IT-Sicherheit im Handwerk

Modularisierung IT-GRUNDSCHUTZ-PROFIL

FÜR HANDWERKSBETRIEBE – Fundament (IT-Sicherheitsleitlinie & Checklisten)

Modularisierung
IT-Grundschutz-Profil Für Handwerksbetriebe
- Fundament (IT-Sicherheitsleitlinie und Checklisten)
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 Checklisten 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.

Mit dieser Unterlage stellen Sie den Stand Ihrer IT-Sicherheit auf Basis der Stufe Fundament fest und dokumentieren diesen. 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. Durch die Checklisten werden Sie mit konkreten Sicherheitsaspekten vertraut gemacht, die beim Umgang mit geschäftsrelevanten Informationen und beim Einsatz von Informationstechnologie in einem kleinen Handwerksbetrieb zu beachten sind.

2 IT-Sicherheitsleitlinie Handwerk

Template
IT-Sicherheitsleitlinie
- Handwerk

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.

3 Checklisten Fundament

Checklisten Fundament - Handwerk

3.1 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 Checklisten lässt sich kein dauerhaft sicherer Zustand erreichen. Gehen Sie regelmäßig den Fragenkatalog durch.

Auf den nachfolgenden Seiten sind Checklisten 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.

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.

3.2 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. Cloudanbietern) abgeschlossen?	□	□	□
Liegt eine Dokumentation zu den Technisch und organisatorische Maßnahmen vor?	□	□	□

3.3 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?	□	□	□

3.4 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?	□	□	□

3.5 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?	□	□	□

3.6 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?	□	□	□

3.7 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?	□	□	□

3.8 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?	□	□	□

3.9 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?	□	□	□

3.10 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?	□	□	□

3.11 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?	□	□	□

3.12 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?	□	□	□

3.13 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 Faxnutzung 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?	□	□	□

3.14 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?	□	□	□

3.15 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?	□	□	□

3.16 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)?	□	□	□

4 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**.

5 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.

6 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

7 Stichwortverzeichnis

M

P

R

S

T

V

W

Z