Home Office**		
	Zuordnung	Kürzel	Name
	nötig für	A007	MS-Office
	nötig für	A008	E-Mail-Client
	nötig für	A009	Web-Browser

Kürzel	Name		
L001	**Laptop Geschäftsführung (wie PC Home Office)**		
	Zuordnung	Kürzel	Name
L002	**Laptop Kundendienst**		
	Zuordnung	Kürzel	Name
	nötig für	A006	Auftrags- und Kundenverwaltung
	nötig für	A007	MS-Office
	nötig für	A008	E-Mail-Client
	nötig für	A009	Web-Browser
	nötig für	A012	Zeiterfassung
M001	**Smartphone (wie Laptop Kundendienst)**		
	Zuordnung	Kürzel	Name
M002	**Tablet (wie Laptop Kundendienst)**		
	Zuordnung	Kürzel	Name

3.4 Zuordnungen von Räumen und IT-Systemen bzw. IT-Komponenten

Kürzel	Name		
R001	**Büro Geschäftsführung (Chef-Zimmer)**		
	Zuordnung	Kürzel	Name
	beinhaltet	C002	PC Geschäftsführung
	beinhaltet	D001	Drucker
	beinhaltet	O002	VoIP Telefon
	beinhaltet	L001	Laptop
	beinhaltet	M001	iPhone
	beinhaltet	M002	Ipad
	beinhaltet	O005	Kartenleser
R002	**Handwerksbüro**		
	Zuordnung	Kürzel	Name
	beinhaltet	C001	PC Handwerksbüro
	beinhaltet	D001	Multifunktions-Drucker
	beinhaltet	O002	VoIP Telefon
	beinhaltet	O004	Fax-Geräte
R003	**Server- / Technikraum (Abstellraum)**		
	Zuordnung	Kürzel	Name
	beinhaltet	N001	WLAN-Router mit integrierter Firewall zum Internet
	beinhaltet	N003	Switch
	beinhaltet	S001	Domänen-Controller
	beinhaltet	S002	Dateiserver / App-Server
	beinhaltet	S003	Druckserver
	beinhaltet	S004	Kommunikationsserver
	beinhaltet	O001	Videoüberwachnung
	beinhaltet	O002	Alarmanlage

R004	Werkstatt / Produktionshalle		
	Zuordnung	Kürzel	Name
	beinhaltet	O006	CNC-Maschine
	beinhaltet	C003	Client Produktion
	beinhaltet	O002	VoIP Telefon
R005	Besprechungsraum		
	Zuordnung	Kürzel	Name
	beinhaltet	O002	VoIP Telefon
Kürzel	Name		
R006	Home Office Geschäftsführer		
	Zuordnung	Kürzel	Name
	beinhaltet	N001	WLAN- Router zum Internet mit integrierter Firewall
	beinhaltet	C004	PC Geschäftsführung
	beinhaltet	L001	Laptop GF
	beinhaltet	D001	Drucker
	beinhaltet	O002	VoIP Telefon
	beinhaltet	M001	iPhone GF
	beinhaltet	M002	iPad GF
	beinhaltet	O001	Videoüberwachung
	beinhaltet	O002	Alarmanlage

3.3 Zuordnung der Anwendungen zu den Netz- und Telekommunikationskomponenten

Netz-/ TK Komponente		Anwendungen																
Kürzel	Name	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17
S001-S004	Server	x	x	x	x	x	x	x	x	x	x		x	x	x	x		x
O002	TK-Anlage											x						
	Strom	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
N001-N003	Router zum Internet					x			x	x		x		x	x			x
N003	Switch	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
D001	Multifunktionsdrucker			x			x	x										

4. Liste der Dienstleister

Dienstleister haben Zutritt, Zugang oder Zugriff zu Zielobjekten. Es werden die folgenden Dienstleister eingesetzt:

Kürzel	Name des Dienstleisters	Beschreibung	Anschrift	Ansprechpartner	Telefon
DL001	Die Putzfee AG	Zuständig für die Gebäudereinigung	Hinter der Pforte 1 55116 Mainz	Herr B.Schmidt	06131 9992-0
DL002	Hosting Webseite GmbH & Co.KG	Hosting der Webseite	Musterstraße 1, 12345 Musterstadt	Frau C. Meier	030-123456
DL003	Telfcom	Dienstleister für die TK-Anlage	Industriestraße 1, 12345 Musterstadt	Herr A. Güll	030-123456
DL004	GetMobileDevice GmbH	Hosting und Wartung des Mobile Device Managements	Stefans Straße 107, 75181 Pforzheim	Frau E. Ellermann	0645-4578
DL005	Indust GmbH & Co.KG	Dienstleister für die CNC-Maschine	Alte Straße 6, 12345 Musterstadt	Frau A. Fuchs	030-123456
DL006	VPN Ware GmbH	Führt Wartungen für VPN durch	Stefans Straße 107, 75181 Pforzheim	Frau K. Lehmann	0645-4578
DL007	Branchensoftware GmbH	Führt Wartungen der Branchensoftware durch	Vor der Pforte 1 55116 Mainz	Frau K. Müller	06131 1234
DL008	FiBu GmbH	Führt Wartungen der Finanzbuchhaltungssoftware durch	Vor der Pforte 1 55116 Mainz	Frau K. Müller	06131 1234
DL009	Telfcom	Dienstleister des Internet-Anschlusses	Industriestraße 1, 12345 Musterstadt	Herr A. Güll	030-123456

4.1.3 Modellierung des Informationsverbunds (A.3)

Template A.3
Modellierung des Informationsverbundes

Autor:
Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz
Telefon: (06131) 9992 – 277
Telefax: (06131) 9992 – 8277
E-Mail: j.schueler@hwk.de
Webseite: www.it-sicherheitsbotschafter.de

Stand: August. 2020

Die folgende Tabelle bietet eine Übersicht über die im Rahmen des IT-Grundschutz-Profils für Handwerksbetriebe ausgewählten Bausteine des IT-Grundschutz-Kompendiums und die entsprechend den verschiedenen Sicherheitsstufen (Fundament, Einsteiger, Fortgeschrittene, Profi, BSI Basisschutz) zu erfüllenden Anforderungen.

	Anforderungen																							
Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24
ISMS.1 Sicherheitsmanagement	X	X	X	X	X	X	X	X	X															
ORP.1 Organisation	X	X	X	X	X																			
ORP.2 Personal	X	X	X	X	X																			
ORP.3 Sensibilisierung und Schulung	X	X	X																					
ORP.4 Identitäts- und Berechtigungsmanagement	X	X	X	X	X	X	X	X	X													X	X	
ORP.5 Compliance Management	X	X	X																					
CON.1 Kryptokonzept	X	X																						
CON.2 Datenschutz	X																							
CON.3 Datensicherungskonzept	X	X		X	X																			
CON.4 Auswahl und Einsatz von Standardsoftware	X	X	X																					
CON.5 Entwicklung und Einsatz von Allg. Anwendungen	X	X	X	X	X																			
CON.6 Löschen und Vernichten	X	X																						
CON.9 Informationsaustausch	X	X	X	X	X	X	X	X																
OPS.1.1.2 Ordnungsgemäße IT-Administration	X	X	X	X	X	X																		
OPS.1.1.3 Patch- und Änderungsmanagement	X	X	X																					
OPS.1.1.4 Schutz vor Schadprogrammen	X	X	X	X	X	X	X																	
OPS.1.1.5 Protokollierung	X	X	X	X	X																			
OPS.1.1.6 Software-Tests und -Freigaben	X	X	X	X	X																			

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24
OPS.1.2.4 Telearbeit (vgl. INF.8)	X	X	X	X	X																			
OPS.1.2.5 Fernwartung	X	X	X	X			X																	
OPS.2.1 Outsourcing für Kunden	X																							
OPS.2.2 Cloud-Nutzung	X	X	X	X																				
DER.1 Detektion von sicherheitsrelevanten Ereignissen	X	X	X	X	X																			
DER.2.1 Behandlung von Sicherheitsvorfällen	X	X	X	X	X	X																		
DER.2.2 Vorsorge für die IT-Forensik	X	X	X																					
DER.3.1 Audits und Revisionen	X	X	X	X																				
DER.4 Notfallmanagement	X	X																						
APP.1.1 Office-Produkte	X	X	X	X																				
APP.1.2 Web-Browser	X	X	X	X																				
APP.1.4 Mobile Anwendungen (Apps)	X	X	X	X	X	X	X	X																
APP.5.1 Allgemeine Groupware	X	X	X	X																				
APP.5.2 Microsoft Exchange und Outlook	X	X	X		X																			
SYS.2.1 Allgemeiner Client	X	X	X	X	X	X	X	X																
SYS.2.2.2 Clients unter Windows 8.1	X	X	X																					
SYS.2.2.3 Clients unter Windows 10	X	X	X	X	X	X																		
SYS.3.1 Laptops	X	X	X	X	X																			
SYS.3.2.1 Allgemeine Smartphones und Tablets	X	X	X	X	X	X	X	X																
SYS.3.2.4 Android	X																							
SYS.3.3 Mobiltelefon	X	X	X	X																				
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	X	X										X												

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24
SYS.4.4 Allgemeines IoT-Gerät	X	X	X	X	X																			
SYS.4.5 Wechseldatenträger	X	X		X	X	X	X			X	X	X	X	X	X	X								
IND.2.1 Allgemeine ICS-Komponente	X	X	X	X	X	X																		
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	X	X	X																					
IND.2.3 Sensoren und Aktoren	X																							
IND.2.4 Maschine	X	X																						
NET.1.1 Netzarchitektur und -design	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X									
NET.2.1 WLAN-Betrieb	X	X	X	X	X	X	X	X																
NET.2.2 WLAN-Nutzung	X	X	X																					
NET.3.1 Router und Switches	X	X	X	X	X	X	X	X	X															
NET.3.2 Firewall	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X									
NET.3.3 VPN	X	X	X	X	X																			
NET.4.1 TK-Anlagen	X	X	X	X	X																			
NET.4.2 VOIP	X	X	X	X	X	X		X																
NET.4.3 Fax	X	X	X																					
INF.1 Allgemeines Gebäude	X	X	X	X	X	X	X	X																
INF.2 Rechenzentrum	X	X	X	X	X	X	X	X	X	X	X													
INF.3 Elektrotechnische Verkabelung	X	X	X																					
INF.4 IT-Verkabelung	X	X	X																					
INF.7 Büroarbeitsplatz	X	X	X	X	X	X	X																	
INF.8 Häuslicher Arbeitsplatz	X	X	X																					
INF.9 Mobiler Arbeitsplatz	X	X	X	X																				

4.2 Zu überprüfende Bausteine

Die nachfolgenden Abschnitte befassen sich beispielhaft mit einigen Bausteinen des IT-Grundschutz-Kompendiums basierend auf dem IT-Sicherheitsniveau „Fundament“. Die Fragen dienen zur Kontrolle, ob die Maßnahmen auch durchgeführt wurden.

Die Ergebnisse der überprüften Bausteine können in einer Software dokumentiert werden. Für jeden Baustein muss konkret ermittelt werden, ob alle Maßnahmen umgesetzt sind, d.h. die Fragen mit „Ja“ beantwortet wurden und wie dies dokumentiert wurde.

In den meisten Fällen gibt es einige Maßnahmen, die noch nicht oder nur teilweise realisiert sind. Der nächste Schritt besteht darin, diese Defizite soweit wie möglich zu beheben.

Mit dem einmaligen Bearbeiten der Templates lässt sich kein dauerhaft sicherer Zustand erreichen. Aktualisieren Sie ihre Templates daher regelmäßig und gehen Sie den Fragenkatalog durch.

Auf den nachfolgenden Seiten sind Templates basierend auf der Modularisierung der Bausteine des Informationsverbundes zusammengestellt, die Sie bei der Erstellung eines Sicherheitskonzepts unterstützen sollen. Auch dieses Ergebnis halten Sie anschließend in Ihrem Ordner für das Sicherheitskonzept fest.

Jedem Template haben wir noch eine Checkliste für die Selbstüberprüfung beigefügt. Nachdem Sie diese Checkliste bearbeitet und ausgefüllt haben, kommt auch sie in den Ordner für das Sicherheitskonzept. Vergessen Sie nicht, die Checklisten regelmäßig neu auszufüllen, um Änderungen an Ihrem IT-Verbund und daraus erforderliche neue Maßnahmen zu erkennen.

4.2.1 CON.2 Datenschutz

Template
Con.2 Datenschutz

Autor:
Henrik Klohs
Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg
Bahnhofstraße 12
15230 Frankfurt (Oder)

Telefon: (0335) 5619 – 122
Telefax: (0335) 5619 – 123
E-Mail: henrik.klohs@hwk-ff.de
Webseite: www.hwk-ff.de

Stand: Januar. 2021

Baustein: Datenschutz (CON.2)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
CON.2 Datenschutz	X																		

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).

CON.2.A1 Umsetzung Standard-Datenschutzmodell

Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG und LDSG) wurden eingehalten. Ein Verzeichnis von Verarbeitungstätigkeiten sowie weitere Dokumentationen wie die Erteilung von Auskünften an Kunden liegen vor.

Checkliste: Datenschutzsicherungskonzept (CON.2)

Leitfragen	Ja	Nein	Nachweis
Liegt ein Verzeichnis von Verarbeitungstätigkeiten vor	□	□	□
Wurden Kunden über die gespeicherten Daten informiert?	□	□	□
Wurden Mitarbeitern, die personenbezogene Daten verarbeiten, zur Wahrung der Vertraulichkeit verpflichtet?	□	□	□
Bei Internetauftritten: Ist ein Impressum und eine Datenschutzerklärung vorhanden?	□	□	□
Wurden Auftragsverarbeitungsverträge mit externen Datenverarbeitern (z.B. Cloudanbieter) abgeschlossen?	□	□	□
Liegt eine Dokumentation zu den Technisch und organisatorische Maßnahmen vor?	□	□	□

4.2.2 CON.3 Datensicherungskonzept

Template
CON.3 Datensicherungskonzept

Autor:
Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 - 277
Telefax: (06131) 9992 - 8277
E-Mail: *j.schueler@hwk.de*
Webseite: *www.it-sicherheitsbotschafter.de* Stand: Januar. 2021

Baustein: Datensicherungskonzept (Con.3)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
CON.3 Datensicherungskonzept	X	X		X	X														

Da auch die besten Sicherheitsmaßnahmen Naturkatastrophen, Brandschäden oder gezielten Vandalismus nicht ausschließen können, ist die regelmäßige Datensicherung immer noch eine unverzichtbare Risikovorsorge. Dazu gehört aber auch, dass Vorkehrungen dafür geschaffen werden, dass die gesicherten Daten außer Haus gelagert werden.

CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen

Das Unternehmen hat in einem Datensicherungskonzept für alle IT-Systeme sowie den darauf ausgeführten Anwendungen das Speicher- und Änderungsvolumen sowie die Verfügbarkeitsanforderungen ermittelt und dokumentiert.

CON.3.A2 Festlegung der Verfahrensweise für die Datensicherung

Im Datensicherungskonzept ist die Verfahrensweise festgelegt, welche Daten in mehreren Sicherungssätzen gesichert werden und wie häufig von wem auf welches Speichermedium gesichert werden. [*Die Datensicherung erfolgt nach der 3-2-1 Backup-Regel.*] Die Aufbewahrungsmodalitäten sind dokumentiert. [*Die täglichen inkrementellen Sicherungssätze werden im Tresor, die wöchentlichen Voll-Sicherungssätze in einem anderen Brandabschnitt gelagert.*] Die Mitarbeiter sind verpflichtet, regelmäßig Sicherungen ihrer lokal gespeicherten Dateien vorzunehmen und sind mit der Wiederherstellung der Daten vertraut. Eine zusätzliche externe [*wöchentliche Voll-*] Sicherung der Daten erfolgt über eine sichere Internetverbindung [*in die Cloud an einem externen Standort*].

CON.3.A4 Erstellung eines Minimaldatensicherungskonzeptes

Im Datensicherungskonzept ist beschrieben,

- welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,
- wie die Datensicherungen [*vollständig, inkrementell oder differenziell*], erstellt und wiederhergestellt werden können,
- welche Parameter zu wählen sind sowie
- welche Hard- und Software [*z.B. NAS bzw. mobile Wechselplatte und z.B. Acronis True Image*] eingesetzt wird.

CON.3.A5 Regelmäßige Datensicherung

Das Unternehmen erstellt nach einem im Datensicherungskonzept festgelegten Plan regelmäßig [*täglich und wöchentlich*] Datensicherungen und schützt diese vor dem Zugriff Dritter. Wichtige Daten werden täglich oder wöchentlich durch eine *Vollsicherung* gesichert. Die Sicherungsdatenträger werden regelmäßig kontrolliert und es wird überprüft, ob die Datensicherung problemlos zurückgespielt werden kann.

Checkliste: Datensicherungskonzept (CON.3)

Leitfragen	Ja	Nein	Nachweis
Gibt es einen Plan für die zentrale Datensicherung?	□	□	□
Gibt es feste Verantwortlichkeiten für die Durchführung der zentralen Datensicherung?	□	□	□
Ist festgelegt, welche Daten wie lange gesichert werden?	□	□	□
Ist berücksichtigt, dass die Daten in mehreren Sicherungssätzen gesichert werden?	□	□	□
Werden die Sicherungssätze an unterschiedlichen Orten innerhalb und außerhalb des Unternehmens verteilt aufbewahrt?	□	□	□
Erfolgt eine externe Sicherung der Daten über eine sichere Internetverbindung?	□	□	□
Werden alle Daten täglich sequenziell und wöchentlich voll gesichert?	□	□	□
Ist eine schnelle Rücksicherung der Daten möglich?	□	□	□
Werden die Sicherungsdatenträger regelmäßig kontrolliert und wird dabei ein Rücksicherungstest durchgeführt?	□	□	□
Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?	□	□	□
Sind die Mitarbeiter verpflichtet, regelmäßig Sicherungen ihrer lokal gespeicherten Dokumente vorzunehmen, und sind sie mit der Wiederherstellung der Daten vertraut?	□	□	□

4.2.3 CON.6 Löschen und Vernichten

Template
CON.6 Löschen und Vernichten

Autor:
Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 – 277
Telefax: (06131) 9992 – 8277
E-Mail: j.schueler@hwk.de
Webseite: www.it-sicherheitsbotschafter.de

Stand: Januar. 2021

Baustein: Löschen und Vernichten (CON.6)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
CON.6 Löschen und vernichten	X	X																	

Schützenswerte, unternehmenskritische Informationen und personenbezogene Daten auf analogen und digitalen Datenträgern sind zuverlässig zu löschen oder zu vernichten, damit diese nicht durch unbefugte Dritte ausgelesen oder entwendet werden können.

CON.6.A1 Regelungen der Vorgehensweise für die Löschung und Vernichtung von Informationen

Es wurde ein Löschkonzept erstellt, welches beschreibt, welche Informationen und Betriebsmittel unter welchen Voraussetzungen gelöscht und wie entsorgt werden dürfen. Für die zentrale Sammlung wurden Entsorgungsbehälter und Aktenvernichter beschafft und im Meisterbüro platziert. Mit dem zertifizierten Outsourcing-Dienstleister wurde eine Abholung auf Abruf vereinbart.

CON.6.A2 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen

Bis zur Entsorgung stehen für analoge Daten verschlossene Entsorgungsbehälter und ein Schredder zur Verfügung. Für die Entsorgung wurde ein zertifizierter Outsourcing-Dienstleister beauftragt, der die Entsorgung schriftlich nachvollziehbar dokumentiert.

Checkliste: Löschen und Vernichten (CON.6)

Leitfragen	Ja	Nein	Nachweis
Existiert ein Löschkonzept?	□	□	□
Existieren abgesicherte Entsorgungsbehälter und Aktenvernichter?	□	□	□
Existiert ein Vertrag mit einem zertifizierten Entsorgungs-Dienstleister und gibt es Entsorgungsprotokolle?	□	□	□
Werden Datenträger vor der Weitergabe sicher gelöscht?	□	□	□
Stehen den Mitarbeitern Tools für ein sicheres Löschen zur Verfügung?	□	□	□
Kennen die Mitarbeiter die Richtlinien für die Löschung und Vernichtung von Informationen?	□	□	□
Nutzen die Mitarbeiter die Tools für sicheres Löschen?	□	□	□
Werden bei der „Aussonderung" neben klassischen IT-Systemen auch IT-Systeme berücksichtigt, die nichtflüchtige Speicherelemente beinhalten, wie Z.B. Drucker, Fax?	□	□	□
Wird der Prozess dokumentiert?	□	□	□

4.2.4 OPS.1.1.3 Patch- und Änderungsmanagement

Template OPS.1.1.3 Patch- und Änderungsmanagement

Autor:
Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 – 277
Telefax: (06131) 9992 – 8277
E-Mail: *j.schueler@hwk.de*
Webseite: *www.it-sicherheitsbotschafter.de*

Stand: Januar. 2021

Baustein: Patch- und Änderungsmanagement (OPS.1.1.3)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
OPS.1.1.3 Patch- und Änderungsmanagement	X	X	X																

Sicherheitslücken und Neuerungen in Programmen erfordern zeitnahe Anpassungen und Aktualisierungen der Software. Ein fehlendes oder vernachlässigtes Patchmanagement führt zu Lücken in der Sicherheit einzelner Komponenten und damit zu möglichen Angriffspunkten.

OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement

Das Unternehmen verfügt über ein Patchmanagement und hat es dokumentiert. Updates werden vom IT-Verantwortlichen geplant und nach Information der Mitarbeiter durchgeführt. Die Verfügbarkeit mobiler Geräte wird bei der Planung berücksichtigt.

Updates der Branchensoftware werden vom Dienstleister im Rahmen eines Wartungsvertrages durchgeführt. Der Patch-Level der auf der IT-Infrastruktur (Server, Clients, mobile Geräte) installierten Software wird über ein Softwaretool (z.B. SUMO bei Clients) ermittelt. Die Verfügbarkeit von Updates wird regelmäßig überprüft.

Vor der Installation aller Updates wird als Rückfall-Lösung eine Sicherung auf ein externes Speichermedium durchgeführt. Die Installation der Updates wird in den Bemerkungen der Sicherung dokumentiert.

OPS.1.1.3.A2 Festlegung der Verantwortlichkeiten

Der IT-Dienstleister ist für das Patch-Management des Betriebssystems, der Anwendungen und der IT-Infrastruktur (Router, Switch etc.) verantwortlich. Die Verantwortung für das Patch-Management der Branchensoftware liegt beim IT-Dienstleister [*bzw. beim Anbieter der Branchensoftware*].

OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen

Updates des Betriebssystems werden zunächst automatisch heruntergeladen. Um Unterbrechungszeiten zu reduzieren, wurden für Betriebssystem-Updates Nutzungszeiten festgelegt. In diesem Zeitraum werden keine Neustarts ausgeführt. Bei der Beschaffung neuer Komponenten werden die Update-Mechanismen überprüft und dokumentiert.

Checkliste: Patch- und Änderungsmanagement (OPS.1.1.3)

Leitfragen	Ja	Nein	Nachweis
Gibt es einen Verantwortlichen für Sicherheits-Updates?	□	□	□
Werden Sicherheits-Updates regelmäßig eingespielt?	□	□	□
Werden Betriebssystem-Updates zentral vorgenommen?	□	□	□
Sind Benutzer verpflichtet, Sicherheits- und Betriebssystem-Updates selbst durchzuführen, wenn sie nie ins Firmennetzwerk eingebunden sind?	□	□	□
Wird die Durchführung der Software-Updates regelmäßig überprüft?	□	□	□
Wurden alle Benutzer darauf hingewiesen, dass Software-Updates nur nach ausdrücklicher Genehmigung des IT-Verantwortlichen heruntergeladen und installiert werden dürfen?	□	□	□

4.2.5 OPS.1.1.4 Schutz vor Schadprogrammen

Template OPS.1.1.4 Schutz vor Schadprogrammen

Autor:
Jürgen Schüler
Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 – 277
Telefax: (06131) 9992 – 8277
E-Mail: j.schueler@hwk.de
Webseite: www.it-sicherheitsbotschafter.de

Stand: August. 2020

Baustein: Schutz vor Schadprogrammen (OPS.1.1.4)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
OPS.1.1.4 Schutz vor Schadprogrammen	X	X	X		X	X	X												

Schadprogramme gelangen zumeist über E-Mail-Anhänge wie z.B. durch infizierte Bewerbungsunterlagen in das Unternehmensnetz und können zum Ausfall der Unternehmens-IT führen. Dem kann durch „Virenschutzprogramme" entgegengewirkt werden.

OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen

Es wurde ein Dokument erstellt, das beschreibt, welche IT-Systeme vor Schadprogrammen wie geschützt werden müssen. Zum Einsatz kommt eine Client-basierte Antiviren-Lösung.

OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen

Schutzmechanismen der IT-Systeme sowie der darauf genutzten Betriebssysteme und Anwendungen und Schutzmechanismen der Browser wurden konfiguriert. Betriebssystem-Patches werden bei Systemstart (Autoupdate des Betriebssystems) bzw. wöchentlich eingespielt. Die installierten Anwendungen werden wöchentlich mit einer Software analysiert und Anwendungs-Patches werden eingespielt.

OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes für Endgeräte

Ein geeignetes Schutzprogramm wurde ausgewählt und auf allen Clients und dem Server installiert.

OPS.1.1.4.A5 Betrieb und Konfiguration von Virenschutzprogrammen

Die Verantwortlichkeiten für die Überwachung und die Aktualisierung von Signaturen wurden festgelegt. Die Eskalationswege wurden geregelt. Dezentrale Filter-Komponenten informieren den potentiellen Empfänger einer Datei oder E-Mail und verschieben diese in eine Quarantäne-Umgebung, ohne automatisch zu löschen. Die Benutzer wissen, welche Änderungen sie an den Konfigurationen vornehmen dürfen und wie sie bei Warn- und Alarmmeldungen reagieren. Ergänzend wurden Vorkehrungen wie Datensicherungen getroffen.

OPS.1.1.4.A6 Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen

Die dezentrale Scan-Engine des Virenschutzprogramms sowie die Signaturen für die Schadprogramme werden regelmäßig bei Systemstart aktualisiert. Updates auf neue Programmversionen erfolgen automatisch auf Vorschlag des Schutzprogramms. Die Benutzer überprüfen nach einem Update die Konfigurationseinstellungen.

OPS.1.1.4.A7 Sensibilisierung und Verpflichtung der Benutzer

Die Benutzer wurden für den sicheren Umgang mit mobilen Datenträgern und den Umgang mit E-Mail-Anhängen sensibilisiert und werden regelmäßig über Bedrohungen durch Schadprogramme aufgeklärt. Sie kennen die grundlegenden Verhaltensregeln, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien aus nicht vertrauenswürdigen Quellen dürfen nicht geöffnet werden.

Checkliste: Schutz vor Schadprogrammen (OPS.1.1.4)

Leitfragen	Ja	Nein	Nachweis
Wurde ein Konzept zur Malware-Abwehr inkl. Patch-Management und Awareness-Maßnahmen erstellt?	□	□	□
Ist dokumentiert, wie der Schutz zu erfolgen hat?	□	□	□
Wurde geprüft, welche Schutzmechanismen die verwendeten IT-Systeme selbst bieten?	□	□	□
Wurden Schutzprogramme ausgewählt und installiert??	□	□	□
Wurde das Virenschutzprogramm entsprechend der Einsatzumgebung konfiguriert?	□	□	□
Wurden Verantwortlichkeiten für die Überwachung, die Aktualisierung von Signaturen und Komponenten und die Eskalationswege geregelt?	□	□	□
Werden das Virenschutzprogramm sowie die Signaturen regelmäßig aktualisiert?	□	□	□
Gibt es einen Verantwortlichen für Sicherheits-Updates und werden diese regelmäßig eingespielt?	□	□	□
Wird die Durchführung der Software-Updates regelmäßig überprüft?	□	□	□
Kennen Benutzer die Verhaltensregeln, um die Gefahr durch Schadprogramme zu reduzieren?	□	□	□
Werden Benutzer regelmäßig über die Bedrohungen durch Schadprogramme aufgeklärt?	□	□	□

4.2.6 APP.1.4 Mobile Anwendungen (Apps)

Template
APP.1.4 Mobile Anwendungen

Autor:
Michael Pfister
Handwerkskammer für Unterfranken
Rennweger Ring 3
97070 Würzburg

Telefon: (0931) 30908 – 1160
Telefax: (0931) 30908 – 1660
E-Mail: m.pfister@hwk-ufr.de
Webseite: www.hwk-ufr.de

Stand: Dezember. 2020

Baustein: Mobile Anwendungen (App.1.4)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
APP.1.4 Mobile Anwendungen (Apps)	X																		

Smartphones, Tablets und ähnliche Geräte sind heute auch in Unternehmen weit verbreitet. Mitarbeiter können so unabhängig von Ort und Zeit auf Daten des Unternehmens, auf Informationen und Anwendungen zugreifen. Mobile Anwendungen (Applikationen, kurz Apps) sind Anwendungen, die auf mobilen Betriebssystemen wie iOS oder Android auf entsprechenden Endgeräten installiert und ausgeführt werden.

APP.1.4.A1 Anforderungsanalyse für die Nutzung von Apps

Bevor eine App installiert und genutzt wird, wurde unter Einbeziehung der jeweiligen Fachverantwortlichen klar definiert, welche Geschäftsprozesse die App unterstützen und an welche IT-Komponenten des Betriebes sie angebunden werden soll. Ferner wurden Sicherheitsanforderungen für die App festgelegt. Außerdem wurden der Schutzbedarf und die rechtlichen Rahmenbedingungen der zu verarbeitenden Daten betrachtet. In der Anforderungsanalyse wurden insbesondere Risiken betrachtet, die sich aus der mobilen Nutzung ergeben. Das Unternehmen prüfte, ob seine Kontroll- und Einflussmöglichkeiten auf die Betriebssystemumgebung mobiler Endgeräte ausreichend sind, um sie sicher nutzen zu können.

Checkliste: Mobile Anwendungen (Apps) APP.1.4

Leitfragen	Ja	Nein	Nachweis
Existiert eine Übersicht welche mobilen Anwendungen auf welchen Geräten installiert sind?	☐	☐	☐
Gibt es Regeln für die Verwendung von mobilen Endgeräten und Apps?	☐	☐	☐
Ist sichergestellt, dass nur vertrauenswürdige App-Stores verwendet werden können?	☐	☐	☐
Werden Updates der Apps zeitnah installiert?	☐	☐	☐

4.2.7 SYS.3.1 Laptops

Template
SYS.3.1 Laptops

Autor:
Hendrik Böker
Handwerkskammer Hildesheim-Südniedersachsen
Braunschweiger Str. 19
31134 Hildesheim

Telefon: (05121) 162 – 114
Telefax: (05121) 703 – 432
E-Mail: hendrik.boeker@hwk-hildesheim.de
Webseite: www.hwk-hildesheim.de

Stand: September. 2020

Baustein: Laptops (SYS.3.1)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
SYS.3.1Laptops	X	X																	

Ein mobil genutzter Laptop muss über externe Netzwerke auf die betriebsrelevanten Daten zugreifen können. Damit zusammenhängend muss der Laptop eine ausreichende Sicherheitsarchitektur besitzen, um vor unbefugtem Zugriff auf die Daten zu schützen.

SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops

Es wurde geregelt, was Mitarbeiter bei der mobilen Nutzung von Laptops berücksichtigen müssen, welche Geräte verwendet werden dürfen und welche Sicherheitsmaßnahmen zu beachten sind. Die Benutzer wurden auf die Regelungen hingewiesen.

SYS.3.1.A2 Zugriffsschutz am Laptop

Auf allen Laptops wird [*ein 20-stelliges Passwort*] als Zugriffsschutz eingesetzt, das verhindert, dass das Gerät unberechtigt benutzt werden kann.

Checkliste: Laptops (SYS.3.1)

Leitfragen	Ja	Nein	Nachweis
Sind die Mitarbeiter mit den Regelungen für die Verwendung von Laptops vertraut?	□	□	□
Ist ein administrativer Zugriffsschutz (Passwort, 2-Faktor-Authentifizierung, o.ä.) für den Laptop eingerichtet?	□	□	□
Besteht ein Update- bzw. Patch-Plan für Laptops?	□	□	□
Ist ein geeigneter Schutzmechanismus (Antivirenprogramm) installiert?	□	□	□
Besteht ein Verfahren zur Datensicherung?	□	□	□

4.2.8 SYS.3.3 Mobiltelefon

Template
SYS.3.3 Mobiltelefon

Autor:
Hendrik Böker
Handwerkskammer Hildesheim-Südniedersachsen
Braunschweiger Str. 19
31134 Hildesheim

Telefon: (05121) 162 – 114
Telefax: (05121) 703 – 432
E-Mail: hendrik.boeker@hwk-hildesheim.de
Webseite: www.hwk-hildesheim.de

Stand: September. 2020

Baustein: Mobiltelefon (SYS.3.3)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
SYS.3.3 Mobiltelefon	X																		

Mobiltelefone besitzen weniger Funktionen als Smartphones und Tablets und sind daher leichter zu administrieren. Dennoch müssen grundlegende Sicherheitseinstellungen vorgenommen werden, um einen Basisschutz zu gewährleisten, vor allem in den Bereichen Telefonie und Nachrichtenübermittlung.

SYS.3.3.A1 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

Für Mobiltelefone, die für Firmenzwecke verwendet werden, besteht eine Nutzungs- und Sicherheitsrichtlinie, die jedem Benutzer ausgehändigt wird.

Checkliste: Mobiltelefon (SYS.3.3)

Leitfragen	Ja	Nein	Nachweis
Lässt sich das Mobiltelefon bei Verlust oder Diebstahl sperren?	□	□	□
Werden die Mitarbeiter hinsichtlich der Sicherheit, der Sicherheitseinstellungen und der Aufbewahrung geschult?	□	□	□

4.2.9 SYS.4.5 Wechseldatenträger

Template
SYS.4.5 Wechseldatenträger

Autor:
Manfred Fülbier
Heinz-Piest-Institut für Handwerkstechnik
an der Leibniz Universität Hannover
Wilhelm-Busch-Straße 18
30167 Hannover

Telefon: (0511) 70155 – 18 ab 01.05.2021 (0176) 561 692 31
Telefax: (0511) 70155 – 32
E-Mail: fuelbier@hpi-hannover.de ab 01.05.2021 manfred.fuelbier@gmx.de
Webseite: www.hpi-hannover.de

Stand: Januar. 2021

Baustein: Wechseldatenträger (SYS.4.5)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
SYS.4.5 Wechseldatenträger	X	X																	

Wechseldatenträger werden oft eingesetzt, um Daten zu transportieren, zu speichern oder um mobil auf sie zugreifen zu können. Zu Wechseldatenträgern gehören externe Festplatten, CD-ROMs, DVDs, Speicherkarten, Magnetbänder und USB-Sticks. Wechseldatenträger können dabei auch Schadsoftware transportieren.

SYS.4.5.A1 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit Wechseldatenträgern

Alle Mitarbeiter sind für den sicheren Umgang mit Wechseldatenträgern sensibilisiert. Die Mitarbeiter sind insbesondere darauf hingewiesen worden, wie sie mit den Wechseldatenträgern umgehen sollen, um einem Verlust oder Diebstahl vorzubeugen und eine lange Lebensdauer zu gewährleisten. Die Mitarbeiter sind darüber informiert, dass keine Wechseldatenträger an die Systeme angeschlossen werden dürfen, die aus unbekannten Quellen stammen.

SYS.4.5.A2 Verlust- bzw. Manipulationsmeldung

Benutzer melden umgehend, wenn ein Wechseldatenträger gestohlen wurde oder der Verdacht einer Manipulation besteht.

Checkliste: Wechseldatenträger (SYS.4.5)

Leitfragen	Ja	Nein	Nachweis
Sind die Mitarbeiter informiert, dass keine unbekannten Wechseldatenträger an die Systeme angeschlossen werden dürfen?	□	□	□
Sind die Meldewege für den Verlust oder Manipulationsverdacht an Wechseldatenträgern bekannt?	□	□	□
Wird der Wechseldatenträger auf Schadsoftware überprüft, bevor auf die Daten zugegriffen werden kann?	□	□	□

4.2.10 NET.2.2 WLAN-Nutzung

Template
NET.2.2 WLAN-Nutzung

Autor:
Michael Pfister
Handwerkskammer für Unterfranken
Rennweger Ring 3
97070 Würzburg

Telefon: (0931) 30908 – 1160
Telefax: (0931) 30908 – 1660
E-Mail: *m.pfister@hwk-ufr.de*
Webseite: *www.hwk-ufr.de*

Stand: Dezember. 2020

Baustein: WLAN-Nutzung (Net.2.2)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
NET.2.2 WLAN-Nutzung		X																	

Über WLAN können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden.

NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzer

Die Benutzer wurden für die möglichen Gefahren sensibilisiert, die von fremden WLANs ausgehen.

Checkliste: WLAN-Nutzung (Net.2.2)

Leitfragen	Ja	Nein	Nachweis
Wurden die WLAN-Nutzer über mögliche Gefahren sensibilisiert und geschult?	□	□	□
Sind die WLAN-Nutzer über die Verwendung von externen Hotspots sensibilisiert?	□	□	□

4.2.11 NET.3.1 Router und Switches

Template
NET.3.1 Router und Switches

Autor:
Michael Pfister
Handwerkskammer für Unterfranken
Rennweger Ring 3
97070 Würzburg

Telefon: (0931) 30908 – 1160
Telefax: (0931) 30908 – 1660
E-Mail: *m.pfister@hwk-ufr.de*
Webseite: *www.hwk-ufr.de*

Stand: Dezember. 2020

Baustein: Router und Switches (Net.3.1)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
NET.3.1 Router und Switches	X																		

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

NET.3.1.A1 Sichere Grundkonfiguration eines Routers oder Switches

Der Router oder Switch wurde vor dem Einsatz durch eine autorisierte Person sicher konfiguriert. Die Integrität der Konfigurationsdateien wurde geschützt und die Passwörter verschlüsselt gespeichert. Alle Änderungen wurden dokumentiert. Router und Switches wurden so konfiguriert, dass nur zwingend erforderliche Dienste, Protokolle und funktionale Erweiterungen genutzt werden. Nicht benötigte Dienste, Protokolle und funktionale Erweiterungen wurden deaktiviert oder ganz deinstalliert. Ebenfalls wurden nicht benutzte Schnittstellen auf Routern und Switches deaktiviert.

Checkliste: Router und Switches (Net.3.1)

Leitfragen	Ja	Nein	Nachweis
Wurde der Router sicher konfiguriert?	□	□	□
Wurden die Konfigurationsdateien durch ein Passwort geschützt?	□	□	□
Wurden alle Updates und Patches eingespielt?	□	□	□
Wurde geregelt, wer auf das System zugreifen darf?	□	□	□
Werden regelmäßige Datensicherungen erstellt?	□	□	□

4.2.12 NET.4.3 Fax

Template
NET.4.3 Fax

Autor:
Henrik Klohs
Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg
Bahnhofstraße 12
15230 Frankfurt (Oder)

Telefon: (0335) 5619 – 122
Telefax: (0335) 5619 – 123
E-Mail: henrik.klohs@hwk-ff.de
Webseite: www.hwk-ff.de

Stand: Januar. 2021

Baustein: Fax (NET.4.3)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
NET.4.3 Fax	X	X																	

In Handwerksbetrieben sind Faxgeräte und Multifunktionsgeräte fester Bestandteil der IT im Büroumfeld und können für Angreifer auch als Angriffsweg dienen, da vertrauenswürdige Informationen und Inhalte auch per Fax versendet werden. Um die Vertraulichkeit und Integrität der übermittelten Daten zu schützen, ist es wichtig Maßnahmen gegen den Zugriff bzw. die Manipulation durch Unbefugte zu implementieren.

NET.4.3.A1 Geeignete Aufstellung eines Faxgerätes

Das Faxgerät [*z. B. RICOH…, Brother MFC …, …*] ist in einem Bereich aufgestellt, der nicht frei öffentlich zugänglich ist, sodass eingehende Faxsendungen nicht von Unberechtigten eingesehen oder entnommen werden können. Ein Verantwortlicher zur Kontrolle des Zutritts zu diesem Bereich oder der Nutzung des Faxgerätes wurde benannt.

NET.4.3.A2 Informationen für alle Mitarbeiter über die Faxnutzung

Alle Beschäftigten wurden auf die Besonderheiten der Informationsübermittlung per Fax hingewiesen. Eine verständliche Bedienungsanleitung mit Anweisung zur korrekten Faxnutzung liegt am Faxgerät aus.

Checkliste: Fax (NET.4.3)

Leitfragen	Ja	Nein	Nachweis
Sind das Faxgerät und das Lesen von Faxsendungen vor Unbefugten geschützt?	□	□	□
Liegt eine verständliche Bedienungsanleitung mit Anweisung zur korrekten Faxnutzung am Faxgerät vor?	□	□	□
Wurde auf die Besonderheiten der Informationsübermittlung per Fax hingewiesen?	□	□	□
Werden Einzelsendenachweise bzw. Übertragungsprotokolle für die korrekte Übertragung kontrolliert, diese den Unterlagen beigefügt und bei Bedarf archiviert?	□	□	□

4.2.13 INF.3 Elektrotechnische Verkabelung

Template
INF.3 Elektrotechnische Verkabelung

Autor:
Sven-Erik Laars
Handwerkskammer Erfurt
Fischmarkt 13
99084 Erfurt

Telefon: (0361) 6707 – 6280
Telefax: (0361) 6707 – 9368
E-Mail: slaars@hwk-erfurt.de
Webseite: www.hwk-erfurt.de

Stand: September. 2020

Baustein: Elektrotechnische Verkabelung (INF.3)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
INF.3 Elektrotechnische Verkabelung			X																

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher. Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb.

INF.3.A3 - Fachgerechte Installation

Die Installationsarbeiten der elektrotechnischen Verkabelung wurden nach VDE und DIN sorgfältig und fachkundig durchgeführt. Dies garantiert z.B. der Innungsfachbetrieb aus dem Elektrohandwerk, welcher den E-Check durchführt. Damit sind gleichzeitig alle relevanten Normen und Vorschiften der VDE beachtet und garantiert.

Checkliste: Elektrotechnische Verkabelung (INF.3)

Leitfragen	Ja	Nein	Nachweis
Wurde eine geeignete Auswahl nach Umgebungsbedingungen und Notwendigkeit der Übertragungssicherheit an Kabeltypen vorgenommen?	□	□	□
Wird die Installation und Verkabelung nach VDE und DIN durchgeführt?	□	□	□
Übernimmt die Verkabelung ein fachkundiges Elektrohandwerksunternehmen?	□	□	□
Wurde die Planung von einem fachkundigen Elektrohandwerksunternehmen oder einem Elektro-Fachplaner durchgeführt?	□	□	□

4.2.14 INF.7 Büroarbeitsplatz

Template
INF.7 Büroarbeitsplatz

Autor:
Norbert Speier
Handwerkskammer Münster
Bismarckallee 1
48151 Münster

Telefon: (0209) 38077 – 22
Telefax: (0209) 38077 – 99
E-Mail: *norbert.speier@hwk-muenster.de*
Webseite: *www.hwk-muenster.de*

Stand: September. 2020

Baustein: Büroarbeitsplatz (INF.7)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
INF.7 Büroarbeitsplatz	X	X	X		X	X	X												

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

INF.7.A1 Geeignete Auswahl und Nutzung eines Büroraumes

Es werden geeignete Räume als Büroräume genutzt. Diese werden für den Schutzbedarf bzw. das Schutzniveau der dort verarbeiteten Informationen angemessen ausgewählt und ausgestattet.

INF.7.A2 Geschlossene Fenster und abgeschlossene Türen

Wenn Mitarbeiter ihre Büroräume verlassen, werden alle Fenster geschlossen. Befinden sich vertrauliche Informationen in dem Büroraum, werden auch beim kurzfristigen Verlassen die Türen abgeschlossen. Die entsprechenden Vorgaben sind in einer geeigneten Anweisung festgehalten. Ebenso wird darauf geachtet, dass Brand- und Rauchschutztüren tatsächlich geschlossen sind.

INF.7.A3 Fliegende Verkabelung

Die Stromanschlüsse und Zugänge zum Datennetz im Büroraum befinden sich dort, wo die IT-Geräte aufgestellt sind. Verkabelungen, die über den Boden verlaufen, wurden geeignet abgedeckt.

INF.7.A5 Ergonomischer Arbeitsplatz

Die Arbeitsplätze aller Mitarbeiter sind ergonomisch eingerichtet. Vor allem die Bildschirme sind so aufgestellt, dass ein ergonomisches und ungestörtes Arbeiten möglich ist. Dabei wird darauf geachtet, dass Bildschirme nicht durch Unbefugte eingesehen werden können.

INF.7.A6 Aufgeräumter Arbeitsplatz

Jeder Mitarbeiter wird dazu angehalten, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Unbefugte erhalten dadurch keinen Zugang zu IT-Anwendungen und können keine vertraulichen Informationen einsehen.

INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

Die Mitarbeiter werden angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn diese nicht verwendet werden. Dafür stehen geeignete Behältnisse in den Büroräumen oder in deren Umfeld zur Verfügung.

Checkliste: Büroarbeitsplatz (INF.7)

Leitfragen	Ja	Nein	Nachweis
Entsprechen die genutzten Büroräume dem Schutzbedarf der von Ihnen verwendeten Daten?	□	□	□
Gibt es eine Anweisung für die Bereiche, in denen Publikumsverkehr vorhanden ist, dass Türen und Fenster beim Verlassen des Büroraums geschlossen sein müssen?	□	□	□
Befinden sich Stromanschlüsse und Zugänge zum Datennetz an der Stelle, an der die IT-Geräte aufgestellt sind?	□	□	□
Gibt es ein Sicherheitskonzept für die Zutrittsregelung zu dem Betrieb?	□	□	□
Sind die Arbeitsplätze so eingerichtet, dass Daten auf den Monitoren nicht von Unberechtigten eingesehen werden können?	□	□	□
Gibt es eine Anweisung darüber, dass Mitarbeiter ihren Arbeitsplatz aufgeräumt hinterlassen, damit Unbefugte keinen Zugriff auf Daten oder Dokumente haben?	□	□	□
Werden Mitarbeiter angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren und gibt es hierfür geeignete Möglichkeiten?	□	□	□

4.2.15 INF.8 Häuslicher Arbeitsplatz

Template
INF.8 Häuslicher Arbeitsplatz

Autor:
Norbert Speier
Handwerkskammer Münster
Bismarckallee 1
48151 Münster

Telefon: (0209) 38077 – 22
Telefax: (0209) 38077 – 99
E-Mail: *norbert.speier@hwk-muenster.de*
Webseite: *www.hwk-muenster.de*

Stand: September. 2020

Baustein: Häuslicher Arbeitsplatz (INF.8)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
INF.8 Häuslicher Arbeitsplatz	X	X	X																

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 der Arbeitsplatz oft auch für Dritte oder Familienangehörige zugänglich. Das erfordert einen besonders intensiven Blick auf geeignete Schutzmaßnahmen.

INF.8.A1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz

Verfügbarkeit, Vertraulichkeit und Integrität von Daten sind durch ausreichend starken Passwortschutz und Zugangsbeschränkungen gewährleistet. Es sind ausreichend verschließbare Behältnisse wie ein abschließbarer Schreibtisch, Rollcontainer oder Schrank vorhanden.

INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz

Regelungen für den Austausch von Datenträgern und Unterlagen sind festgelegt [*z.B. ausreichend stark gesichertes Behältnis*] und wurden an die Mitarbeiter kommuniziert.

INF.8.A3 Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz

Insbesondere Türen und Fenster sollten während längerer Abwesenheit geschlossen sein.

Checkliste: Häuslicher Arbeitsplatz (INF.8)

Leitfragen	Ja	Nein	Nachweis
Sind ausreichend verschließbare Behältnisse vorhanden?	□	□	□
Gibt es ein Verfahren, durch welches sichergestellt wird, dass die Verbindung zum Firmennetzwerk verschlüsselt erfolgt?	□	□	□
Gibt es eine Anweisung, aus der hervorgeht, mit welchen Endgeräten aus dem häuslichen Arbeitsplatz auf die Firmendaten zugegriffen wird?	□	□	□
Ist sichergestellt, dass der Zugriff auf die Hardware wie auch auf das Firmennetzwerk nur durch Zugriffsschutz (z. B. ausreichend starkes Passwort oder 2FA) möglich ist?	□	□	□
Ist festgelegt, wie der Austausch von Daten und Unterlagen erfolgt und haben die Mitarbeiter Kenntnis darüber?	□	□	□
Gibt es eine Anweisung, wie Unterlagen und Daten auch am häuslichen Arbeitsplatz vor unbefugtem Zugriff zu schützen sind (z. B. Schließen von Fenstern und Türen bei Abwesenheit)?	□	□	□

5 Zusammenfassung

Die aufgezeigte Vorgehensweise hat Sie schrittweise an die Erstellung der Sicherheitskonzeption für den IT-Verbund Kleiner Handwerksbetrieb herangeführt. Sie haben nun dokumentiert,

- dass Ihnen Sicherheit wichtig ist und
- welche Maßnahmen Sie hierfür umgesetzt haben.

Der von Ihnen geleistete Aufwand zahlt sich in jedem Fall aus. So beziehen Banken zur Bewertung ihrer Risiken bei einer Kreditvergabe die IT-Risiken der Unternehmen mit ein. Aber auch beim Abschluss einer Versicherung für Ihre IT-Systeme kann sich die vorhandene Sicherheitskonzeption positiv auf die zu zahlenden Beiträge auswirken. Sie können jetzt z. B. leicht nachweisen, dass die Wiederbeschaffung der Daten z. B. im Falle einer defekten Festplatte für Sie kein Problem ist, weil Sie täglich ein Backup erstellen. Die Versicherung könnte sich bei der Risikobewertung also auf die reinen Hardwarekosten beschränken.

Sie haben gelernt, dass IT-Sicherheit nicht kompliziert ist und Sie die Nutzung einer standardisierten Vorgehensweise schnell ans Ziel geführt hat.

IT Sicherheitsmaßnahmen werden nicht zum Selbstzweck eingeführt. Alle Maßnahmen haben das Ziel, **Ihr Kerngeschäft zu sichern**.

6 Glossar

ISB	IT-Sicherheitsbeauftragter
IT-Grundschutz	IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von IT-Verbünden über Standard-Sicherheitsmaßnahmen
IT-Anwendung Programm	Ein Anwendungsprogramm ist beispielsweise ein Text verarbeitungs- oder ein Bildbearbeitungsprogramm.
IT-Sicherheits-konzeption	Die IT-Sicherheitskonzeption ist das „zentrale“ Dokument im IT-Sicherheitsprozess eines Unternehmens. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Eine IT-Sicherheitskonzeption enthält zunächst die Beschreibung des aktuellen Zustandes eines IT-Verbunds und der dort verarbeiteten Informationen. Der aktuelle Zustand eines IT-Verbunds umfasst neben der Beschreibung der technischen Komponenten, der dort betriebenen IT-Anwendungen und dabei zu verarbeitenden Informationen auch eine Auflistung der vorhandenen Schwachstellen, möglicher Bedrohungen und bereits umgesetzter Maßnahmen
IT-System	Unter einem IT-System werden allgemein Geräte verstanden, mit denen Informationen/Daten verarbeitet werden. Dazu gehören nicht nur PCs, sondern auch Geräte wie Kopierer, Faxgeräte oder Telefone
IT-Verbund	Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT eines Unternehmens oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Rechnernetz innerhalb einer Abteilung) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind
LTSB/LTSC	LTSB steht für "*Long Term Servicing Branch Version*". Es handelt es sich dabei um eine Windows-Version, die besonders für sicherheitskritische Systeme geeignet sein soll. Sie bietet dem IT-Profi den vollständigen Enterprise-Support und die Security-

	Updates im Rahmen des Mainstream- und Extended Supports für je fünf Jahre. Dabei ist garantiert, dass Microsoft keine neuen Funktionalitäten in diese Version einbauen wird, so dass die Administratoren auf eine verlässliche Plattform ohne neue Features setzen können. Zudem aktualisieren sich LTSB-Versionen von Windows grundsätzlich nur über WSUS. Der IT-Administrator behält so die volle Kontrolle darüber, wann welche Features auf die Systeme gelangen.
Sandbox-Technologie	Sandbox bezeichnet einen isolierten Bereich, innerhalb dessen Maßnahmen keine Auswirkung auf die äußere Umgebung haben.
Telemetrie	Unter Telemetrie versteht man in der Softwaretechnik das Sammeln von Rohdaten, die per automatischer Datenübertragung durch einen im Hintergrund laufenden Dienst an den Entwickler übertragen werden.
Verzeichnisdienste	Mit Hilfe von Verzeichnisdiensten wie Active Directory kann ein Administrator die Informationen der Objekte organisieren, bereitstellen und überwachen. Den Benutzern des Netzwerkes können Zugriffsbeschränkungen erteilt werden. So darf zum Beispiel nicht jeder Benutzer jede Datei ansehen oder jeden Drucker verwenden.

7 Quellenangaben

IT-Grundschutz-Profil für Handwerksbetriebe (Version 1.)0
Zentralverband des Deutschen Handwerks (ZDH), Berlin, 28.März 2019

IT-Grundschutz-Kompendium (Edition 2020)
Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2020

IT-Grundschutz-Kompendium
Änderungsdokumente zur Edition 2019, Bonn, Februar 2020

Routenplaner: Cyber-Sicherheit für Handwerksbetriebe,
Zentralverband des Deutschen Handwerks (ZDH), Berlin, Juni 2019

Analyse der Telemetriekomponente in Windows 10, Version: 1.2
Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2020

8 Stichwortverzeichnis