Mai 2023

DIN SPEC 27076

ICS 03.080.20; 35.030

IT-Sicherheitsberatung für Klein- und Kleinstunternehmen

IT security consulting for small and micro enterprises

Conseil en sécurité informatique pour les petites et micro-entreprises

Gesamtumfang 34 Seiten

Dieses Dokument wurde durch die im Vorwort genannten Verfasser erarbeitet und verabschiedet.

www.din.de
www.beuth.de

Alleinverkauf durch Beuth Verlag GmbH, 10772 Berlin

3419322

Inhalt

Tabellen

Vorwort

Diese DIN SPEC wurde nach dem PAS-Verfahren erarbeitet. Die Erarbeitung von DIN SPEC nach dem PAS-Verfahren erfolgt in DIN SPEC (PAS)-Konsortien und nicht zwingend unter Einbeziehung aller interessierten Kreise.

Die vorliegende DIN SPEC (PAS) ging aus dem Projekt „mIT Standard sicher“ („Entwicklung und Verbreitung eines Standards für KMU-geeignete IT-Sicherheitsberatung/KMU SEC“) im Rahmen der vom Bundesministerium für Wirtschaft und Klimaschutz geförderten Initiative „IT-Sicherheit in der Wirtschaft, Handlungsfeld 2 (Förderkennzeichen: 01MS21003A)“ hervor [10].

Gefördert durch:

IT-Sicherheit IN DER WIRTSCHAFT

Mittelstand-Digital

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

mIT Standard sicher

Die Erarbeitung und Verabschiedung des Dokuments erfolgten durch die nachfolgend genannten Initiatoren und Verfasser:

— B^2 Berlin Beratungsgesellschaft mbH

  Thomas Balzer

— Basec GmbH

  Jannik Schumann

— Bundesamt für Sicherheit in der Informationstechnik

  Manuel Bach, Angela Steiner

— 2Consulting UG (haftungsbeschränkt)

  René Eck

— Datenbeschützerin Regina Stoiber GmbH

  Regina Stoiber

— Der Mittelstand, BVMW e.V.

  Marc Dönges, Julian Rupp

— Deudat GmbH

Mario Arndt

— Digitalagentur Berlin GmbH

Paul Sonnenberg

— DResearch Digital Media Systems GmbH

Ines Peters

— FINOBIT GmbH

Antje Kühn, Stefan Reichel

— IFIS-FR Ingenieurbüro für Informationssicherheit

Bernd Frenz

— Institut für betriebliche Integration und Digitalisierung (IBID), THB

Felix Eifert, Prof. Dr. Andreas Johannsen, Daniel Kant

— InTo-Consulting GmbH

Ines Tóth-Strichirsch

— IT-Dienstleistungsgesellschaft mbH Emsland

Alexander Bose

— LWsystems GmbH & Co. KG

Ansgar Licher

— mindt.systems UG (haftungsbeschränkt)

Heiko Mindt

— OFFICESCHOCH GmbH

Melanie Schoch

— Scio GmbH

Markus Wolff

— Securepoint GmbH

Mathias Millahn

— tti Technologietransfer und Innovationsförderung Magdeburg GmbH

Andreas Neuenfels

— Vidano GmbH

Bianca Bach

Für dieses Thema bestehen derzeit keine Normen im Deutschen Normenwerk.

DIN SPEC (PAS) sind nicht Teil des Deutschen Normenwerks.

Für diese DIN SPEC (PAS) wurde kein Entwurf veröffentlicht.

Trotz großer Anstrengungen zur Sicherstellung der Korrektheit, Verlässlichkeit und Präzision technischer und nicht-technischer Beschreibungen kann das DIN SPEC (PAS)-Konsortium weder eine explizite noch eine implizite Gewährleistung für die Korrektheit des Dokuments übernehmen. Die Anwendung dieses Dokuments geschieht in dem Bewusstsein, dass das DIN SPEC (PAS)-Konsortium für Schäden oder Verluste jeglicher Art nicht haftbar gemacht werden kann. Die Anwendung der vorliegenden DIN SPEC (PAS) entbindet den Nutzer nicht von der Verantwortung für eigenes Handeln und geschieht damit auf eigene Gefahr.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Die kostenfreie Bereitstellung dieses Dokuments als PDF-Version über den Beuth WebShop wurde im Vorfeld finanziert.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Einleitung

Dieses Dokument setzt sich zum Ziel, den Beratungsprozess zwischen IT-Sicherheitsdienstleister und beratenem Unternehmen zu verbessern und somit das IT-Sicherheitsniveau im Mittelstand zu erhöhen. Es legt Anforderungen für einen standardisierten Beratungsprozess zur IT- und Informationssicherheit mit Fokus auf die Zielgruppe der kleinen und Kleinstunternehmen („KKU“) fest, die sich bisher noch nicht bzw. nur in sehr geringem Umfang mit ihrer eigenen Informationssicherheit auseinandergesetzt haben. Als KKU gelten Unternehmen mit bis zu 50 Beschäftigten. Oft ist dieser Gruppe von Unternehmen der eigene Gefährdungsgrad kaum bekannt und die Sensibilisierung für bestehende Risiken gering. Über IT-Fachpersonal oder gar eine eigene IT-Abteilung verfügen diese Unternehmen meist nicht, weswegen sie auf die Unterstützung von externen Beratungsdienstleistern mit Fokus auf IT- und Informationssicherheit angewiesen sind. Diese sollen den für die Zielgruppe handhabbaren, standardisierten Beratungsprozess des vorliegenden Dokuments anwenden und die KKU in der Folge zeit- und kosteneffizient auf ein höheres IT- bzw. Informationssicherheitsniveau heben.

Im Gegensatz zu Dokumenten wie dem IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verzichtet das vorliegende Dokument auf den Anspruch der weitestgehenden Vollständigkeit und fokussiert sich stattdessen auf die Beratung von Unternehmen, die umfangreichere Ansätze aus personellen, finanziellen und zeitlichen Gründen nicht verfolgen können. Ziel ist die Erhebung des IST-Zustands des Informationssicherheitsniveaus eines KKU, die Nennung eines Risiko-Status, die Visualisierung des Risikoprofils sowie das Nennen von verständlichen Handlungsempfehlungen. Dies erreicht dieses Dokument mittels der Beschränkung auf die für die Zielgruppe relevantesten Anforderungen der IT- bzw. Informationssicherheit. Das entwickelte Punktesystem definiert zudem den persönlichen Risiko-Status der Unternehmen, welcher diese auf die zu setzenden Prioritäten aufmerksam macht. Um Zeitaufwand und Kosten möglichst gering zu halten, ist es nötig, eine Option zur digitalen Durchführung des Beratungsprozesses durch Video-Konferenz zu ermöglichen. Dieses Dokument gibt IT-Dienstleistern standardisierte, offene und verständliche Fragen an die Hand, aus deren Antworten sich ein realistisches Bild des Status Quo der Informationssicherheit im befragten Unternehmen ablesen lässt.

Wichtig zu verstehen ist, dass selbst ein Unternehmen, dass alle in diesem Dokument aufgeführten IT-Sicherheitsanforderungen zu 100 Prozent erfüllt und die volle Punktzahl erhält, damit kein sehr gutes Schutzniveau, sondern nur das für ein Klein- oder Kleinstunternehmen vertretbare absolute Minimum an Informationssicherheit nachgewiesen hat. Zum Vergleich: Das IT-Grundschutz-Kompendium des BSI enthält über 800 Seiten mit Anforderungen an die Informationssicherheit eines Unternehmens.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen für einen Beratungsprozess zur IT- und Informationssicherheit zwischen IT-Sicherheitsdienstleister und Unternehmen mit Beratungsbedarf und bis zu 50 Beschäftigten fest. Die Anwendung dieses Dokuments ist für ein kleines oder Kleinstunternehmen mit einem realistischen, niedrigen Aufwand verbunden.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

In diesem Dokument werden keine Begriffe aufgeführt.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— DIN-TERMinologieportal: verfügbar unter https://www.din.de/go/din-term/

— DKE-IEV: verfügbar unter https://www.dke.de/DKE-IEV

4 Allgemeines

4.1 Einleitung

Dieses Dokument sieht eine klare Struktur im Ablauf vor. Es beginnt bei der Anbahnung der Beratung und endet mit der Präsentation des Ergebnisberichts bzw. einer möglichen Wiederholung des Gesamtprozesses nach Umsetzung der Handlungsempfehlungen. Dieser Abschnitt erläutert den beratenden IT-Dienstleistern den Gesamtprozess und geht auf die zu beachtenden Details zur korrekten Durchführung ein.

4.2 Ziele

Die Ziele der IT-Sicherheitsberatung für ein Unternehmen mit Beratungsbedarf sind:

— **Ermittlung des IST-Zustandes der Informationssicherheit des Unternehmens und Sichtbarmachung der wichtigsten Sicherheitsrisiken**. Damit verbunden ist die Generierung eines Risiko-Status, der mit der Aufnahme des IST-Zustandes ermittelt wird. Werden Anforderungen nicht erfüllt, erscheinen diese im Ergebnisbericht deutlich markiert und weisen das Unternehmen auf Handlungsbedarf hin.

— **Unterbreitung von Handlungsempfehlungen**. Das Unternehmen erhält in Form von Handlungsempfehlungen konkrete Vorschläge, wie es seine IT- und Informationssicherheit erhöhen kann. Mögliche staatliche Fördermaßnahmen (Bund, Land, und Kommune), die für das Unternehmen in Frage kommen, um diese Maßnahmen umzusetzen, sollten durch den IT-Dienstleister in den Ergebnisbericht aufgenommen werden.

— **Sensibilisierung**. Der IT-Dienstleister sensibilisiert das Unternehmen bei der Überreichung von Ergebnisbericht und Handlungsempfehlungen für gängige Gefahren.

4.3 Grundsätze

Es gelten die folgenden Grundsätze für den Einsatz dieses Dokumentes:

— Der die Beratung durchführende Dienstleister muss eine objektive Rolle einnehmen.

— Sowohl das zu beratende Unternehmen als auch der die Beratung durchführende Dienstleister müssen alle Angaben nach bestem Wissen und Gewissen machen.

— Der Bericht darf nicht dazu geeignet sein, einen Dritten über das Informationssicherheitsniveau des zu beratenden Unternehmens zu täuschen.

— Die an der Befragung und Berichtserstellung beteiligten Personen müssen die Einhaltung dieser Vorgaben im Bericht durch Unterschrift bestätigen.

4.4 Angemessenheit der Informationssicherheit

Unternehmen, die bei der Anwendung dieses Dokuments einen guten Risiko-Status erreichen und denen daher keine Handlungsempfehlungen unterbreitet werden, sollten sich darauf nicht ausruhen, sondern sich bemühen, zusätzliche Informationssicherheitsanforderungen wie beispielsweise die des IT-Grundschutzes zu erfüllen. Gleiches gilt für Unternehmen, die über deutlich größere personelle und finanzielle Ressourcen verfügen, als sie ein Unternehmen mit weniger als 50 Beschäftigten für die Erhöhung der Informationssicherheit in der Regel aufbringen kann.

Dieses Dokument trägt dem Gedanken Rechnung, dass es sich bei Informationssicherheit nicht um einen Zustand, sondern um einen Prozess handelt.

5 Anforderungen an die durchführenden IT-Dienstleister

Es muss sichergestellt sein, dass der beratende IT-Dienstleister über eine ausreichende fachliche Qualifikation verfügt. Hierzu zählt sowohl akademisches als auch praxisbezogenes Wissen. Die Kompetenz zur Beratung sollte durch nachweisbare Qualifikationen belegt werden können.

Berater sollten folgende Eigenschaften erfüllen:

— mindestens ein Jahr Erfahrung in der Durchführung von IT-Sicherheitsberatungen/Audits;

— mindestens drei Referenzprojekte der Durchführung von IT-Sicherheitsberatungen/Audits mit Klein- oder Kleinstunternehmen;

— Nachweis des für die Beratung notwendigen methodischen Wissens zur Gesprächsmethode des semistrukturierten Leitfadeninterviews, beispielsweise:

  — erfolgreiche Teilnahme an einer Schulung zum Einsatz der DIN SPEC 27076 in der Beratung von KKU;

  — Erfahrung in der Durchführung semistrukturierter Leitfadeninterviews.

6 Durchführung der IT-Sicherheitsberatung

6.1 Gesamtprozess der IT-Sicherheitsberatung

Die Durchführung der IT-Sicherheitsberatung muss in vier Schritten erfolgen:

— Erstinformation des zu beratenden Unternehmens (siehe 6.2);

— Durchführung des Gespräches zur Erhebung des IST-Zustandes (siehe 6.3);

— Auswertung der Erhebungsdaten und Erstellung des Ergebnisberichts (siehe 6.4);

— Präsentation des Ergebnisberichts und Hinweis auf umzusetzende Handlungsempfehlungen (siehe 6.5).

6.2 Erstinformation des zu beratenden Unternehmens

Im ersten Schritt muss ein Informationsgespräch zwischen dem IT-Dienstleister und dem zu beratenden Klein- oder Kleinstunternehmen erfolgen. Dies kann ein Präsenztreffen, ein Online-Meeting oder ein Telefongespräch sein. Der IT-Dienstleister muss das zu beratende Unternehmen hierin über folgende Aspekte informieren:

— den groben Ablauf des Beratungsprozesses, wie in diesem Abschnitt beschrieben;

— den zeitlichen und personellen Aufwand, den der zu beratende Betrieb bei der Umsetzung zu erwarten hat;

— die Personen, die seitens des zu beratenden Betriebes am Prozess teilnehmen sollten. Verpflichtend ist die Teilnahme der Geschäftsführung am gesamten Prozess. Diese muss die mit der IT-Sicherheit oder der grundsätzlichen IT-Infrastruktur im Unternehmen betrauten Personen – sofern vorhanden – für jeden Schritt des Prozesses hinzuziehen. Wurde seitens des Unternehmens ein externer Dienstleister mit dem Management der IT-Infrastruktur bzw. der IT- und Informationssicherheit beauftragt, muss dieser in den Prozess mit eingebunden werden. Ziel ist die zeiteffiziente Umsetzung der Beratungstermine und eine maximale Aussagefähigkeit des zu beratenden Unternehmens;

— die groben Themenbereiche, die im Prozess der Beratung abgefragt werden;

— die Kosten der Beratung nach diesem Dokument und die existierenden Möglichkeiten, die Kosten mittels einer Förderung für das zu beratende Unternehmen zu senken. Hierbei ist klar zwischen der Förderung der Beratung nach diesem Dokument und der Förderung eines möglichen späteren Umsetzungsplan für Maßnahmen, die auf der Beratung basieren, zu unterscheiden. Der IT-Dienstleister sollte dem zu beratenden Unternehmen richtungsweisende Hinweise geben, um einen möglichen Förderantrag zu stellen, sofern dies nicht ausschließlich durch den IT-Dienstleister abdeckbar ist.

Der IT-Dienstleister kann diese Informationen zusätzlich im Anschluss an das Austauschgespräch als Checkliste an das zu beratende Unternehmen aushändigen.

Im selben Informationsgespräch muss der IT-Dienstleister einige Eckdaten des zu beratenden Unternehmens aufnehmen. Damit kann sich der IT-Dienstleister im Vorfeld der Beratung ein grobes Bild des Unternehmens machen. Diese Daten sind später außerdem im Ergebnisbericht anzugeben. Diese Eckdaten sind:

a) Name des Unternehmens (Firma);

b) Sitz des Unternehmens (Straße, Postleitzahl, Stadt, Bundesland, Land);

c) Rechtsform des Unternehmens;

d) Handelsregister-Nummer (falls vorhanden);

e) Name der verantwortlichen Person der Geschäftsführung;

f) Name und Rollen weiterer Personen oder externer Dienstleister, die mit der IT-Sicherheit im Unternehmen beauftragt sind und im Beratungsprozess eingebunden werden sollen;

g) Anzahl der Beschäftigten im Unternehmen insgesamt;

h) Anzahl der Beschäftigten im Unternehmen, die informationstechnische Endgeräte (stationär oder mobil) nutzen;

i) WZ-Code des Unternehmens basierend auf der Klassifikation der Wirtschaftszweige des Statistischen Bundesamtes, Ausgabe 2008 (WZ 2008).

Im Rahmen des Erstinformationsgespräches können auch Fragen vom zu beratenden Unternehmen gestellt werden. Diese müssen beantwortet werden, dürfen aber nicht Inhalte des Erhebungsgespräches vorwegnehmen.

6.3 Durchführung des Gespräches zur Erhebung des IST-Zustandes

6.3.1 Grundsätzliches zum Gespräch zur Erhebung des IST-Zustandes

Für die Erhebung des IST-Zustandes muss ein mindestens dreistündiger Termin vereinbart werden. Der Anforderungskatalog wurde so entwickelt, dass das Gespräch zur Erhebung des IST-Zustandes in der Regel nicht länger als zwei Stunden beansprucht. Diese Zeit kann jedoch je nach Situation des Unternehmens kürzer oder länger ausfallen.

Das Gespräch muss als Präsenztermin oder als Online-Videokonferenz bzw. hybride Online-Videokonferenz stattfinden.

Die gesamte Geschäftsführung des zu beratenden Unternehmens muss an dem Gespräch zur Erhebung des IST-Zustandes teilnehmen.

Falls eine gesonderte Person im Unternehmen für das Thema IT- und Informationssicherheit zuständig ist, muss diese am Evaluationsgespräch teilnehmen.

Falls ein externes Dienstleistungsunternehmen mit der Wahrnehmung von Aufgaben im Bereich Informationssicherheit beauftragt ist, muss dieses am Evaluationsgespräch teilnehmen.

Darüber hinaus sollten Personen, welche nicht mit dem Thema Informationssicherheit betraut sind, nicht am Gespräch teilnehmen.

Personen, welche nicht auskunftsfähig sind, sollten nicht am Gespräch teilnehmen.

Das zu befragende Unternehmen muss sich auf das Gespräch zur Erhebung des IST-Zustandes vorbereiten. Folgende Dokumente sollten, falls vorhanden, beim Gespräch zur eigenen Information zur Verfügung stehen:

— Back-Up-Konzepte;

— Sicherheitsrichtlinien;

— Vertraulichkeitserklärungen;

— Betriebsanweisungen für die IT;

— Notfallpläne;

— Rollenkonzepte;

— Zugriffs- und Zutrittsrechte;

— Übersicht über die hauptsächlich genutzte Hard- und Software.

Die Erhebung des IST-Zustandes ist explizit als Gespräch konzipiert. Es handelt sich nicht um einen Test, bei dem es richtige oder falsche Antworten gibt. Das Gespräch besteht im Stellen der im Anforderungskatalog (siehe Anhang A) aufgeführten Leitfragen und den Antworten der befragten Personen. Die im Anforderungskatalog aufgeführten Fragen stellen eine Hilfestellung für den Dienstleister dar und sollten verwendet werden. Die befragten Personen dürfen jederzeit rückfragen, wenn sie eine Frage nicht verstehen. Der Dienstleister muss sicherstellen, dass die befragten Personen den Inhalt der Fragen verstanden haben.

Das Erhebungsgespräch dient ausschließlich dazu, den Dienstleister in die Lage zu versetzen, herauszufinden, ob das Unternehmen die jeweiligen Anforderungen erfüllt. Das Gespräch darf keine beratenden Anteile besitzen.

Im Gespräch darf der Dienstleister dem befragten Unternehmen gegenüber nicht zu erkennen geben, ob eine Anforderung erfüllt wurde. Sollte ein Unternehmen die Befürchtung haben, eine Anforderung nicht erfüllt zu haben, würde dies vermutlich zu Rückfragen führen („Was war denn falsch?“, „Was sollten wir idealerweise tun?“). Dies zöge die Erhebung in die Länge und führte zwangläufig zu einem Beratungsgespräch, das an dieser Stelle nicht gewünscht ist. Bei Fragen des Unternehmens dazu, ob es eine Anforderung erfüllt hat, muss der Dienstleister daher auf den abschließenden Bericht verweisen.

Da das Erhebungsgespräch auch als Online-Videokonferenz stattfinden kann und keine Vor-Ort-Begehung vorsieht, ist der durchführende Dienstleister darauf angewiesen, die Ausführungen der befragten Personen zur Situation des Unternehmens als Basis seiner Bewertung anzunehmen. Der Dienstleister braucht den Wahrheitsgehalt der Aussagen des Unternehmens nicht zu überprüfen. Der Dienstleister muss die Antworten jedoch auf Plausibilität prüfen. Im Zweifel muss der Dienstleister konkrete Nachfragen stellen.

6.3.2 Anforderungskatalog

Das Erhebungsgespräch basiert auf einem Anforderungskatalog (Tabelle A.1).

Dieser Anforderungskatalog mit den 27 Anforderungen, welche sich in sechs Themenbereiche aufteilen, muss nach der vorgegebenen Reihenfolge gemeinsam mit dem zu beratenden Unternehmen durchgegangen werden.

Der Anforderungskatalog enthält die folgenden Komponenten:

— **Themenbereiche**: Jede Anforderung ist einem von sechs Themenbereichen zugeordnet. Diese sind Organisation & Sensibilisierung, Identitäts- und Berechtigungsmanagement, Datensicherung, Patch- und Änderungsmanagement, Schutz vor Schadprogrammen sowie IT-Systeme und Netzwerke.

— **Anforderung**: Jede Anforderung beschreibt einen Zustand, der im Unternehmen hergestellt sein muss, um die volle Punktzahl für die jeweilige Anforderung zu erreichen. Manche Anforderungen sind in mehrere Komponenten unterteilt (bspw. „01-1“, „01-2“ und „01-3“). Neben den regulären Anforderungen gibt es zudem TOP-Anforderungen, die stärker gewichtet sind.

— **Leitfragen**: Die Leitfragen dienen dazu das zu befragende Unternehmen „ins Erzählen“ zu bringen und den Dienstleister in die Lage zu versetzen, einzuschätzen, ob die Anforderung erfüllt ist.

— **Statuspunkte**: Jede reguläre Anforderung bringt bei Erfüllung 1 Punkt bzw. bei Nicht-Erfüllung 0 Punkte. Besonders wichtige Anforderungen (TOP-Anforderungen) bringen bei Erfüllung 3 Punkte. Bei Nicht-Erfüllung werden 3 Punkte abgezogen. Eine Anforderung kann nur als erfüllt gelten und Punkte erhalten, wenn alle Teilkomponenten (bspw. „01-1“, „01-2“ und „01-3“) erfüllt sind. Detaillierte Ausführungen zum Risiko-Status sind 6.4.1 „Die Errechnung des Risiko-Status“ zu entnehmen.

— **Handlungsempfehlungen**: Die Handlungsempfehlungen sind als kompakte und verständlich formulierte Handlungshilfen für die zu beratenden Klein- und Kleinstunternehmen zu verstehen. Diese werden mit dem Ergebnisbericht ausgehändigt und sollen den Unternehmen konkrete Anhaltspunkte dazu geben, wie eine nicht erfüllte Anforderung zukünftig als „erfüllt“ bewertet werden kann. Die Handlungsempfehlungen müssen bewusst kurz, kompakt und verständlich gehalten, um Klein- bzw. Kleinstunternehmen ohne IT-Fachkenntnis nicht zu überfordern. Erfolgt die Beauftragung eines externen Dienstleisters zur Umsetzung und Verbesserung der Informationssicherheit, wird empfohlen, sich an dieser Handlungsempfehlung zu orientieren.

6.3.3 Durchführung des Erhebungsgesprächs

Dieser Schritt bildet den Kern des definierten Beratungsprozesses ab. Zur Durchführung der Erhebung des IST-Zustandes muss der Anforderungskatalog (Tabelle A.1) mit den Anforderungen zur IT- und Informationssicherheit verwendet werden.

Der Ablauf des Gespräches ist wie folgt:

1) Der Dienstleister nennt den aktuellen Themenbereich und die Anforderungsnummer. Dann stellt er die zugehörige Leitfrage. Die Anforderung selbst ist nur für den Dienstleister gedacht und darf nicht vorgelesen werden.

2) Aus der Antwort muss der Dienstleister selbständig folgern, ob die zugehörige Anforderung erfüllt ist. Er muss so lange nachfragen, bis er dazu eine valide Aussage treffen kann.

3) Der Dienstleister muss dokumentieren, ob die Anforderung erfüllt bzw. nicht erfüllt wurde. Er muss mindestens stichpunktartig dokumentieren, aufgrund welcher Angaben des Unternehmens er zu dieser Bewertung gelangt ist.

4) Leitfragen zu Anforderungen, die für das beratene Unternehmen nicht relevant sind, dürfen nicht vorgelesen werden. In diesem Fall wird die Erfüllung der Anforderung nicht bewertet. Sollten Anforderungen aus besagtem Grund nicht bewertet werden, senkt dies die maximal erreichbare Punktzahl um den durch die Erfüllung der Anforderung erreichbaren Risiko-Status-Wert.

5) Der Vorgang wiederholt sich, bis alle relevanten Anforderungsnummern abgearbeitet wurden.

6.4 Auswertung der Erhebungsdaten und Erstellung des Ergebnisberichts

6.4.1 Errechnung des Risiko-Status

Der Risiko-Status ist der zentrale Wert, der am Ende der IT-Sicherheitsberatung das Gefährdungsrisiko des Unternehmens, auf Basis der in diesem Dokument verankerten Anforderungen, quantifiziert abbildet. Die Summe der zu vergebenen Punkte muss, wie folgt, errechnet werden.

Jede der TOP-Anforderungen erhält:

— bei Erfüllung 3 Punkte;

— bei Nicht-Erfüllung −3 Punkte.

Jede der regulären Anforderungen erhält:

— bei Erfüllung 1 Punkt;

— bei Nicht-Erfüllung 0 Punkte.

Anforderungen müssen entweder als „erfüllt“ oder „nicht erfüllt“ bewertet werden. Eine Bewertung dazwischen, wie z. B. „in Teilen erfüllt“, darf nicht vorgenommen werden. Kann das Unternehmen zu einer Anforderung keine Aussage treffen, obwohl alle für die Aussage relevanten Personen anwesend sind, muss die Anforderung als „nicht erfüllt“ bewertet werden.

Anforderungen stehen entweder allein (bspw. „01“) oder bestehen aus mehreren Komponenten (bspw. „01-1“, „01-2“ und „01-3“). In letzterem Fall darf jedoch nicht ein Punktwert je Komponente vergeben werden, sondern nur je gesamter Anforderung, sofern alle Komponenten erfüllt sind.

Sind einzelne Anforderungen für ein Unternehmen als irrelevant einzustufen, bspw. Anforderungen zum Arbeiten im Homeoffice, wenn es keine Mitarbeiter gibt, die aus dem Homeoffice arbeiten, dürfen nachgelagerte Fragen zu diesem Aspekt nicht gestellt werden. Die für die nicht relevanten Fragen theoretisch zu erreichenden Punkte müssen aus den maximal zu erreichenden Punkten herausgerechnet werden. Das bedeutet, dass der Maximalwert der zu erreichenden Punkte dynamisch ist. Er ist abhängig davon, welche Anforderungen für das Unternehmen relevant sind. Im Ergebnisbericht muss kenntlich gemacht werden, welche Punkte aufgrund von Irrelevanz nicht gewertet wurden. Sind alle Anforderungen für das Unternehmen relevant und werden erfüllt, so sind maximal 37 Punkte zu erreichen.

Obwohl es rechnerisch möglich ist, darf das Endergebnis der Bewertung im Ergebnisbericht keinen negativen Punktwert aufweisen. In diesem Fall muss der Gesamt-Status als 0 angegeben werden.

6.4.2 Erstellung des Ergebnisberichts

6.4.2.1 Struktur des Ergebnisberichts

Nach dem Gespräch zur Erhebung des IST-Zustandes muss der Dienstleister mit den erhobenen Informationen den Ergebnisbericht vorbereiten. Dieser muss aus folgenden Teilen bestehen:

— **Bericht**

Der Bericht sollte eine Länge von maximal 2 DIN-A4-Seiten, welche die wichtigsten Erkenntnisse für das Klein- bzw. Kleinstunternehmen zusammenfassen, haben (siehe 6.4.2.2).

— **Anhang A**

Zusätzlich zu diesen zwei Seiten muss die tabellarische Auflistung der 27 Anforderungen und ihrer Komponenten einschließlich jeweiligem erreichten Status-Wert, stichpunktartiger Begründung und Handlungsempfehlung als Anhang angefügt werden (siehe 6.4.2.3).

— **Anhang B**

Zusätzlich muss eine Auflistung von für das Klein- oder Kleinstunternehmen relevanten Förderprogrammen für die weitere Verbesserung der IT- und Informationssicherheit erstellt und angefügt werden. Dies können Förderungen auf Basis von kommunalen, regionalen, Bundes- oder EU-Mitteln sein. Alle aufgelisteten Förderprogramme müssen für das individuelle Unternehmen relevant und grundsätzlich geeignet sein (siehe 6.4.2.4).

6.4.2.2 Inhalte des Ergebnisberichts

Der Bericht muss folgende Anforderungen erfüllen:

Erste Seite:

a) Die erste Seite des Berichts muss die Überschrift „Ergebnisbericht: Beratung zur IT- und Informationssicherheit für Klein- und Kleinstunternehmen nach DIN SPEC 27076“ verwenden.

b) Rechtsbündig darüber muss das Berichtsdatum eingefügt werden.

c) Darunter muss ein Abschnitt zu den Daten des zu beratenden Unternehmens unter dem Titel „Unternehmensdaten“ angegeben werden. Er muss folgende, zuvor erhobene Daten beinhalten:

   1) Name des Unternehmens (Firma);

   2) Sitz des Unternehmens (Straße, Postleitzahl, Stadt, Bundesland, Land);

   3) Rechtsform des Unternehmens;

   4) Handelsregister-Nummer (falls vorhanden);

   5) Name des verantwortlichen Geschäftsführers/der verantwortlichen Geschäftsführer;

   6) Name und Rollen weiterer Personen oder externer Dienstleister, die mit der IT-Sicherheit im Unternehmen beauftragt sind und in den Beratungsprozess eingebunden waren;

   7) Anzahl der Beschäftigten im Unternehmen insgesamt;

8) Anzahl der Beschäftigten im Unternehmen, die informationstechnische Endgeräte (stationär oder mobil) nutzen;

9) WZ-Code des Unternehmens basierend auf der Klassifikation der Wirtschaftszweige des Statistischen Bundesamtes, Ausgabe 2008 (WZ 2008);

10) Darunter muss der Risiko-Status wie folgt angegeben werden: „Ihr Unternehmen hat XX/XX Punkte erreicht“ (min. Schriftgröße 30). Die Aussage muss von einem erklärenden Text begleitet werden:

11) Wurde die für das Unternehmen maximal erreichbare Punktzahl erreicht, muss folgende Aussage angefügt werden: „Herzlichen Glückwunsch! Ihr Unternehmen erfüllt alle Anforderungen nach DIN SPEC 27076, Anhang A. Ein guter Start für die Informationssicherheit in Ihrem Betrieb! Nehmen Sie nun die nächsten Ziele in den Blick und befragen Sie Ihren durchführenden Dienstleister nach weiterführenden Zertifizierungen und Maßnahmen.“

12) Hat das Unternehmen weniger als die für das Unternehmen erreichbare Maximalpunktzahl erreicht, wobei jedoch alle TOP-Anforderungen erfüllt sind, muss folgende Aussage angefügt werden: „Setzen Sie umgehend die offenen Handlungsempfehlungen um (siehe Seite 2).“

13) Hat das Unternehmen weniger als die für das Unternehmen erreichbare Maximalpunktzahl erreicht und sind nicht alle TOP-Anforderungen erfüllt, muss folgende Aussage angefügt werden: „Setzen Sie umgehend die Handlungsempfehlungen der TOP-Anforderungen und anschließend alle weiteren Handlungsempfehlungen um (siehe Seite 2).“

14) Die Ergebnisse müssen am Ende der 1. Seite mit einem Spinnennetzdiagramm visualisiert werden. Dieses stellt den prozentualen Fortschritt je Themenbereich dar. Jede erfüllte Anforderung des Themenbereichs erhöht den prozentualen Fortschritt der entsprechenden Ecke des Diagramms.

Zweite Seite:

a) Die 2. Seite muss zunächst die zu priorisierenden TOP-Handlungsempfehlungen und dann die weiteren ermittelten Handlungsempfehlungen in Listenform darstellen.

b) Am Ende der 2. Seite muss der folgende Satz abgedruckt sein: „Ich versichere, dass im Gespräch zur Erhebung des IST-Zustandes unseres Unternehmens eine objektive Rolle eingenommen wurde, alle an mich/uns gestellten Fragen nach bestem Wissen und Gewissen beantwortet wurden und der Bericht nicht geeignet ist, einen Dritten über das Informationssicherheitsniveau des zu beratenden Unternehmens zu täuschen.“, Darunter folgt die Unterschrift der Geschäftsführung des befragten Unternehmens einschließlich Vor- und Nachname, Ort und Datum.

c) Darunter muss der folgende Satz abgedruckt sein: „Ich versichere, den hier vorliegenden Bericht nach bestem Wissen und Gewissen erstellt zu haben.“ Darunter folgt die Unterschrift des durchführenden IT-Dienstleisters einschließlich Vor- und Nachname, Ort und Datum.

Weitere Informationen bzw. Details der Beratungsdurchführung können in den Bericht aufgenommen werden, sofern nur so eine Qualifikation für ein bestehendes, relevantes Förderprogramm zur (Ko-)Finanzierung der Beratung nach DIN SPEC 27076 herzustellen ist. Die oben beschriebene Gesamtstruktur muss dabei weiterhin erhalten bleiben.

6.4.2.3 Anhang A des Ergebnisberichts

Der Anhang A zum Ergebnisbericht der Beratung nach diesem Dokument muss angefügt werden und muss folgende Anforderungen erfüllen:

1) Ausführung als DIN-A4-Querformat;

2) Schriftgröße 11;

3) eine maximale Seitenanzahl muss nicht eingehalten werden. Der Umfang soll jedoch so kompakt wie möglich gehalten werden;

4) Titel: „Anhang A: Ihre Ergebnisse im Detail“;

5) tabellarische Auflistung der ausführlichen Ergebnisse und Handlungsempfehlungen zu allen Anforderungen und ihren Komponenten, unabhängig davon, ob die Anforderung erfüllt worden ist oder nicht;

6) die Tabellarische Auflistung hat folgende auszufüllende Tabellenspalten:

   a) Themenbereich;

   b) Anforderung;

   c) Risiko-Status;

   d) Handlungsempfehlung.

Wurde eine Anforderung bzw. Anforderungskomponente nicht erfüllt, muss die Zellenfarbe der gesamten Zeile in Rot hinterlegt werden.

6.4.2.4 Anhang B des Ergebnisberichts

Der Anhang B muss angefügt werden. Dazu muss geprüft werden, ob es aktuelle Fördermöglichkeiten gibt, die für das Unternehmen relevant sind (siehe bspw. [7]).

Der Anhang B muss folgende Anforderungen erfüllen:

1) Ausführung als DIN-A4-Querformat;

2) Schriftgröße 11;

3) eine maximale Seitenanzahl muss nicht eingehalten werden. Der Umfang soll jedoch so kompakt wie möglich gehalten werden;

4) Titel: „Anhang B: Übersicht relevanter Fördermöglichkeiten“;

5) tabellarische Auflistung von für das Unternehmen relevanten Förderprogrammen für die weitere Verbesserung der IT- und Informationssicherheit. Anzuführen sind alle für das beratene Unternehmen relevanten Förderungen auf Basis von kommunalen, regionalen, Bundes- oder EU-Mitteln;

6) die Tabelle enthält die folgenden auszufüllenden Spalten je Fördermöglichkeit:

   a) Fördermittelgeber;

   b) Name der Fördermöglichkeit;

   c) Gegenstand der Förderung;

   d) Weiterführende Informationen.

In der Spalte „Weiterführende Informationen“ ist der Link bzw. die URL zur Fördermöglichkeit anzugeben.

6.5 Präsentation des Ergebnisberichts mit dem beratenen Unternehmen und Hinweis auf wichtigste Handlungsempfehlungen

Für die Präsentation des Ergebnisberichtes und der einzelnen Handlungsempfehlungen muss ein gemeinsamer Termin mit dem Klein- oder Kleinstunternehmen vereinbart werden. Dieser kann ebenfalls als Präsenz- oder Online-Videokonferenz bzw. hybrider Online-Videokonferenz stattfinden. Während des Termins müssen folgende Elemente behandelt werden:

— detaillierte Erläuterung des Ergebnisses sowie des Ergebnisberichts für das beratene Unternehmen;

— Aufzeigen und Erklärung der priorisierten Handlungsempfehlungen, sofern TOP-Anforderungen nicht erfüllt wurden;

— Aufzeigen und Erklärung der weiteren Handlungsempfehlungen;

— Sensibilisierung des beratenen Unternehmens zu den gängigsten Gefahren auf Basis des ermittelten individuellen Risikoprofils;

— restlose Klärung der Fragen des Unternehmens zum Bericht;

— Aufzeigen von relevanten Möglichkeiten zur weiteren Förderung der IT- und Informationssicherheit für die individuellen Bedarfe des Unternehmens (sofern vorhanden). Dies können bspw. Hinweise auf kommunale, regionale, Bundes- oder EU-Förderprogramme sein.

6.6 Mögliche Wiederholung des Prozesses

Ein Unternehmen darf eine Beratung nach diesem Dokument beliebig oft in Anspruch nehmen. Dies ist allerdings erst nach der Umsetzung einiger (möglichst aller) der ermittelten Handlungsempfehlungen sinnvoll.

Durch eine Wiederholung der Beratung kann ein Unternehmen die Verbesserung seines Informationssicherheitsniveaus sichtbar machen.

Anhang A
(normativ)

Anforderungskatalog

Tabelle A.1 — Anforderungskatalog

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
01	TOP	Organisa-tion & Sensibilisie-rung	Die Geschäftsführung muss die Gesamtverantwortung für die Informationssicherheit im Unternehmen tragen.	Wer trägt die Gesamtverantwortung für IT- und Informationssicherheit in Ihrem Unternehmen?	3/−3	Die Geschäftsführung muss die Gesamtverantwortung für die Informationssicherheit im Unternehmen übernehmen. Das Thema IT- und Informationssicherheit muss als relevantes und immer aktuelles Alltagsthema von der Geschäftsleitung in alle Abteilungen des Unternehmens hineingetragen werden. Wenn die Geschäftsführung das Thema Informationssicherheit nicht vorlebt, wird sich das Bewusstsein auch nicht auf die Belegschaft übertragen und führt so zu Sicherheitslücken in allen Abteilungen.
02–1		Organisa-tion & Sensibilisie-rung	Die Geschäftsführung muss – sofern sie sich nicht alleine um die IT kümmert – eine verantwortliche Person benennen können.	Haben Sie jemanden, der für die IT- und Informationssicherheit zuständig ist? Wenn ja, wer ist das?	1/0	Ernennen Sie eine für die Informationssicherheit zuständige Person oder beauftragen Sie formell einen Dienstleister. Die Geschäftsführung ist häufig überlastet. Es hat sich in der Praxis gezeigt, dass bei einem Fehlen von verantwortlichen Personen das Informationssicherheitsrisiko erhöht ist.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
02–2		Organisation & Sensibilisierung	Die Geschäftsführung muss dafür sorgen, dass die für IT- und Informationssicherheit beauftragte Person für die Wahrnehmung ihrer Aufgaben über die notwendigen Kapazitäten verfügt.	Wieviel Kapazitäten stehen Ihnen oder der von Ihnen benannten Person für diese Tätigkeit zur Verfügung?		Die zuständige Person muss über genug freie Kapazitäten verfügen und sich regelmäßig zur IT- und Informationssicherheit weiterbilden können. Eine gewissenhafte Aufgabenwahrnehmung als beauftragte Person ist nur mit entsprechenden Ressourcen sicherzustellen. Die Halbwertszeit von IT-Wissen und Kenntnisse über neue Risikofaktoren (Angriffsszenarien) beschränkt sich auf etwa 1,5 Jahre. Jährliche Schulungen sind daher notwendig.
02–3		Organisation & Sensibilisierung	Die Geschäftsführung muss dafür Sorge tragen, dass die beauftragte Person über relevante Kenntnisse im Bereich der Informationssicherheit verfügt.	Über welche Kenntnisse zur IT- und Informationssicherheit verfügen Sie bzw. die zuständige Person?		Die beauftragte Person muss über relevante Kenntnisse im Bereich der Informationssicherheit verfügen. Diese Kenntnisse beziehen sich auf die internen und externen Risiken, die das Unternehmen betreffen. Schwachstellen und Risiken können nur dann realistisch erkannt und bewertet werden, wenn die zuständige Person über das notwendige Know-How verfügt.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
03		Organisation & Sensibilisierung	Es muss ein Notfallkontakt für unregelmäßige oder ungewöhnliche Vorkommnisse (im IT-System, Telefonanrufe, verdächtige E-Mail-Nachrichten usw.) zur Verfügung stehen. Dies gilt auch für den Verlust von IT-Arbeitsgeräten und Datenträgern.	An wen wenden sich Beschäftigte, wenn ein unregelmäßiges oder ungewöhnliches Vorkommnis erkannt wird oder IT-Arbeitsgeräte verloren gehen? (Beispielsweise eine merkwürdige E-Mail, ungewöhnliches Vorkommnis im System bzw. der Firma)	1/0	Beschäftigte müssen jederzeit eine Ansprechperson (Notfallkontakt) erreichen können, um ungewöhnliche Vorkommnisse oder Verluste unverzüglich zu melden. Bei kritischen Vorkommnissen muss schnell gehandelt werden, um das Ausmaß des Schadens zu begrenzen.
04–1		Organisation & Sensibilisierung	Im Falle eines Sicherheitsvorfalles muss jedem Beschäftigten klar sein, wie er sich zu verhalten hat und wem er was und wann melden muss (Notfallplan)	Angenommen, Sie hätten einen IT-Sicherheitsvorfall in Ihrem Unternehmen. Haben Sie klar geregelt, wie sich Beschäftigte verhalten und wem sie was und wann in welcher Form mitteilen müssen, damit der Vorfall zügig und fachgerecht bearbeitet werden kann? Falls ja, bitte erläutern Sie das näher.	1/0	Es muss ein Notfallplan entwickelt und allen Beschäftigten zur Verfügung gestellt werden. Bei kritischen Vorkommnissen muss schnell und zielgerichtet gehandelt werden. Dies kann nur sichergestellt werden, wenn es einen Notfallplan gibt. Hier erfahren Beschäftigte, wie sie sich verhalten und wem sie was, wann und in welcher Form mitteilen müssen.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
04–2		Organisation & Sensibilisierung	Es muss – wenn es nicht die Geschäftsleitung selbst vornimmt – eine verantwortliche Person benannt werden, die dafür Sorge trägt, dass allen Beschäftigten klar ist, wie sie sich bei einem IT-Notfall zu verhalten haben.	Wer kümmert sich darum, dass Beschäftigte die Verhaltensweisen bei IT-Notfällen kennen und beachten?		Es muss eine Person bestimmt werden, die Beschäftigte über die Verhaltensweisen bei IT-Notfällen informiert und kontrolliert, dass diese Bestimmungen auch eingehalten werden. Nur wenn der IT-Notfallplan von allen eingehalten wird, werden Schäden durch Unsicherheiten und Reaktionsverzögerungen vermieden.
05–1	TOP	Organisation & Sensibilisierung	Alle Unternehmensangehörigen, die die Unternehmens-IT nutzen, müssen mit der IT und dem Netzwerk sicher umgehen und verdächtige Vorkommnisse und Nachrichten (z. B. Phishingmails) identifizieren können. Hierfür bedarf es Einweisungen, Schulungen und Sensibilisierungsmaßnahmen.	Wie stellen Sie sicher, dass alle Firmenangehörigen mit der IT und dem Netzwerk sicher umgehen und verdächtige Vorkommnisse und Nachrichten identifizieren können?	3/−3	Sie müssen sicherstellen, dass alle Firmenangehörigen sicher mit der IT und dem Netzwerk umgehen und verdächtige Vorkommnisse und Nachrichten (z. B. Phishingmails) identifizieren können. Hierfür bedarf es Einweisungen, Schulungen und Sensibilisierungsmaßnahmen. Die IT-Sicherheit eines Unternehmens bemisst sich an der Person, die die größten Unsicherheiten im Umgang mit IT und Netzwerk vorweist.
05–2		Organisation & Sensibilisierung	Externe Personen (z. B. externe Dienstleister) müssen mit der IT und dem Netzwerk – wie Firmenangehörige auch – sicher umgehen können. Hierfür müssen sie entsprechend eingewiesen, geschult oder sensibilisiert worden sein.	Wie stellen Sie sicher, dass externe Personen (z. B. externe Dienstleister) über den gleichen Kenntnisstand verfügen, wie Ihre Beschäftigten, was den sicheren Umgang mit IT und Netzwerk anbelangt?		Sie müssen sicherstellen, dass externe Personen (z. B. externe Dienstleister) sicher mit der IT und dem Netzwerk umgehen können. Die IT-Sicherheit eines Unternehmens bemisst sich an der Person, die die größten Unsicherheiten im Umgang mit IT und Netzwerk vorweist.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
06–1		Organisation & Sensibilisierung	Es müssen interne Regelungen zur Vertraulichkeit formuliert sein.	Haben Sie interne Regelungen zur Vertraulichkeit formuliert? Wenn ja, bitte erläutern Sie diese.	1/0	Die Geschäftsleitung muss interne Regelung zur Vertraulichkeit im Umgang mit der IT formulieren. Zum einen sichert sich die Geschäftsleitung in Haftungsfällen ab, zum anderen werden alle Beschäftigten gleichermaßen im Umgang mit vertraulichen Daten, Firmeninterna usw. sensibilisiert.
06–2		Organisation & Sensibilisierung	Externe Personen (z. B. externe Dienstleister) müssen schriftlich verpflichtet werden, interne Regeln der Vertraulichkeit einzuhalten.	Werden externe Personen (z. B. externe Dienstleister) verpflichtet, interne Regelungen zur Vertraulichkeit einzuhalten?		Die Geschäftsleitung muss interne Regelungen zur Vertraulichkeit für externe Personen (z. B. externe Dienstleister) im Umgang mit der IT formulieren. Zum einen sichert sich die Geschäftsleitung in Haftungsfällen ab, zum anderen werden alle mobil-arbeitenden Personen (Arbeiten im Homeoffice) gleichermaßen im Umgang mit vertraulichen Daten, Firmeninterna usw. sensibilisiert.
07–0		Organisation & Sensibilisierung	Statusabfrage	Haben Sie Beschäftigte, die im Homeoffice oder die mobil arbeiten?		
07–1		Organisation & Sensibilisierung	Es muss eine Richtlinie existieren, die die Sicherheitsmaßnahmen im Homeoffice und beim mobilen Arbeiten festlegt.	Haben Sie eine Richtlinie, die sich auf die Sicherheitsmaßnahmen im Homeoffice und beim mobilen Arbeiten bezieht?	1/0	Es muss eine Richtlinie für Sicherheitsmaßnahmen zum mobilen Arbeiten (Arbeiten im Homeoffice) vorliegen. Zum einen sichert sich die Geschäftsleitung in Haftungsfällen ab, zum anderen werden alle mobil-arbeitenden Personen und solche, die im Homeoffice arbeiten gleichermaßen im Umgang mit vertraulichen Daten, Firmeninterna usw. sensibilisiert.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
07–2		Organisation & Sensibilisierung	Die Richtlinie muss vom Beschäftigten unterschrieben ans Unternehmen zurückgegeben werden.	Wie bestätigen Ihnen die Beschäftigten den Empfang der Richtlinie zu Sicherheitsmaßnahmen?		Die Kenntnisnahme der Richtlinie muss von allen Beschäftigten schriftlich bestätigt werden. So sichert sich die Geschäftsleistung im Haftungsfall ab.
07–3		Organisation & Sensibilisierung	Eine Kopie der Richtlinie muss beim Beschäftigten verbleiben.	Erhalten Beschäftigte eine Kopie?		Die von den Beschäftigten bestätigte Richtlinie muss den Beschäftigten im Anschluss als Kopie ausgehändigt werden. Die Richtlinien können so jederzeit von den Beschäftigten eigenständig eingesehen werden.
07–4		Organisation & Sensibilisierung	Die Richtlinie muss auf Aktualität überprüft werden.	Wann erfolgt eine Prüfung der Richtlinie im Hinblick auf Aktualität?		Prüfen Sie die Richtlinien auf Aktualität, wann immer sich eine Änderung bzgl. Informationssicherheit in Ihrem Unternehmen ergibt (Softwarewechsel, neue Firewall usw.) oder aufgetretene Sicherheitsvorfälle und neue Erkenntnisse öffentlich werden. Wenn die IT-Sicherheitsmaßnahmen nicht auf dem aktuellen Stand der Dinge sind, erhöht sich die Gefahr, dass Sicherheitsvorfälle auftreten.
08–1		Identitäts- und Berechtigungsmanagement	Es muss sichergestellt sein, dass nur berechtigte Personen Zutritt zu den Räumlichkeiten des Unternehmens haben.	Wie regeln Sie, dass ausschließlich berechtigte Personen in Ihr Unternehmen und in bestimmte Räumlichkeiten gelangen?	1/0	Gewähren Sie den Zutritt zu den Räumlichkeiten ausschließlich Personen, die diesen benötigen. Eine Dokumentation zu Zutrittsberechtigungen ist zu empfehlen. Ohne Kontrolle und Dokumentation besteht die Gefahr, dass sich Unbefugte Zutritt zu Ihrer IT verschaffen.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
08–2		Identitäts- und Berech-tigungsma-nagement	Jeder Beschäftigte darf nur Zugriff auf Daten, Ordner, Anwendungen und Netzwerkbereiche haben, für die er zuständig ist.	Haben alle Beschäftigten uneingeschränkten Zugriff auf alle Daten, Ordner, Anwendungen und Netzwerkbereiche?		Gewähren Sie den Zugriff zu den Daten, Ordnern, Anwendungen und Netzwerkbereiche nur denjenigen Personen, die diese benötigen. Wenn jeder Zugriff auf alle Daten, Ordner, Anwendungen und Netzwerkbereiche hat, kann jeder auch alles verändern, löschen und manipulieren, was insgesamt zu einem Kontrollverlust in der Informationssicherheit führt.
09–1		Identitäts- und Berech-tigungsma-nagement	Alle Beschäftigten müssen angewiesen werden, für jedes Benutzerkonto ein individuelles Passwort zu benutzen.	Müssen alle Ihre Beschäftigten bei der Anmeldung an ihren Benutzerkonten immer ein individuelles Passwort nutzen?	1/0	Jeder Beschäftigte muss bei der Anmeldung an seinen Benutzerkonten stets ein individuelles Passwort eingeben. Ohne individuelles Passwort können auch unberechtigte Personen Zugriff auf den Computer erhalten.
09–2		Identitäts- und Berech-tigungsma-nagement	Verwendete Passwörter müssen möglichst lang und komplex sein.	Nach welchem Muster sind Ihre Passwörter zusammengesetzt?		Nutzen Sie möglichst lange und komplexe Passwörter und ggfs. zusätzlich einen Passwortmanager. Es hat sich in der Vergangenheit gezeigt, dass ein langes und komplexes Passwort eine größere Sicherheit bietet und daher schwerer zu hacken ist.
10		Identitäts- und Berech-tigungsma-nagement	Sofern eine 2-Faktor-Authentifizierung von der verwendeten Software bzw. von Cloud-Dienstleistern angeboten wird, muss sie benutzt werden.	Nutzen Sie eine 2-Faktor-Authentifizierung zur Anmeldung wie zum Beispiel Face-ID, Tan-Generator, Fingerprint, usw.?	1/0	Nutzen Sie, wann immer Sie die Möglichkeit haben, die 2-Faktor-Authenifizierung zur Anmeldung an Ihrer Software und zu Online-Diensten. Ein zweiter Faktor erhöht Ihren Schutz – neben einem (komplexen) Passwort – um ein Vielfaches.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
11–0	TOP	Datensiche-rung	Statusabfrage	Führen Sie in Ihrem Unternehmen Datensicherungen durch?		
11–1		Datensiche-rung	Datensicherungen müssen in bestimmten Intervallen (branchenabhängig) durchgeführt werden.	Wie häufig führen Sie die Datensicherung durch? Wie läuft die Datensicherung in Ihrem Unternehmen ab ?	3/−3	Sichern Sie Ihre Daten regelmäßig so, dass bei einem Datenverlust die Fortführung des Geschäftsbetriebes sichergestellt ist. Die Sicherung sollte mindestens einmal wöchentlich erfolgen. Auf eine Aktualität der Datensicherung ist zu achten, da im Falle eines Verlusts mit den Daten aus der Datensicherung weitergearbeitet werden muss. Je älter der Datenbestand aus der Datensicherung ist, desto mehr Daten müssen neu (manuell) rekonstruiert werden, sofern dies überhaupt möglich ist. Datenverluste sind mit hohen Kosten verbunden.
12		Datensiche-rung	Die Datensicherung muss vor unbefugtem Zugriff gesichert werden.	Welche Möglichkeiten nutzen Sie, um Ihre Datensicherung vor unbefugtem Zugriff zu schützen.	1/0	Datenträger, auf dem sich die Datensicherung befinden, müssen immer an sicheren Orten verwahrt werden. Darüber hinaus müssen sie verschlüsselt sein. So wird verhindert, dass Unberechtigte, die trotz allem in Besitz der Datenträger gelangen (könnten), auf die darauf befindlichen Dateien zugreifen können. Hierdurch kann das Unternehmen Schaden erleiden, sowohl finanziell als auch in Bezug auf den guten Ruf.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
13–1		Datensiche-rung	Es muss festgelegt werden, wie die Daten gesichert werden.	Ist das Verfahren der Datensicherung, der Prozess, verschriftlicht? Liegt eine Art Beschreibung vor?	1/0	Es wird empfohlen, ein (verschriftlichtes) Verfahren zu erarbeiten, das Art, Speicherorte, Häufigkeit und Zeitpunkte der Datensicherung festlegt. So können Sie nachvollziehen, wie im Falle eines Schadens (Datenverlust!) Ihre Daten wieder zeitnah und vollständig hergestellt werden können.
13–2		Datensiche-rung	Es muss eine Zuständigkeit festgelegt werden, wer die Daten sichert.	Wer führt die Datensicherung durch?		Wenn Sie sich selbst nicht darum kümmern können, bestimmen Sie eine verantwortliche Person in Ihrem Unternehmen, die sich um die Datensicherung kümmert. Das kann auch ein externer IT-Dienstleister sein. Die Datensicherung ist ein ständiger Prozess, dem besondere Aufmerksamkeit geschenkt werden muss. Nur wenn es eine verantwortliche Person gibt, wird die Datensicherung immer zuverlässig und verbindlich durchgeführt.
14–1		Datensiche-rung	Die Datensicherung muss auf externen Speichermedien abgelegt werden.	Wo wird Ihre Datensicherung gespeichert bzw. abgelegt?	1/0	Die Datensicherung muss auf externen Speichermedien (außerhalb des zu sichernden Systems) erfolgen und abgelegt werden. Wird die Datensicherung im gleichen Raum oder auf dem gleichen System (bzw. Speichermedium) abgelegt, kann sie gleichermaßen vom Schadensfall betroffen sein. Im Schadensfall ist die Datensicherung der einzige Weg zur Wiederherstellung von Daten und IT-Systemen und somit Ihrer Arbeits- und Betriebsfähigkeit.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
14–2		Datensiche-rung	Es muss getestet werden, ob extern gesicherte Daten funktionsfähig und vollständig vorhanden sind.	Wie überprüfen Sie, ob die externe Datensicherung funktioniert hat und ob die Daten vollständig sind?		Es müssen entsprechende Tests der Datensicherungen auf Funktionsfähigkeit und Vollständigkeit (der Daten) durchgeführt werden. Es kann durchaus vorkommen, dass Datensicherungen fehlerhaft sind. Dies ist auf den ersten Blick nicht erkennbar. Tests geben Ihnen entsprechende Hinweise.
14–3		Datensiche-rung	Die Testung der externen Datensicherung auf Funktionsfähigkeit und Vollständigkeit muss in sinnvollen Abständen erfolgen.	Wie oft überprüfen Sie die externe Datensicherung?		Es wird empfohlen, ein regelmäßiges Testen der Datensicherung in (für Ihre Branche) sinnvollen Abständen – mindestens jedoch zweimal jährlich und nach maßgeblichen Veränderungen im Ablauf (z. B. neue Hardware, andere Datensicherungsroutinen, neue Speicherorte, Wechsel der zuständigen Person) durchzuführen. Im akuten Schadensfall muss die Wiederherstellung der Datensicherung funktionieren.
15–1	TOP	Patch- und Änderungs-manage-ment	Updates für IT-Systeme und Software müssen installiert werden.	Machen Sie Updates?	3/−3	Aktivieren Sie, wenn möglich, die von Herstellern bereitgestellten Update-Funktionen Ihrer IT-Arbeitsgeräte oder Software. Sollten Hersteller die automatisierte Update-Funktion nicht anbieten, müssen Sie eigenständig (manuell) den Update-Vorgang anstoßen. Aktuelle Updates schließen bekanntgewordene Schwachstellen und Sicherheitslücken, die Ihr Unternehmen gefährden könnten.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
15–2		Patch- und Änderungs-manage-ment	Updates müssen unverzüglich nach ihrer Veröffentlichung installiert werden.	Wie lange dauert es, bis Sie Updates installieren, sobald die Updates verfügbar sind?		Updates müssen unverzüglich installiert werden, sobald Hersteller sie anbieten. Fehlende Updates machen Ihr Unternehmen angreifbar und schädigen Ihren Betriebsablauf.
16		Patch- und Änderungs-manage-ment	Es muss festgelegt werden, wer die Updates installiert.	Wer installiert die Updates?	1/0	Wenn Sie sich selbst nicht darum kümmern können, bestimmen Sie eine verantwortliche Person in Ihrem Unternehmen, die sich um die Updates kümmert. Das kann auch ein externer IT-Dienstleister sein. Das Updaten ist ein ständiger Prozess, dem besondere Aufmerksamkeit geschenkt werden muss. Nur wenn es eine verantwortliche Person gibt, werden Updates immer zuverlässig und rechtzeitig durchgeführt.
17–1		Patch- und Änderungs-manage-ment	Hardware, relevante Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen identifiziert werden.	Wie prüfen Sie, ob Ihre verwendete Hard- oder Software herstellerseitig noch Sicherheitsupdates erhält?	1/0	Sie müssen prüfen, ob Ihre verwendete Hard- oder Software herstellerseitig noch Sicherheitsupdates erhält. Aktuelle Updates schließen bekanntgewordene Schwachstellen und Sicherheitslücken, die Ihr Unternehmen gefährden könnten.
17–2		Patch- und Änderungs-manage-ment	Hardware, relevante Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen ausgemustert werden.	Was machen Sie mit Ihrer Hard- oder Software, die herstellerseitig keine Sicherheitsupdates mehr erhält?		Hard- und Software, die herstellerseitig keine Sicherheitsupdates mehr erhalten, müssen ausgetauscht bzw. durch aktuelle Komponenten ersetzt werden. Veraltete Komponenten oder Softwareversionen stellen ein Sicherheitsrisiko dar.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
18		Schutz vor Schadpro-grammen	IT-Geräte wie beispielsweise Server, Arbeitsplatzrechner, Notebooks oder Smartphones müssen mit einem Schutz vor Schadsoftware ausgestattet sein.	Wie schützen Sie Ihre IT-Geräte vor Schadsoftware?	1/0	IT-Geräte wie beispielsweise Server, Arbeitsplatzrechner, Notebooks oder Smartphones müssen mit einem Schutz vor Schadsoftware ausgestattet sein. Ein Virenschutzprogramm schützt Sie vor Bedrohungen, die beispielsweise häufig durch E-Mail-Anhänge (auch Links in E-Mails, auf die geklickt wird) oder gefälschte Internetseiten Ihre IT-Systeme gefährden. Hiervor ist niemand geschützt, auch Kleinstunternehmen sind betroffen.
19–1		Schutz vor Schadpro-grammen	Software darf nur von vertrauenswürdigen Quellen bezogen werden.	Woran machen Sie fest, dass eine Quelle zum Herunterladen von Software vertrauenswürdig ist?	1/0	Software muss immer von vertrauenswürdigen Quellen bezogen bzw. heruntergeladen werden. Die Gefahr ist sehr groß, von unseriösen Internetseiten gefährliche Software herunterzuladen, die Ihre Betriebsfähigkeit dauerhaft und in hohem Maß schädigen kann. Auch sogenannte Spähsoftware kann durch das Herunterladen und Installieren von vermeintlich harmlosen Programmen in Ihr Unternehmensnetzwerk gelangen. Das Ausmaß kann sich über die Unternehmensgrenzen hinweg auf die IT-Netzwerke Ihrer Geschäftspartner oder Zulieferer ausweiten.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
19–2		Schutz vor Schadpro-grammen	Nur IT-verantwortliche Personen dürfen Software installieren.	Wer kann bei Ihnen Software installieren?		Software muss immer von IT-verantwortlichen Personen heruntergeladen und installiert werden. Die Gefahr ist sehr groß, von unseriösen Internetseiten gefährliche Software herunterzuladen, die Ihre Betriebsfähigkeit dauerhaft und in hohem Maß schädigen kann. Auch sogenannte Spähsoftware kann durch das Herunterladen und Installieren von vermeintlich harmlosen Programmen in Ihr Unternehmensnetzwerk gelangen. Das Ausmaß kann sich über die Unternehmensgrenzen hinweg auf die IT-Netzwerke Ihrer Geschäftspartner oder Zulieferer ausweiten.
20–1	TOP	Schutz vor Schadpro-grammen	Das Ausführen von aktiven Inhalten oder Makros (z. B. in Tabellenkalkulationspro-grammen) muss standardmäßig deaktiviert sein.	Sind Makros bei Ihnen standardmäßig aktiviert?	3/−3	Das Ausführen von Makros (häufig in Tabellenkalkulationsprogrammen enthalten) muss standardmäßig deaktiviert sein. Makros können Viren bzw. Schadsoftware enthalten, die beim Einschalten von Makros aktiviert werden und IT-Systeme angreifen. Dies kann Ihre Betriebsfähigkeit dauerhaft und in hohem Maß schädigen.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
20–2		Schutz vor Schadpro-grammen	Nur in begründeten Ausnahmefällen ist das Aktivieren von Makros erlaubt. Makros müssen dann von einer autorisierten Person aktiviert werden.	Wer kann in Ihrem Unternehmen Makros in begründeten Ausnahmefällen aktivieren?		Es muss festgelegt werden, unter welchen Voraussetzungen autorisierte Personen Makros (z. B. in Tabellenkalkulationsprogrammen) aktivieren dürfen. Makros können Viren bzw. Schadsoftware enthalten, die beim Einschalten von Makros aktiviert werden und IT-Systeme angreifen. Dies kann Ihre Betriebsfähigkeit dauerhaft und in hohem Maß schädigen.
21		IT-Systeme und Netzwerke	Eine Firewall muss installiert werden.	Setzen Sie eine Firewall ein, um Ihr Firmennetzwerk vor Angriffen zu schützen?	1/0	Es muss eine Firewall installiert sein. Eine Firewall schützt das Firmennetzwerk vor Angriffen (Cyberattacken).
22–1		IT-Systeme und Netzwerke	Um ein Netzwerk mit einer Firewall zu schützen, muss sie so konfiguriert sein, dass nur erforderliche Dienste zugelassen sind.	Ist Ihre Firewall individuell konfiguriert?	1/0	Um ein Netzwerk mit einer Firewall zu schützen, muss sie so konfiguriert sein, dass nur erforderliche Dienste zugelassen sind. Sollten Sie mit der Konfiguration von Firewalls nicht vertraut sein, sollte eine fachliche Unterstützung hinzugezogen werden. Durch individuelle Konfigurationen von Firewalls (bzw. Firewall-Regeln) können Fehler unterlaufen. Netzwerke können ungeschützt und damit für jeden zugänglich sein. Cyberattacken sind dann ohne Weiteres möglich und gefährden die Betriebsfähigkeit dauerhaft.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
22–2		IT-Systeme und Netzwerke	Es muss eine Person bestimmt werden, die über die Konfiguration der Firewall (Firewall-Regeln) entscheidet.	Wer entscheidet darüber, wie die Firewall konfiguriert wird?		Es muss eine Person bestimmt werden, die über die Konfiguration der Firewall (Firewall-Regeln) entscheidet. Nur ein Experte kann auch die für den Betrieb richtigen Einstellungen der Firewall vornehmen.
23		IT-Systeme und Netzwerke	Alle Computer, Laptops, Tablets oder Smartphones müssen passwortgeschützt sein.	Schützen Sie Computer, Laptops, Tablets und Smartphones vor unberechtigtem Zugriff mit einem Passwort?	1/0	Alle Computer, Laptops, Tablets oder Smartphones müssen passwortgeschützt sein. Durch den Passwortschutz können unberechtigte Dritte nicht zugreifen. Ihre IT-Systeme und Datenbestände werden durch die Vergabe eines Passworts geschützt und so Schaden von Ihrem Unternehmen abgewendet.
24–0		IT-Systeme und Netzwerke	Statusabfrage	Greifen Ihre Beschäftigten von unterwegs oder aus dem Homeoffice auf das Firmennetzwerk zu?		
24–1		IT-Systeme und Netzwerke	Beim mobilen Arbeiten oder im Homeoffice müssen Beschäftigte eine verschlüsselte Verbindung (VPN) nutzen, um auf das Firmennetzwerk zuzugreifen.	Nutzen Sie eine verschlüsselte Verbindung (VPN) zum externen Zugriff auf das Firmennetzwerk?	1/0	Der Zugriff auf das Firmennetzwerk von extern (mobil oder Homeoffice) muss verschlüsselt erfolgen. Dies kann durch eine VPN-Verbindung ermöglicht werden. Es besteht die Gefahr, dass bei nicht verschlüsselten Verbindungen Ihre Daten durch unbefugte Dritte manipuliert oder ausgespäht werden. Dies kann dazu führen, dass die Vertraulichkeit Ihrer Daten verloren geht.
25–0		IT-Systeme und Netzwerke	Statusabfrage	Gehen Sie über WLAN ins Internet?		

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
25–1		IT-Systeme und Netzwerke	Das WLAN muss nach aktuellen Standards verschlüsselt sein.	Wissen Sie, mit welcher Verschlüsselung Sie über WLAN ins Internet gehen? Wenn ja, erläutern Sie bitte.	1/0	Das WLAN muss mindestens mit WPA-2 verschlüsselt werden. Ältere Verschlüsselungsverfahren wie bspw. WPA-1 sind überholt und gelten als nicht sicher.
25–2		IT-Systeme und Netzwerke	Das WLAN muss mit einem komplexen Passwort (mindestens 20 Zeichen) geschützt werden.	Nach welchem Muster setzt sich Ihr Passwort für das WLAN zusammen?		Das WLAN muss mit einem mindestens 20 Zeichen langen, möglichst komplexen Passwort geschützt werden. Ohne langes, komplexes Passwort können auch unberechtigte Personen Zugriff auf den Computer erhalten.
25–3		IT-Systeme und Netzwerke	Statusabfrage	Gehen Gäste oder Beschäftigte mit privaten Geräten über WLAN ins Internet?		
25–4		IT-Systeme und Netzwerke	Sofern Gäste oder Mitarbeiter mit privater Hardware über WLAN ins Internet gehen, muss hierfür ein gesondertes, vom Firmennetzwerk getrenntes, verschlüsseltes und passwortgeschütztes WLAN eingerichtet sein.	Wie gehen die Gäste oder Beschäftigten mit privater Hardware bei Ihnen ins Internet?		Für Gäste muss ein getrenntes WLAN eingerichtet werden, das WPA-2 verschlüsselt sein muss. Wenn Ihre Beschäftigten Zugang für deren privaten Endgeräte (Tablets, Mobiltelefone) erhalten, muss der Zugang über das Gäste-WLAN oder ein vom Unternehmensnetzwerk getrenntes WLAN erfolgen. Durch die getrennten WLAN-Netzwerke wird das Unternehmensnetzwerk geschützt, da es Gästen nicht möglich ist, auf unternehmensinterne Daten oder IT-Systeme zuzugreifen und Schäden anzurichten.

Tabelle A.1 (*fortgesetzt*)

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
26–0		IT-Systeme und Netzwerke	Statusabfrage	Greift jemand mittels Fernwartung auf Server oder Computer in Ihrem Unternehmen zu?		
26–1		IT-Systeme und Netzwerke	Es muss geregelt werden, unter welchen Bedingungen und zu welchem Zeitpunkt eine Fernwartung der IT-Systeme des Unternehmens erfolgt.	Unter welchen Bedingungen erfolgt bei Ihnen die Fernwartung Ihrer IT-Systeme?	1/0	Es muss geregelt werden, unter welchen Bedingungen und zu welchem Zeitpunkt eine Fernwartung der IT-Systeme des Unternehmens erfolgt. Eine Regelung ist erforderlich, da eine für das Unternehmen unkontrollierte Fernwartung Möglichkeiten einer unerkannten Manipulation der IT-Systeme bietet.
26–2		IT-Systeme und Netzwerke	Fernwartungen müssen immer verschlüsselt sein.	Sind die Fernwartungen verschlüsselt?		Wenn Fernwartungen durchgeführt werden, müssen diese immer verschlüsselt sein. Der Zugriff kann via VPN erfolgen, es gibt aber auch Softwaretools, die die Fernwartungsverbindung verschlüsseln können. Es besteht die Gefahr, dass bei nicht verschlüsselten Verbindungen Ihre Daten durch unbefugte Dritte manipuliert oder ausgespäht werden. Dies kann dazu führen, dass die Vertraulichkeit Ihrer Daten verloren geht.
27		IT-Systeme und Netzwerke	Sämtliche IT-Komponenten müssen vor Elementarschäden geschützt werden.	Wie schützen Sie Ihre IT vor Elementarschäden?	1/0	Sämtliche IT-Komponenten müssen vor Elementarschäden wie Feuer, Wasser, ungünstigen Temperaturen (Hitze und Kälte), Überspannung usw. geschützt werden. Ungünstige Umgebungsbedingungen sowie unvorhersehbare Schadensereignisse beschädigen die IT.

Literaturhinweise

[1] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 2023. [Zugriff am 2023-03-10]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[2] Zentralverband des Deutschen Handwerks (ZDH): IT-Grundschutz-Profil für Handwerksbetriebe, 2019. [Zugriff am 2023-03-10]. Verfügbar unter: https://www.hwk-omv.de/downloads/technisches-it-grundschutz-profil-handwerksbetriebe-zdh-18,815.pdf

[3] VdS 10000:2018-12, *VdS-Richtlinien für die Informationsverarbeitung — Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU) — Anforderungen*

[4] VdS 10005:2021-07, *VdS-Richtlinien für die Informationsverarbeitung — Mindestanforderungen an die Informationssicherheit von Klein- und Kleinstunternehmen — Anforderungen*

[5] FAULBAUM, FRAUKE; PRÜFER, PETER; REXROTH, MARGIT: Was ist eine gute Frage? Die systematische Evaluation der Fragequalität. Lehrbuch, Wiesbaden: VS Verlag, 2009

[6] MAYRING, PHILIPP: Einführung in die qualitative Sozialforschung: eine Anleitung zu qualitativem Denken, Weinheim Basel: Beltz, 2016

[7] Bundesministerium für Wirtschaft und Klimaschutz: Förderdatenbank. [Zugriff am 2023-03-10]. https://www.foerderdatenbank.de/

[8] Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheit für KMU, 2023. [Zugriff am 2023-03-13]. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_KMU.html

[9] Bundesamt für Sicherheit in der Informationstechnik: Webseite für KMU. [Zugriff am 2023-03-13]. Verfügbar unter: https://www.bsi.bund.de/kmu

[10] Der Mittelstand, BVMW e.V.: Projektwebseite „mIT Standard sicher“. [Zugriff am 2023-03-13]. Verfügbar unter: https://mit-standard-sicher.de/