Handreichung für den Mittelstand

So werde ich sicher

Eine einfache Anleitung zur IT-Sicherheit für den Mittelstand

Bundesverband IT-Mittelstand e.V.

Vorwort

Der Mittelstand ist historisch Deutschlands Motor für Wachstum und Innovation; beides hängt heute mehr denn je mit der Digitalisierung zusammen.

Digitalisierung ist ein Thema, das alle Unternehmen, unabhängig von Branche und Größe, ständig fordert und gerade auch für kleinere Unternehmen enorme Chancen bietet. Die Grundlage dieser Digitalisierung sind die Daten, die jedes Unternehmen zum eigenen Betrieb benötigt oder von Kunden erlangt und verantwortlich gemäß DSGVO verwaltet. Der Schutz dieser Daten gestaltet sich jedoch zunehmend schwierig. Grund dafür ist vor allem, dass im deutschen Mittelstand in den seltensten Fällen ausreichend IT-Sicherheitswissen oder Fachkräfte vorhanden sind. Durch die enorm hohe Vernetzung, kombiniert mit einer ständig wachsenden Angriffsoberfläche von unzureichend geschützten Unternehmen, vervielfacht sich das Risiko von Angriffen durch alle Formen von Datendiebstahl durch professionelle kriminelle Organisationen, Wirtschaftsspionage und vielen anderen ungewollten Nutznießern der Daten. Schon im Jahr 2013 wurde mehr Geld durch Cyber Kriminalität in einem Jahr ergaunert als mit physischen Banküberfällen in allen vorangegangenen Jahren zusammen. Durch die hohe technische Komplexität des Themas ist es für Unternehmen ohne eigenes Wissen grundsätzlich empfehlenswert, verstärkt auf Cloud oder Managed Service Dienstleistungen, möglichst aus Deutschland, für die Datenhaltung zurückzugreifen. Sichere Clouddienstleistungen helfen zwar sehr, nichtsdestotrotz sollte jedes Unternehmen für sich selbst zudem die eigenen Systeme bestmöglich schützen.

Hierzu wurde diese Handreichung von der Fachgruppe IT-Sicherheit des Bundesverband IT-Mittelstand e.V. für den Mittelstand entwickelt.

Verfasser der Handreichungen:

Tobias Bümmerstede	Robert Drexler	Sebastian Feik
Lukas Hartmann	Tobias Hoffmann	Sascha Kessel
Philip Kobel	Christian Koch	Virginia Ostfeld
Christian Schottmüller	Stephan Schwichtenberg	Arved Graf von Stackelberg

Inhaltsverzeichnis

Handreichung für den Mittelstand

So werde ich sicher- eine einfache Anleitung für den Mittelstand

1. Warum Informationssicherheit?

Geschäftsgeheimnisse, Kundendaten, Abrechnungen; dies sind nur wenige Beispiele für Informationen, über die jedes Unternehmen verfügt. Unerheblich ist dabei in welcher Form, also ob diese Informationen ausgedruckt auf Schreibtischen oder in Ordnern zu finden, digital auf lokalen Endgeräten oder in einer Cloud abgespeichert sind.

Ob das Unternehmen dabei zwei oder tausende Mitarbeiter hat, spielt ebenfalls keine Rolle. Dokumente mit empfindlichen Informationen finden sich beinahe überall.

Gehen solche Informationen nun verloren oder werden sie sogar gestohlen, bedeutet dies in erster Linie nichts Gutes. In einigen Fällen kann ein solches Vorkommnis existenzielle Konsequenzen mit sich bringen. Der vielleicht einzige Unterschied zwischen dem 2-Personen Unternehmen und einem Großkonzern besteht darin, dass ein Großkonzern die unter Umständen anfallenden Bußgelder oder Vertragsstrafen schultern könnte; ein 2-Personen Unternehmen könnte in einem solchen Fall hingegen in seiner Existenz bedroht sein.

Es ist daher nicht von der Hand zu weisen, dass der Schutz von Daten und Informationen nicht nur Großkonzerne beschäftigen muss.

Mit dem Schutz von Informationen beschäftigt sich die Informationssicherheit. Sie beschäftigt sich keineswegs, wie es vielleicht der Name andeuten mag, nur mit Informatik oder Fragen aus dem IT-Bereich. Sie soll, grob gesprochen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherstellen:

Vertraulichkeit von Informationen bedeutet in diesem Zusammenhang, dass Maßnahmen vorhanden sind, die sicherstellen, dass nur berechtigte Personen bzw. Mitarbeiter auf diese zugreifen können.

Integrität bedeutet, dass die Informationen und Daten nicht verändert, gelöscht oder hinzugefügt werden können.

Verfügbarkeit stellt sicher, dass die Informationen und Daten in definierten Zeiträumen in einem festgelegten Umfang vorhanden, also verfügbar sind. Verfügbarkeit gewährleistet somit, dass z.B. die Funktionalität der Systeme, die Informationen und Daten speichern, gegeben ist.

Die Begriffe „Vertraulichkeit, Integrität und Verfügbarkeit“ werden vielen Lesern bereits aus der Beschäftigung mit der Datenschutzgrundverordnung bekannt vorkommen. Im Anforderungskatalog der technisch-organisatorischen Maßnahmen werden nämlich auch genau diese Schutzziele verfolgt.

Merke: Die Schnittstelle zwischen Datenschutz und Informationssicherheit sind die technisch-organisatorischen Maßnahmen.

Ein erfolgreicher Datenschutz kann insofern auch nur dann bestehen, wenn Maßnahmen zur Informationssicherheit getroffen wurden.

2. IT-Sicherheit in a Nutshell

Stellen Sie sich vor, es gäbe eine Technologie, die dafür sorgt, dass Ihre Unternehmensdaten geschützt sind, Ihre Mitarbeiter auch von zu Hause jederzeit arbeiten können, oder dass Sie zum Beispiel die Fernwartungen bei Ihren Kunden jederzeit so durchführen können, als ob Sie persönlich vor Ort wären. Diese Technologie gibt es schon seit Längerem, aber es ist nicht eine einzelne Technologie. Es ist ein Bündel an Maßnahmen, das immer wieder an Ihre Firma und Ihre speziellen Gegebenheiten angepasst werden muss. Diese Technologie heißt: IT-Sicherheit.

In den letzten Jahren ist vielen Akteuren auf dem Markt klar geworden, dass IT-Sicherheit als Disziplin lange vernachlässigt wurde. Warnungen und Bedenken in Bezug auf mangelnde IT-Sicherheit entstehen dabei bei allen Beteiligten! Sie entstehen auf der Anwenderseite zum einen durch immer neue Schwachstellen, die gefunden werden. Die Bedenken entstehen aber zum anderen auf der Anbieterseite dadurch, dass etablierte IT-Sicherheitsmaßnahmen nicht oder nur teilweise umgesetzt werden.

Bedingt durch die Covid19-Pandemie haben viele Unternehmen ad hoc Ihre Mitarbeiter in Heimarbeit geschickt. Der Begriff Heimarbeit ist bewusst gewählt: von einem Homeoffice sind wir in Deutschland weit entfernt – dafür fehlen wichtige Elemente und IT-Ausstattung. Ein Küchentisch kann nicht die professionelle Einrichtung eines Büros ersetzen, und im Sinne der IT-Sicherheit fehlen viele Maßnahmen, die Ihre Mitarbeiter bei Ihrer Arbeit schützen. Das haben Angreifer schnell begriffen! Aber aus der Pandemie können wir lernen. Es ist ein Paradebeispiel für geänderte Rahmenbedingungen, die eine Anpassung Ihres Unternehmens erzwingen. Risikobewertungen und IT-Sicherheitsmaßnahmen mussten von einem auf den anderen Tag überarbeitet werden. Es ist auch in der Bekämpfung der Pandemie ein Paradebeispiel: Jedes Unternehmen hat zum Teil anders auf die Pandemie reagiert, andere Maßnahmen umgesetzt. Und genau wie ein Virus „mutieren“ Cybersecurity Angriffe im Laufe der Zeit: das sieht man unter anderem an der zunehmenden Anzahl von Angriffen auf die Zulieferer in der Wertschöpfungskette.

Innerhalb der BITMi Fachgruppe IT-Sicherheit besteht ein Konsens darüber, dass richtig angewendete IT-Sicherheit einen Mehrwert darstellt, der auch an Kunden kommuniziert werden kann. Viel zu häufig wird darauf hingewiesen, dass bestimmte Maßnahmen umgesetzt werden „müssen“, ohne diesen Mehrwert zu verdeutlichen. Es gilt daher die Befürchtung, dass das Argument, „weil es dann sicherer ist“ sich selber entkräftet, unter anderem durch „IT-Sicherheit ist ein Prozess“ bzw. neu gefundene Schwachstellen. Verständlicherweise sinkt bei Geschäftsführern und IT-Verantwortlichen die Bereitschaft etwas zu tun, wenn zunächst nur Kosten entstehen bzw. gesehen werden oder der Eindruck entsteht, dass eigentlich alles unsicher ist. Obwohl viele der oben genannten Punkte richtig sind und sich auch widersprechen, gibt es heutzutage eigentlich keinen Grund mehr, IT-Sicherheit nicht umzusetzen.

Daher wollen wir Sie mit ein paar (zum Teil kontroversen) Fragestellungen zum Nachdenken anregen und Ihnen zeigen, was IT-Sicherheit alles für Sie als Geschäftsführer bedeuten sollte und wie einfach der Einstieg in das Thema sein kann.

Banken benutzen seit Jahrhunderten Tresore, um Wertgegenstände sicher zu verstauen und Zugriff auf diese Wertgegenstände zu limitieren.
Nennen Sie die 10 wichtigsten Gründe, warum Ihr Laptop auch als „Tresor“ zu klassifizieren ist!

Worin besteht denn eigentlich der „Wert“ Ihrer Firma? Nur falls er wirklich auf Ihren Laptop passt: Es gibt inzwischen verschiedene Festplattenverschlüsselungen, um Ihre Daten im Falle eines Verlustes vor neugierigen Blicken zu schützen. Sie werden diese Verschlüsselung in den meisten Fällen bei Ihrer täglichen Arbeit noch nicht einmal bemerken! Warum sollten Sie also darauf verzichten?

Der „Wert“ Ihrer Firma bestimmt sich aber im Wesentlichen durch ein bestimmtes Know-how, das in den seltensten Fällen nur noch mündlich übertragen wird. Damit wird es dann auch für Konkurrenten interessant, dieses Know-how abzugreifen. Im einfachsten Fall verlieren Sie nur Mitarbeiter, die Ihr Wissen mitnehmen. Im schlimmsten Fall aber nimmt dieser Mitarbeiter Ihre digitalen Unterlagen mit, was ungefähr das Gleiche ist, wie den eigenen Laptop zu verlieren.

Darüber hinaus versuchen aber Angreifer vor allem mit Hilfe von Phishing Ihre Daten zu erhalten, Zugriff auf Daten zu blockieren (Erpressungs-Trojaner) oder maschinelle oder IT-Prozesse zu blockieren. Je nach Art des Unternehmens führt das zu unangenehme Konsequenzen. Daher sollten Sie Dateien zum Beispiel niemals via E-Mail versenden, und auch nicht empfangen. E-Mail (und speziell deren Anhänge und Links) sind immer noch das Haupteinfallstor für Angriffe. Unbekannten Absendern sollten Sie (und Ihre Mitarbeiter) niemals vertrauen. Woran Sie unbekannte Absender erkennen? Sie und Ihre Geschäftspartner könnten bzw. sollten Mailsignaturen benutzen. Wahrscheinlich benutzen Sie bis jetzt keine Mail-Signaturen, aber es ist ein einfacher Weg, um das Vertrauen Ihrer Partner und Kunden zu steigern. Egal ob SMIME / PGP oder PEP: Eine Mail-Signatur ist ein verlässlicher Indikator, dass Sie einen Absender identifizieren und ihm vertrauen können!

Die Technologie hinter Mailsignaturen benutzt Digitale Identitäten, und die verlässliche Identifikation von Mitarbeitern oder Partner ist ein weiterer wichtiger Baustein der IT-Sicherheit. Sie und Ihre Mitarbeiter lassen sich mit Digitalen Identitäten eindeutig identifizieren. Die Basis dafür liefert z.B. der Einsatz von OpenIDConnect als Authentifizierungsprotokoll, idealerweise verbunden mit einer sog. 2-Faktor Authentifizierung. Damit lassen sich auch Zugriffsrechte realisieren und die Benutzung von Passwörtern (die entweder in einem Passwort-Manager oder auf den Müll landen sollten) wird minimiert. Softwarelösungen stehen sowohl als Open Source als auch als Lizenzmodell von Anbietern zur Verfügung. Zusätzliche Sicherheit erhalten Sie bei der Kombination von Hardware-Token mit Ihrer Authentifizierungslösung.

Auch für die Übertragung von Dateien gibt es inzwischen eine große Anzahl von Anbietern, die Ihnen helfen, Dateien nicht nur lokal, sondern auch mit entsprechenden Backups zu speichern. Gerade kleine Firmen sollten heutzutage lieber der Cloud vertrauen (trotz aller möglichen Bedenken). Lassen Sie Ihre Mitarbeiter lieber einen „Mehrwert“ schaffen, ohne dass jeder ein IT-Systemadministrator sein muss!

Ihr Auto wird alle zwei Jahre vom TÜV überprüft. Wann war Ihr IT-Getriebe das letzte Mal beim TÜV?

Apropos Systemadministration und Software: Interessanterweise akzeptieren wir bei Autos entsprechende regulatorische Maßnahmen (TÜV). Aber selbst in Ihrem Auto läuft Software, die überprüft werden muss!
Um einen Überblick über die eingesetzten Technologien und Anwendungen zu erhalten ist es empfehlenswert, ein Enterprise Architecture Framework oder die Benutzung eines ISMS einzuführen. Diese liefern Ihnen verlässliche Informationen darüber, welche Software bei Ihnen mit welcher Version benutzt wird. In einem ersten Schritt geht es noch nicht einmal darum, immer die neueste Version zu benutzen, sondern nur einen sauberen Dokumentationsstand zu erreichen. Ob Sie als Geschäftsführer dann auf die neueste Version wechseln, hängt von Ihrem persönlichen Risikoprofil ab und ist Ihrer eigenen Priorisierung überlassen. Wichtig ist: Es gelten für Software die gleichen Regeln wie für jeden anderen Gebrauchsgegenstand. Beachten und liefern Sie die Gebrauchs- und Pflegeanleitungen. Dazu gehören Security Patches, die es inzwischen zu jedem Betriebssystem gibt und auch zu jeder Software geben sollte. Denken Sie auch an die Entsorgung: Wenn Sie ein System nicht mehr benötigen, müssen die dazugehörigen Daten entsprechend übertragen, danach aber auch gelöscht werden.

Gleiches gilt für die Daten Ihrer Kunden. Die DSGVO hat klare Richtlinien erlassen, wie mit personenbezogenen (Kunden-) Daten umzugehen ist. Die eigentliche Errungenschaft daran ist, dass diese Regeln jetzt EU-weit gelten! In Deutschland galten auch schon vorher klare Richtlinien. Und unter uns gesagt: Es geht nicht darum, personenbezogene Daten nicht zu nutzen. Es geht darum, unsere Partner darüber zu informieren und Ihnen das Recht einzugestehen, „nein“ sagen zu dürfen, bzw. die Löschung Ihrer Daten einfordern zu können. Also eigentlich genau das, was einen respektvollen Umgang miteinander ausmacht. Falls Sie wissen wollen, an welcher Stelle in Ihrem Unternehmen personenbezogene Daten liegen: bitte fragen Sie Ihre Enterprise Architektur! Nutzen Sie diese Gelegenheit zum Aufräumen und zur Steigerung Ihrer Datenqualität. In vielen Fällen werden Daten in einem Unternehmen redundant, also eher drei- bis viermal so häufig auf Festplatten gespeichert, wie es nötig wäre.

Wussten Sie, dass ein fehlendes bzw. nicht dokumentiertes IT-Risiko und Security Management für Sie als Geschäftsführer einer GmbH ein "verwerfbares, pflichtwidriges Verhalten" ist? Warum sollte jemand anderes für IT-Risk & Security zuständig sein?

Und zum Schluss jetzt leider doch noch ein erhobener Zeigefinger! IT-Sicherheitsrisiken gehören zu den unternehmerischen Risiken, die jeder Geschäftsführer auf sich nimmt. Bei einem nicht ordnungsgemäßen Umgang mit Risiken kann ein Geschäftsführer also dafür haftbar gemacht werden. Leider müssen wir mitteilen: inklusive seines Privatvermögens. Es gibt also niemanden in einer Firma, der bessere Gründe hat mit IT-Sicherheit anzufangen und sie vorzuleben als die Geschäftsführung. Sie müssen nicht alles auf einmal anfangen, aber Sie müssen dokumentieren und belegen können, welche IT-Risiken Sie bewusst in Kauf genommen haben, z.B. wegen zu hoher Kosten. Und Sie müssen IT-Sicherheit nicht alleine umsetzen, sondern können sich (externe) Unterstützung holen. Um Ihnen diesen Anfang zu erleichtern, gibt es inzwischen je nach Unternehmensgröße unterschiedliche Standards, die Ihnen den Weg ebnen: Neben CISIS12 existiert die VdS 10000, ISO 27001 und das BSI IT-Grundschutzkompendium, geordnet nach steigender Komplexität. Und auch die EU/ENISA ist mit dem CyberSecurity Act auf dem Weg, entsprechende Standards und Maßnahmen zu definieren.

Wichtig für alle Standards: IT-Sicherheit beginnt bei Ihnen und Ihren Mitarbeitern und schützt Sie und Ihre Mitarbeiter vor Fehlern und Angriffen. IT-Sicherheit öffnet die Tür zu einer geschützten Privatsphäre, Datensouveränität bzw. Datensparsamkeit und Intellectual Property Schutz. Es gibt dabei nichts zu „verlieren“. Auch hier greift die Analogie der Pandemie: Jeder muss für sich entscheiden, ob er sich impfen lassen möchte oder nicht. Für Impfungen und die IT-Sicherheit gilt: Je mehr Unternehmen und Personen IT-Sicherheit ernst nehmen, desto besser ist unser aller Schutz. Am besten fangen Sie bereits heute an: Über IT-Sicherheit zu reden schafft Bewusstsein (Awareness), und hilft Ihnen und Ihrem Team, Gefahren abzuwehren: ganz ohne großen Aufwand oder Kosten, nur durch Nachdenken und Reden. Nicht nur Ihre Angestellten werden es Ihnen danken!

In den folgenden Kapiteln werden wir auf einige der oben genannten Themen vertiefend eingehen. Bei der Vielzahl an Lösungen ist es leider so gut wie unmöglich, alles gleichzeitig in voller Tiefe aufzuarbeiten. Brauchen wir aber auch nicht: Vieles ist ja bereits beschrieben und dokumentiert, in diesem Falle möchte die Fachgruppe IT-Sicherheit des BITMi nur gerne als Leuchtturm im Meer der IT-Sicherheit agieren.

3. Riskmanagement bei IT-Sicherheit und Cyber-Gefahren

„Uns passiert schon nichts“ – „Wir sind safe“ – „Unsere Daten und Informationen interessieren doch niemanden“ – so oder so ähnlich lauten leider immer noch zu oft die Antworten auf die Frage, wer im Unternehmen bei den Themen IT- und Cybersicherheit den Hut auf hat. Dies gilt auch für Unternehmen der IT-Branche. Ein hohes Niveau an **Informations- und IT-Sicherheit ist aber immer Chefsache** und sollte höchste Priorität haben. Denn: Leitungsorgane und Geschäftsführer haften bei Vermögensschäden in Folge eines kapitalen Data-Breach oder eines Cyber-Vorfalls voll mit ihrem privaten Vermögen – und dies verschuldensunabhängig.

Das IT-Sicherheitsmanagement beziehungsweise das IT-Risikomanagement sollte dabei immer ganzheitlich betrachtet werden und alle vier wichtigen Bereiche der IT- und Cybersicherheit berücksichtigen:

Schaubild: Ganzheitliches IT-Sicherheitsmanagement

Alle vier Aspekte sollten bei einer 360 Grad-Betrachtung von IT-Sicherheit analysiert werden, um dann gezielt Maßnahmen für den Schutz der IT und des Unternehmens zu entwickeln. Insbesondere der vierte Bereich des Risikotransfers wird oftmals übersehen oder vernachlässigt – ist aber für das erfolgreiche Management von IT-Sicherheit essentiell. Da die besten Maßnahmen aus den Bereichen “Technik“, „Organisation“ und „Mitarbeiter*innen-Awareness“ keine Garantie für absolute Sicherheit bieten, lassen sich die „Restrisiken“ ab- beziehungsweise versichern. Für Unternehmen jedweder Branche und Größe

kommen dabei für den Transfer von Informationssicherheits- und Cybersicherheitsrisiken verschiedene Versicherungslösungen ins Spiel.

Deckungslücken klassischer Versicherungen
Viele Unternehmen sind sich sicher, dass sie über ihre bestehenden Versicherungspolicen (zum Beispiel Sachversicherung, Rechtsschutz- oder auch Betriebshaftpflichtversicherung) ausreichend gegen Risiken versichert sind, die die Sicherheit ihrer Daten und den Schutz der Privatsphäre betreffen. Genau dies ist leider nicht der Fall. Herkömmliche Versicherungslösungen können sich angesichts der Bedrohungen, denen Unternehmen heute ausgesetzt sind, als völlig unzureichend erweisen. Gerade kleinere oder mittelständische Unternehmen können im Fall von Cyberangriffen oder Datenverlusten (unverhofft) in eine existenzbedrohende Lage geraten. Für den Schutz mittelständischer Unternehmen – insbesondere aus der IT- und Softwarebranche sind spezielle Versicherungslösungen notwendig.

IT- und Cybersicherheitsrisiken absichern
Klassische Versicherungspolicen bieten oft keinen ausreichenden Schutz vor Cyberrisiken. Cyberversicherungen hingegen sind eigens dafür konzipiert, Lücken zu schließen und Deckung für Risiken bereit zu stellen, die schwer einzuschätzen sind. IT-Unternehmen gelten bei ihren Kunden und Geschäftspartnern generell als „Branchenführer“ oder Experten für IT- und Cybersicherheit sowie Datenschutz. Aus diesem Grund haben sie ein besonders hohes Risiko, bei Cybervorfällen Reputationsschäden zu erleiden. Da böswillige und kriminelle Cyberaktivitäten immer ausgeklügelter werden, müssen sich mittelständische Firmen und Unternehmen so gut wappnen wie nie zuvor. Man braucht dabei nicht das direkte Ziel eines Cyber-Angriffs sein, um hiervon betroffen zu werden. Cyber-Angriffe können sich auch über Ihre Lieferanten oder externe Partner ausbreiten und erhebliche Folgen haben, auch wenn Ihr Unternehmen selbst nicht das Angriffsziel ist.

Eine Cyberversicherung übernimmt den Risikotransfer und deckt Restrisiken ab. Sie ist die Feuerversicherung des 21. Jahrhunderts. Generell ist zu beachten, dass Ihr Unternehmen durch entsprechende IT-Sicherheitsstruktur selbst für einen angemessenen Grundschutz sorgen muss. Diesen kann eine Versicherung nicht ersetzen.

Es gilt immer der Grundsatz: *Eine Versicherung ersetzt kein rechtskonformes Handeln!*

Bei den meisten Cyberversicherungen wird (versicherungstechnisch) zwischen zwei Arten von Cybervorfällen unterschieden:

Informationssicherheitsverletzungen, die eine Gefährdung beziehungsweise Bedrohung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten darstellen, wie zum Beispiel

- Gesetzliche Datenschutzbestimmungen
- Vertragliche Datenschutzbestimmungen

- Geheimhaltungspflichten / Vertraulichkeitsvereinbarungen
- Kreditkartenverarbeitungsvereinbarungen

Netzwerksicherheitsverletzungen durch unbefugten Eingriff in die IT-Infrastruktur. Zum Beispiel:

- Übermittlung von Schadprogrammen
- Denial of Service durch Dritte
- Beschädigung, Zerstörung oder Diebstahl von fremden / eigenen elektronisch aufbewahrten Daten
- Unberechtigte Aneignung von Zugangscodes

Die ideale Cyberversicherung ist dabei immer individuell an die Bedürfnisse Ihres Unternehmens angepasst – und sollte mindestens folgende „Bausteine“ enthalten:

Baustein Assistance:

- Professionelle Unterstützung durch IT-Security-Forensik-Experten zur Abwehr, Aufspürung, Dokumentierung und zur Behebung eines Cybervorfalls
- Juristische Unterstützung zur Wahrung der DSGVO-Formalien (Meldepflicht, Benachrichtigung Dritter usw.)

Baustein Eigenschäden:

- Deckung für Ertragsausfälle in Folge eines Cyber-Vorfalls
- Deckung für die Kosten der Wiederherstellung von Daten, Programmen usw.
- Reputationsschutz-Maßnahmen „Erhalt der Marke“

Baustein Haftpflicht:

Dieser Baustein umfasst grundsätzlich eine Deckung für Ansprüche Dritter (Kunden, Partner, Lieferanten), welche aufgrund eines Cyber-Vorfalls Schaden erlitten haben. Dies kann unter anderem die Verletzung von Rechten (zum Beispiel Urheber-, Wettbewerbs- oder Persönlichkeitsrecht) beinhalten. State-of-the-art Cyberversicherungen bieten zudem ein aktives Krisenmanagement im Schadenfall und professionellen Support sowohl im Schaden- als auch im Verdachtsfall. Oftmals sind zudem auch „Folgeschäden“ wie Reputations- und Imageschäden mit abgesichert.

Fazit

IT-Sicherheitsmanagement ist ein Managementthema und ganzheitlich auch unter Einschluss des Bereiches „Risikotransfer“ zu betrachten. Dabei gilt immer der Grundsatz: Eine Versicherung ersetzt kein rechtskonformes Handeln! Eine Cyberversicherung übernimmt aber Restrisiken, sorgt für aktives Krisenmanagement und lässt die Geschäftsführung ruhiger schlafen. Auch kleinere und mittlere IT-Unternehmen können sich damit ein Stück weit Sicherheit einkaufen – und minimieren das Risiko im Fall der Fälle in eine existenzbedrohende Lage zu geraten.

4. Wege in die Informationssicherheit

Fällt der Begriff Informationssicherheit, so öffnet sich das Einfallstor für Assoziationen: „Zertifizierung nach 27001“ „Grundschutzkompendium“ „ISMS“ „…“

Zugegeben: die Reichweite und der Umfang von Informationssicherheit/ Datensicherheit und IT-Security scheint uferlos. Die Komplexität der einzelnen Frameworks lässt die Motivation des Selbststudiums auch leider nicht erwachen.

Den Schutz Ihrer Informationen in diesem Zuge zu vernachlässigen ist aber unter keinen Umständen zu empfehlen. Wir, die BITMi Fachgruppe „IT-Sicherheit“, möchten Ihnen daher einen „kleinen Fahrplan“ in die Informationssicherheit an die Hand geben. Wie aus der gewählten Terminologie „kleiner Fahrplan“ bereits zu entnehmen ist, kann Vollständigkeit natürlich nicht gewährleistet werden.

4.1.Festlegung von Werten

Zunächst sollten Sie sich fragen, welche Werte Ihr Unternehmen besitzt. Werte können dabei Know-how, Geschäftsgeheimnisse aber auch z.B. Informationen von Kunden sein. Wichtig dabei zu beachten: Informationen sind nicht an ein Medium gebunden. Folglich können Werte/Informationen in Papierform, digitaler Form aber auch in Form geistigen Eigentums vorliegen.

In einem ersten Schritt sollten Sie daher eine „Wert-Inventar-Liste“ anfertigen. Wichtig ist, wie bei jeder Inventur, dabei auf Vollständigkeit zu achten.

4.2.Risiken identifizieren

In einem nächsten Schritt sollten Sie Ihre Inventar-Liste auf Risiken untersuchen. Bei Betrachtung jedes Wertes bzw. jeder Information müssen Sie sich fragen, welchen Risiken sie ausgesetzt ist. Beispielsweise sind nur lokal auf einem Laptop gespeicherte Daten einem hohen Verlustrisiko, z.B. bei Diebstahl, ausgesetzt. Geschäftsgeheimnisse können durch nicht sensibilisierte Mitarbeiter mündlich ungewollt verbreitet werden.

4.3.Klassifizieren

Halten wir nochmal fest: Vor Ihnen liegt nun eine Liste mit allen Werten und Informationen, über die Ihr Unternehmen verfügt. Ergänzend hierzu haben Sie herausgearbeitet, welche Risiken für die einzelnen Werte bestehen. Auf Grundlage dieser Aufarbeitung können Sie nun Ihre Werte und Informationen klassifizieren.

Gängig ist hierbei eine Klassifizierung nach „streng vertraulich“, „vertraulich“, „intern“ und „öffentlich“. Welche Stufe einzutragen ist, richtet sich nach dem Schaden, den der Verlust des Wertes bedeuten würde. So bedeutet z.B. der Verlust der Word-Datei mit einem Beitrag für einen Newsletter, der am nächsten Tag

veröffentlicht werden sollte, ein eher geringes bis kein Risiko für das Unternehmen, während eine Liste mit allen ihren Kunden samt Adressen, Geburtstagsdaten und vielleicht auch Bankdaten bei Verlust einen sehr hohen Schaden bedeuten kann.

4.4.Maßnahmen zur Risikominimierung entwickeln

Anhand Ihrer bisherigen Ausarbeitungen haben Sie einen Überblick darüber gewonnen, welche Informationen und Werte Sie besitzen, welche Risiken bestehen und welchen Rang ihre Informationen haben.

In einem nächsten Schritt gilt es nun, Maßnahmen zu implementieren, die Ihre Unternehmenswerte schützen. Selbstredend sind die Informationen, die Sie als „streng vertraulich“ gekennzeichnet haben, stärker zu schützen als Informationen, die mit „öffentlich“ gekennzeichnet wurden. Eine Maßnahme gegen Diebstahl von Daten, die lokal auf Ihrem Laptop gespeichert sind, kann z.B. sein, Ihre digitalen Daten auf einer Cloud zu speichern. Gegen die mündliche Verbreitung von Geschäftsgeheimnissen kann sich geschützt werden, indem Mitarbeiter geschult und auf einen gewissenhaften Umgang hingewiesen werden.

4.5.Kontrolle und Pflege

Sofern Sie die ersten Maßnahmen definiert haben, fängt der wohl schwierigste Teil an: Die Maßnahmen müssen verfolgt und eingehalten werden. Dazu empfiehlt es sich, Ihr ausgearbeitetes Konzept in regelmäßigen Abständen zu kontrollieren. Regelmäßig bedeutet hierbei mindestens einmal im Jahr. Gleichzeitig sollten Sie darauf bedacht sein, dass Sie Ihre Konzepte pflegen; also sobald Sie sich mit neuen Werten oder Risiken konfrontiert sehen, sollten Sie sich darum bemühen, Maßnahmen zur Sicherung und zum Schutz festzulegen.

4.6.Digitale Souveränität

Selbst betriebene Software-Lösungen, Plattformen und Webseiten nutzen oft Dienste Dritter. Diese Zusatzdienste sollten mit Bedacht eingesetzt werden. Auch eigenständige Produkte von Dritten werden für Zusatzfunktionen genutzt, wie etwa für Videokonferenzen.

Im Sinne einer Datensparsamkeit sollten Alternativen für Produkte insbesondere von Anbietern außerhalb Europas geprüft werden. Nicht selten ist der Nutzen eines Dienstes so gering, dass er ersatzlos gestrichen werden kann.

Nicht nur aus Datenschutzgründen, sondern auch aus Sicherheitsgründen sollten unnötige und vor allem unsichere Produkte nicht eingesetzt werden. Ein Produkt ist insbesondere unsicher, wenn die rechtlichen Rahmenbedingungen oder die Anfälligkeit für Angriffe von außen unklar sind.

Beispiele für kritische Produkte und dazu passende Lösungen, die datenschutzfreundlicher, rechtlich besser beherrschbar oder sicherer sind:

- Zoom für Videokonferenzen → ecosero oder edudip (beides deutsche Anbieter)
- Google Analytics → Matomo in lokalem Betrieb
- Google Mail (Gmail) → E-Mail Angebote zahlreicher deutscher Anbieter

Oft werden Produkte von Dritten empfohlen, beispielsweise von Dienstleistern wie Internet-Agenturen. Fragen Sie die Empfehlungsgeber nach den rechtlichen Bedingungen für den Einsatz der Produkte. Auch die Frage nach einer Haftungsübernahme zeigt schnell, ob der Empfehlungsgeber ausreichend Kenntnisse zu dem in Frage stehenden Produkt besitzt.

Nur wer seine IT-Infrastruktur genau kennt, kann digital souverän agieren. Setzen Sie auf Lösungen von Anbietern, die sich an deutsche und europäische Vorgaben halten und im Zweifel verantwortlich gemacht werden können. Das reduziert nicht nur Ihr Haftungsrisiko, sondern stärkt unseren heimischen Markt.

5. Nachweis der technischen und organisatorischen Maßnahmen

Die Datenschutzgrundverordnung fordert u.a. in den Grundsätzen des Art. 5 Abs. 2 in der sogenannten Rechenschaftspflicht, dass die Einhaltung des Datenschutzes nachgewiesen werden muss. Konkretisiert wird das in Art. 32 Abs. 1 lit d), denn es muss „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ umgesetzt werden. Demnach reicht es also beispielsweise nicht mehr aus, eine Firewall zu betreiben, um das eigene Netzwerk vor Angriffen aus dem Internet zu schützen, sondern es muss auch regelmäßig (mit angemessenem Aufwand) überprüft werden, ob diese Firewall wirksam ist. Konkret sollten also IT-Schwachstellenanalysen und in Einzelfällen auch Penetrationstests durchgeführt werden, welche die angeforderte Evaluierung ermöglicht und im besten Fall Hinweise für die Verbesserung der Sicherheitsmaßnahmen gibt. Regelmäßig sollten diese Prüfungen ebenfalls erfolgen, damit man die Weiterentwicklung der möglichen Sicherheitslücken ebenfalls stets berücksichtigt (Sicherheitsupdates, neue Malware, etc.). Hierzu gibt es manuelle, halbmanuelle, aber auch automatisierte Möglichkeiten der Durchführung.

5.1.Beispiele für in Deutschland verhängte Bußgelder nach der DSGVO

Beispiele für in Deutschland verhängte Bußgelder nach der DSGVO
Die Auflistung enthält neben den Verstößen, soweit bekannt, auch die Höhe des Bußgeldes und das jeweils betroffene Unternehmen/Bundesland:

Ort	Unternehmen	Bußgeld	Beschreibung
Hamburg	Hamburger Verkehrsverbunds (HVV)	20.000 EUR	Verspätete Meldung eines Datenschutzvorfalls und unterbliebene Information der Betroffenen
Baden-Württemberg	Lebensmittelhandwerks-unternehmen	100.000 EUR	Unzureichender Schutz personenbezogener Daten in einem Bewerberportal

Baden-Württemberg	Knuddels GmbH & Co. KG	20.000 EUR	Unverschlüsseltes Speichern von Passwörtern bei einem sozialen Netzwerk, so dass diese (ca. 330.000 Datensätze) nach einem Hackerangriff im Internet veröffentlicht wurden
Baden-Württemberg	AOK Baden-Württemberg	1.240.000 EUR	Verwendung der Daten von 500 Gewinnspielteilnehmern für Werbezwecke
Deutschland (Bundesdatenschutz-beauftragter)	1&1 Telecom GmbH	9.550.000 EUR	Unberechtigte konnten durch mangelnde Authentifizierung bei der Kundenbetreuung andere Kundendaten erhalten
Berlin	Deutsche Wohnen SE	14.500.000 EUR	Speicherung von Daten ehemaliger Mieter in einem Archiv ohne Rechtsgrundlage und ohne Löschmöglichkeit
Sachsen-Anhalt	Privatperson	2.629 EUR	Versendung mehrerer E-Mails, in denen die (persönlichen) E-Mail-Adressen aller Empfänger sichtbar waren
Deutschland (Bundesdatenschutz-beauftragter)	Rapidata GmbH	10.000 EUR	Fehlende Benennung eines Datenschutz-beauftragten

6. Übersicht der gängigen Informationssicherheitsstandards

Möchte man sich eingehender mit Informationssicherheit beschäftigen oder Vertragspartnern einen definierten Grad an Informationssicherheit vorlegen, ist die Auseinandersetzung mit den Informationssicherheitsstandards unumgänglich. Auf dem Markt existieren derweil mehrere Standards mit unterschiedlichen Anforderungen, Umfang aber auch Kostenfaktoren. Um herauszufinden, welcher Standard der richtige ist, ist viel Recherchearbeit und Zeit nötig. Wir möchten Ihnen daher an dieser Stelle eine Übersicht an die Hand geben, mit der Sie einerseits einen Überblick über die gängigen Standards bekommen sollen, zum anderen aber auch eine erste Grundlage zur Entscheidungsfindung erhalten, welcher Standard für Sie geeignet ist.

Übersicht der gängigen Informationssicherheitsstandards

Standard	Geltungsbereich	Branche	Vorteile	Nachteile	Aufwand
ISO 27001 ff.	Unternehmen bestimmen individuell den Geltungsbereich; internationale Ausrichtung	Alle	> Hoher Nutzen > Gutes Kosten-/Nutzen-verhältnis > Internationaler Bekanntheits-grad > Gestaltbar	> Komplex und abstrakt > Ggf. nur positive Seiten des Unternehmens einbezogen	30-300 PT Beratungs-leistung; interner Aufwand Faktor 1,5-2
BSI Grund-schutz	Siehe ISO27001, deutschland-weite Ausrichtung	Alle, verpflichtend bei Behörden, halb-öffentlichen Institutionen	> Über Grundschutz-kompendium hoher Nutzen > Sehr detailliert > Klare Führung > Hohe Anerkennung	> Wenig flexibel > Sehr hoher Dokumenta-tionsaufwand > Kein risiko-orientierter Ansatz > Dokumenta-tionen teilw. Nicht immer auf dem akt. Stand der Technik	30-300 PT Beratungs-leistung; interner Aufwand Faktor 2-4

VdS 10000	Office- und Produktions-IT Ausrichtung im DACH-Bereich	Alle	> Pragmatischer Ansatz > Schneller Einstieg > Breite Anerkennung im Versicherungs-umfeld	> Keine weitreichende Bekanntheit	70% Ergebnis der ISO 27001 bei 30% des Aufwands
CISIS12	Scope ist variabel, Office- und Produktions-IT bis zur kompletten Organisation, Ausrichtung im DACH-Bereich, insbesondere Bayern	Alle, insbesondere Kommunen in Bayern	> Schneller, einfacher und kosten-günstiger Einstieg in die Informations-sicherheit > 12 aufbauende Verfahrens-schritte	> Keine Akkreditierung für Zertifizierungs-stelle	Extern: 5-40 PT Berater-aufwand Intern: abhängig vom gewählten Scope und Ist-Zustand
Risiko-manage-ment ISO 31000	Allg. anwendbarer generischer Scope-Standard, internationale Ausrichtung	Alle	> Internationale Anwendbar-keit > Risiken effektiv bewältigen > Erfüllung rechtl.- und behördl. Bestimmungen	> Administrativer Aufwand durch die unternehmens-weite Erhebung und Aktualisierung der Risikodaten	Variiert nach Unter-nehmens-größe und Geschäfts-modell

WP-Standards IDW-PS 951	Dienstleistungs-bezogenes internes Kontrollsystem; bei internationaler Ausrichtung sollte die Prüfung nach ISAE 3401 erfolgen	Kommt zur Anwendung bei Dienstleistern (Outsourcing) deren Auftraggeber vom WP geprüft werden	> Nachweis-fähigkeit ggü. Dritten bezogen auf die ordnungs-gemäße Erbringung der Dienstleistung	> Jährliche Kosten für die WP-Prüfung und interne Aufwände für die Pflege des IKS	20-40 PT Berateraufwand + interner Aufwand
ISO 22301 Business Continuity	Um Unternehmen festzulegen	Alle	> Nachweis-fähigkeit ggü. Dritten > Verbesserte Reaktions-fähigkeit im Notfall	> Jährliche Kosten für die Zertifizierung und interne Aufwände	Abhängig vom Ist-Zustand des Unter-nehmens
TISAX	Betrifft den gesamten Automotive-Bereich, zunehmend auch Luft- und Raumfahrt-technik	Automotive, Luft- und Raumfahrt-technik	> Anerkannter Standard in der europäischen Automobil-industrie > Basiert auf ISO 27001 > Prüfung nur alle drei Jahre	> Branchen-standard der europäischen Automobil-industrie; Anerkennung außerhalb der Automobil-industrie nur bedingt gegeben, Forderung zunehmend auch in der Luft und Raumfahrt	30 - 300 PT Beratungs-leistung zur Herstellung der Zertifizierungs fähigkeit; interner Aufwand Faktor 2 - 2,5

BSI C5 (Cloud Com-puting)	Cloud-Produkt und Organisation, nationale Ausrichtung	Cloud-Anbieter	> Zunehmend anerkannter und nachgefragter Standard in Deutschland, der ein hohes Sicherheits-niveau für Cloud-Anbieter bescheinigt. Sicherheits-niveau liegt über ISO 27001-Anforderun-gen	> WP-Prüfung und interne Aufwände für die Pflege des ISMS sowie Vor-/Nachbereitung und Begleitung der Wirtschafts-prüfung. Insbesondere Vorbereitungs-zeit für initiale Prüfung ist sehr umfangreich.	31 - 300 PT Beratungs-leistung zur Herstellung der Zertifizierungs fähigkeit; interner Aufwand Faktor 2 - 2,5

7. Übersicht über Förderprogramme

Digitalisierungsthemen und die damit verbundenen Themen der IT-Sicherheit und des Datenschutzes sind für den Geschäftsalltag von kleinen und mittleren Unternehmen (KMU) aktuell große Herausforderungen und sind auch zunehmend mit Kosten verbunden. Um Unternehmen bei diesen Herausforderungen und Investitionen aktiv zu unterstützen, sind von verschiedenen Institutionen auf Landes- und Bundesebene Förderprogramme aufgelegt worden. Diese Mittel sollen die Implementierung von Prozessen und die Kosten für externe Beratungsleistungen finanzieren.

Die BITMi Fachgruppe IT-Sicherheit hat sich daher die Aufgabe gestellt, Ihnen eine Übersicht zu den bereits aufgelegten Programmen darzustellen.

7.1.Digital-Programme im Überblick

Digital-Programme im Überblick			
Ort	Name	Zuwendung	Besonderheit
bundesweit	Go Digital	Zuschuss 16.500 Euro	Nur autorisierte Berater
	Go Inno	Zuschuss 27.500 Euro	Nur autorisierte Berater
	KfW Digital	Kredit bis 25 Mio. Euro	
	KfW Mezzanine	Kredit bis 5 Mio. Euro	Bis zu 60% Nachrangkapital
Baden- Württemberg	Hightech Digital	Zuschuss 20.000 Euro	
	Digitalisierungsprämie	Kredit bis 100.000 Euro	Tilgungszuschuss bis 10 %
Bayern	Digitalbonus	Zuschuss 50.000 Euro	
Berlin	Berlin Mittelstand 4.0	Kredit 2 bis 6 Mio. Euro	60% Haftungsfreistellung

Brandenburg	BIG Digital	Zuschuss 550.000 Euro	
Bremen	Bremen – Digitalisierung	Zuschuss 5.000 Euro	
Hamburg	Hamburg-Kredit Innovation	Kredit bis 1,5 Mio. Euro	
Hessen	Digital-Zuschuss	Zuschuss 10.000 Euro	
	Innovationskredit	Kredit 100.000 bis 7,5 Mio. Euro	
Mecklenburg-Vorpommern	DigiTrans	Zuschuss 10.0000 Euro bis 50.000 Euro (Einzelfälle)	
Niedersachsen	Innovationsförderung	Zuschuss 100.000 Euro	
Nordrhein-Westfalen	Mittelstand Innovativ	Zuschuss 25.000 Euro	
	NRW.BANK.Digitali-sierung und Innovation	Kredit ab 25.000 Euro, ab 0%	
Rheinland-Pfalz	BITT – Technologieberatung	Zuschuss 6.000 Euro	
	Innovationskredit RLP	Kredit, 25.0000 bis 2 Mio. Euro	
Saarland	Digital Starter	Zuschuss 10.000 Euro	
Sachsen	E-Business	Zuschuss 50.000 Euro	
Sachsen-Anhalt	Digital Innovation	Zuschuss 70.000 Euro	

	Digital Creativity	Zuschuss 130.000 Euro	
Schleswig Holstein	Aktuell kein Förderprogramm Digital		
Thüringen	Digitalbonus Thüringen	Zuschuss 15.000 Euro	

7.2.Bundesweite Digital-Programme

7.2.1.Go digital (BMWi)

> Zuschuss 16.500 Euro, 50% Förderquote
> Im bundesweiten Förderprogramm "go digital" des BMWi erhalten KMU mit bis zu 100 Mitarbeitern und max. 20 Mio. Euro Umsatz einen Zuschuss über max. 16.500 Euro. Mit dem Programm werden Beratungsleistungen für die digitale Transformation in den Bereichen IT-Sicherheit, Digitale Markterschließung und digitalisierte Geschäftsprozesse bezuschusst. Dabei werden maximal 30 Beratertage zu einem Höchstsatz von 1.100 Euro mit 50% gefördert. Eine Besonderheit von „go digital" ist, dass die Beratung nur von einem autorisierten Berater vorgenommen werden darf. Zudem sind zwei Beratertage zum Thema "IT-Sicherheit" verpflichtend
> Im Zuge der Corona-Krise wurde das Programm wie folgt erweitert: Im Modul „Digitale Prozesse" kann ab sofort auch die Einrichtung von Homeoffice-Plätzen in beantragt werden. Hierzu zählen
  - der Aufbau sowie das Einrichten der zugehörigen Hardware,
  - Software, die dabei zum Einsatz kommt und über die gängigen Standards hinausgeht.

Von der Förderung weiterhin ausgeschlossen sind hingegen reine Investitionsmaßnahmen in Hard- und Standardsoftware.

> Mehr zu diesem Förderprogramm auf den Seiten des BMWi
> https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/go-digital/go-digital.html

7.2.2.Go-Inno (BMWi)

> Zuschuss 27.500 Euro, 50% Förderquote
> Mit dem Fördermittel „go-Inno" fördert das BMWI die Innovationsberatung von KMU (<100 Mitarbeiter, < 20 Mio. Umsatz). Die Rahmenbedingungen des Programms sind analog zu denen von „go digital". Eine Kombination beider Programme ist nicht möglich
> Wie bei „go digital" dürfen Leistungen nur von autorisierten Beratungsunternehmen erbracht werden. Gefördert werden Beratungsleistungen über drei Leistungsstufen:

  - Potenzialanalyse (max. 10 MT)
  - Realisierungskonzept (max. 25 MT)
  - Projektmanagement (max. 15 MT)
- Für einen Beratertag sind bis zu 1.100 Euro zu 50 Prozent förderfähig
- Weitere Informationen zu „go-Inno“ auf der Webseite des BMWi

7.2.3. ERP-Digitalisierungs- und Innovationskredit (KfW)

- Kredit bis 25 Mio. Euro, Zins ab 1%
- Zielgruppe für den Förderkredit sind gewerbliche Unternehmen (<500 Mio. Euro Umsatz) und Freiberufler, die mindestens 2 Jahre am Markt sind. Das Programm ist sehr breit gefasst und so kann mit der zinsgünstigen Finanzierung eine Reihe digitaler Vorhaben umgesetzt werden, die die digitale Transformation der Unternehmen fördern und beschleunigen. Das umfasst Maßnahmen zur strategischen Ausrichtung der Unternehmen über digitale Plattformen bis hin zu organisatorischen Maßnahmen, um Unternehmen agiler zu machen.
- Weitere Informationen zum Digitalkredit der KfW auf den Seiten der KfW.

7.2.4. ERP-Mezzanine für Innovationen (KfW)

- Kredit, bis 5 Mio. Euro, Zins ab 1%, Nachrangkapital
- Im Gegensatz zum Digitalisierungs- und Innovationskredit fördert das Programm „ERP-Mezzanine für Innovationen“ marktnahe Forschung und Entwicklungen, die sich vom Stand der Technik in der EU abheben und Vorhaben, die für das beantragende Unternehmen neu sind. Gefördert werden Investitionen und Betriebsmittel, dabei übernimmt die KfW bis zu 60 % Risikoübernahme durch Nachrangkapital.
- Die Neuartigkeit des Vorhabens muss im Rahmen der Antragstellung von einem von der KfW zertifizierten Gutachter attestiert werden. Zielgruppe sind Unternehmen (<500 Mio. Euro Umsatz) und Freiberufler, die mindestens 2 Jahre am Markt sind
- Weitere Informationen zum Programm „ERP-Mezzanine“ für Innovationen auf den Seiten der KfW

7.3.Landesweite Digital-Programme

7.3.1. Baden-Württemberg

- Baden-Württemberg bietet mit dem Innovationsgutschein Hightech Digital einen Zuschuss über 20.000 Euro, zudem mit dem der Digitalisierungsprämie einen Kredit bis zu 100.000 Euro mit Tilgungszuschuss
- **Innovationsgutschein Hightech Digital**
- Zuschuss 20.000 Euro, 50% Fördersatz

- KMU erhalten einen Zuschuss von max. 20.000 Euro bei einem Fördersatz von 50%. Mit dem Hightech Digital Innovationsgutschein werden umsetzungsorientierte FuE Tätigkeiten im Zusammenhang mit der Entwicklung und Realisierung von digitalen Produkten und Dienstleistungen gefördert. Dazu zählen die Entwicklung und Realisierung neuer digitaler Lösungen über den technischen Stand der Branche hinaus. Für bereits bekannte Lösungen (z.B. die Einführung von ERP oder CRM Systemen) verweist das Ministerium auf die Digitalisierungsprämie.
- Weitere Information zum Innovationsgutschein auf der Webseite des Ministeriums.
- Digitalisierungsprämie
- Kredit bis 100.000 Euro, Tilgungszuschuss bis 10%
- Unternehmen bis 100 Mitarbeiter erhalten einen Kredit bis 100.000 Euro mit Tilgungszuschuss, um damit ihre Digitalisierung voranzutreiben. Gefördert werden u.a. folgende Maßnahmen:
  - Digitalisierung von Produktion und Verfahren (zum Beispiel 3D-Druck, mobile Betriebsgeräte zur Produktionssteuerung, e-commerce, e-procurement)
  - Digitalisierung von Produkten und Dienstleistungen (digitale Plattformen, Fernwartung, Anwendung digitaler Standards)
  - Umsetzung von Strategien und Konzepten zur Digitalisierung (IKT-Sicherheit, digitale Vertriebskanäle, Cloud)
- Der Mindestbetrag beträgt 10.000 Euro, der Höchstbetrag für einen Kredit 100.000 Euro. Dabei erhalten Unternehmen einen Tilgungszuschuss in Abhängigkeit der Darlehenshöhe. Bei dem Bruttodarlehensbetrag von 10.000 bis einschließlich 50.000 Euro ist der Tilgungszuschuss 5.000 Euro, bei dem Bruttodarlehensbetrag von 50.000 bis einschließlich 100.000 Euro ist der Tilgungszuschuss 10% des Bruttodarlehensbetrags
- Weitere Information zur Digitalisierungsprämie in Baden-Württemberg auf der Webseite des Ministeriums.

7.3.2. Bayern

- In Bayern erhalten KMU mit dem Digitalbonus einen Zuschuss bis 50.000 Euro und können zusätzlich einen zinsverbilligten Digitalkredit von bis zu 2 Mio. Euro beantragen.
- Ziel des Digitalbonus und des Digitalkredits ist es, KMU zu unterstützen, ihre Produkte, Dienstleistungen und Prozesse digital zu transformieren und ihre IT-Sicherheit zu verbessern.

Digitalbonus

- Standard: Zuschuss 10.000 Euro, 30-50% Förderquote
- Plus: Zuschuss 50.000 Euro, 30-50% Förderquote
- Den Digitalbonus gibt es in zwei Varianten. Im Digitalbonus Standard erhalten KMU in Bayern bis zu 10.000 Euro, in der Variante Plus bekommen Unternehmen bis zu 50.000 Euro Zuschuss. Die Förderquote von 30% oder 50% orientiert sich an der Unternehmensgröße (siehe EU Definition). Gemäß dieser Einordnung gelten für den Digitalbonus folgende Förderquoten:

- 50% (< 50 Mitarbeiter)
- 30% (< 250 Mitarbeiter)

- Förderfähig sind Ausgaben für die Verbesserung von bestehenden Produkten, Prozessen und Dienstleistungen. Dabei ist entscheidend, dass erstmals digitale Systeme eingesetzt werden oder der Digitalisierungsgrad auf den neuesten Stand erhöht wird. Zudem sind Maßnahmen zur Verbesserung der IT-Sicherheit zuwendungsfähig. Förderfähige Ausgaben sind Leistungen externer Anbieter einschließlich der notwendigen Hard- und Software. Im Vergleich zum Digitalbonus Standard, zielt der Digitalbonus Plus auf Maßnahmen mit besonderem Innovationsgehalt ab.
- Ausgeschlossen sind dagegen herkömmliche Maßnahmen im Online-Marketing (z.B. Webseiten oder Maßnahmen im Online-Marketing), der Erwerb von herkömmlicher Software (z.B. Bürosoftware, Betriebssysteme) oder Hardware (wie PCs, Telefone etc.). Digitalbonus Standard und Plus können nicht miteinander kombiniert werden

7.3.3. Berlin

- Berlin bietet mit Berlin Mittelstand 4.0 einen Kredit 2 bis 6 Mio. Euro mit einer Laufzeit von 3-10 Jahren
- Die Investitionsbank Berlin (IBB) unterstützt Startups, KMU und den gehobenen Mittelstand (< 3.000 Mitarbeiter) mit zinsgünstigen Krediten für Digitalisierung und die Entwicklung sowie Implementierung innovativer IT-Lösungen. Dabei haftet die IBB für 60 Prozent des Kreditrisikos, was die Antragstellung und Kreditgewährung über die Hausbank vereinfacht. Die Darlehen haben eine Laufzeit zwischen 3 und 10 Jahren und Konditionen ab 1%
- Weitere Information zu Berlin Mittelstand 4.0 auf der Webseite der IBB.

7.3.4.Brandenburg

BIG Digital

- Zuschuss 550.000 Euro, 50 % Förderquote
- Mit dem Innovationsgutschein (BIG) unterstützt das Land Brandenburg KMU bei der Konzeption und Umsetzung von Maßnahmen im Bereich Digitalisierung. Dabei können Unternehmen maximal 50.000 Euro für das Modul Beratung und Schulung (6 Monate) und maximal 500.000 Euro für das Modul Implementierung (36 Monate) erhalten.
- Weitere Information zum BIG Digital auf der Webseite des Ministeriums.

7.3.5. Bremen

Bremen – Digitalisierung

- Zuschuss 5.000 Euro, 50% Förderquote
- Mit dem Förderprogramm zu Digitalisierung und Arbeit 4.0 erhalten KMU in Bremen einen Zuschuss von 5.000 Euro für eine Beratung. Dabei können KMU auf eine Vorauswahl von Beratern zurückgreifen.

7.3.6. Hamburg

Hamburg-Kredit Innovation

> Kredit bis 1,5 Mio. Euro
> In Hamburg bietet die Investitions- und Förderbank (IFB) ansässigen KMU und Startups zinsgünstige Darlehen ab 25.000 bis 1,5 Mio. Euro. Schwerpunkt der Förderung sind Digitalisierung, Produktentwicklung, Markteinführung und Wachstum. Die Darlehen haben eine tilgungsfreie Zeit, eine Laufzeit von bis zu 10 Jahren und eine Haftungsfreistellung von 70% für die Hausbank. Im Gegenzug erwartet die IFB Eigenmittel in Höhe von 7,5%.
> Weitere Informationen zum Digital- und Innovationskredit Hamburg auf der Webseite der IFB Hamburg.

7.3.7. Hessen

Digital-Zuschuss

> Zuschuss 10.000 Euro, 50%
> Das Land Hessen fördert kleine und mittlere Unternehmen sowie freie Berufe bei ihrer digitalen Transformation. Dabei wird erwartet, dass die Beratung einen Digitalisierungsfortschritt in den Bereichen Produktion und Verfahren, IT-Sicherheit, Produkte und Dienstleistungen oder Strategie und Organisation des Unternehmens erzielt. Eine Förderung erfolgt ab Ausgaben in Höhe von 4.000 Euro. Maximal werden 10.000 Euro bei einem Zuschuss von 50% gefördert. Dabei gilt es schnell zu sein, denn die Mittel sind nur während des angekündigten Förderaufrufs verfügbar und schnell vergriffen.
> Weitere Informationen zum Digital-Zuschuss und nächsten Förderaufruf auf der Webseite der Förderbank Hessen.

Innovationskredit

> Kredit 100.000 Euro bis 7,5 Mio. Euro
> Mit dem Innovationskredit unterstützt die Wirtschafts- und Infrastrukturbank Hessen (WIBank) Gründer, Freiberufler und KMU (<500 Mitarbeiter). Die Mittel können unter anderem auch für Digitalisierung eingesetzt werden. Voraussetzung für die Inanspruchnahme des zinsgünstigen Darlehens ist die Erfüllung eines der Innovationskriterien (im Merkblatt unter Punkt eins “Antragsberechtigte”). Die Laufzeit beträgt zwischen drei und zehn Jahren.
> Weitere Informationen zum Innovationskredit Hessen und seinen Konditionen auf der Webseite der WIBank.

7.3.8. Mecklenburg-Vorpommern

DigiTrans – Digitalisierung in der Wirtschaft

> Zuschuss 10.000 Euro, Förderquote 35-50%
> Das Landesförderinstitut Mecklenburg-Vorpommern unterstützt Startups und KMU bei der Entwicklung neuer digitaler Lösungen und Geschäftsmodelle sowie der Gestaltung der digitalen Transformation mit einer Förderung bis zu 10.000 Euro. Investitionen in herkömmliche Hard- und Software sind von der Förderung ausgeschlossen. Dabei erhalten Unternehmen bis 50 Mitarbeiter eine Förderung von 50% (auf 20.000 Euro förderfähige Ausgaben), Unternehmen mit bis zu 250 Mitarbeitern (vgl. EU-Einordnung KMU) 35%. In Ausnahmen können Unternehmen auch eine Förderung bis zu 50.000 Euro erhalten, diese setzt jedoch ein umfangreicheres Konzept im Rahmen der Beantragung voraus.
> Weitere Informationen zu DigiTrans auf der Webseite des Landesförderinstitut M-V oder direkt im Merkblatt.

7.3.9. Niedersachsen

Innovationsförderung für KMU und Handwerk (NBank)

> Zuschuss 8.000 bis 100.000 Euro, 35-50% Förderquote
> Die Investitions- und Förderbank des Landes Niedersachsen bietet kleinen und mittleren Unternehmen (KMU) der gewerblichen Wirtschaft einen Zuschuss bis zu 35 % bzw. maximal 100.000 Euro als nicht rückzahlbaren Zuschuss. Damit werden innovative Services und Produkte, Prozess- und Organisationsinnovationen und die Ausgaben für gewerbliche Schutzrechte unterstützt. Förderfähig sind u.a. Personalausgaben, Ausgaben für externe Berater und anteilige Investitionsausgaben.
> Weitere Informationen zu diesem Förderprogramm Digitalisierung auf der Webseite der NBank.

7.3.10. Nordrhein-Westfalen

Mittelstand Innovativ

> Zuschuss 25.000 Euro, 40-70% Förderquote
> Mit seinen Gutscheinen für Digitalisierung und Innovation bietet das Land Nordrhein-Westfalen ein Instrument, um KMU bei der Entwicklung neuer Produkte zu unterstützen. Darüber hinaus wird die Digitalisierung von bestehenden Prozessen, Produkten und Dienstleistungen gefördert.
> Seit Juli 2019 erhalten kleine Unternehmen (<50 Mitarbeiter, 10 Mio. Euro Umsatz) eine Förderung von 70%, mittlere Unternehmen dagegen 40%. Das Antragsformular, ein ausführlicher Kriterienkatalog und weitere Informationen zum Digital-Gutschein NRW befinden sich auf der Webseite des Projektträgers.

NRW BANK Digitalisierung und Innovation

> Kredit ab 25.000 Euro, ab 0% Zinsen
> Mit dem Förderprogramm werden Maßnahmen zur Digitalisierung durch die Bereitstellung zinsgünstiger Darlehen unterstützt. Dabei sind eine Vielzahl von Vorhaben im Bereich Digitalisierung und Innovation förderfähig. Antragsberechtigt sind KMU mit bis zu 500 Mio. Euro Umsatz.
> Mehr Informationen zu diesem Förderprogramm Digitalisierung auf der Webseite der NRW.Bank.

7.3.11. Rheinland-Pfalz

BITT – Technologieberatung

> Zuschuss 6.000 Euro, 50% Förderquote
> Die Investitions- und Strukturbank Rheinland-Pfalz bietet kleinen und mittleren Unternehmen (<250 Mitarbeiter, siehe EU-Definition) einen Zuschuss von 50% zu Beratungsleistungen. Die Förderung ist eingeschränkt auf max. 15 Beratertage und 400 Euro/Tag. Im Vordergrund stehen technologieorientierte Beratungen und Beratungen zum Aufbau eines Qualitäts- und Innovationsmanagement-Systems.
> Weitere Informationen auf der Webseite der Investitions- und Strukturbank Rheinland-Pfalz.

Innovationskredit RLP

> Kredit 25.0000 bis 2 Mio. Euro
> Unternehmen in Rheinland-Pfalz mit bis zu 500 Mitarbeitern, die ein besonderes Innovationsvorhaben verfolgen, können einen Kredit von 25.0000 bis 2 Mio. Euro über 3-10 Jahre mit einer tilgungsfreien Anlaufzeit beantragen. Dabei muss das antragstellende Unternehmen mindestens eines der Innovationskriterien des Europäische Fonds für strategische Investitionen (EFSI) erfüllen.
> Weitere Informationen zum Kredit finden Sie auf der Webseite der Investitions- und Strukturbank Rheinland-Pfalz, die Innovationskriterien können Sie in dem Merkblatt zum Innovationskredit RLP nachlesen.

7.3.12. Saarland

DigitalStarter

> Zuschuss 10.000 Euro, 20-35% Förderquote
> Mit dem Förderprogramm DigitalStarter erhalten KMU im Saarland bis zu 10.000 Euro als Zuschuss zu ihrem Digitalisierungsprojekt. Förderfähig sind Ausgaben für die Digitalisierung von Produkten, Prozessen und Dienstleistungen oder die Entwicklung neuer digitaler Plattformen. Zudem werden Investitionen in die Verbesserung der IT-Sicherheit bezuschusst.
> Gefördert werden Projekte mit Ausgaben in Höhe von mindestens 5.000 Euro. Der Fördersatz beträgt 20% bei mittleren Unternehmen und bis zu 35% bei kleinen Unternehmen jedoch jeweils höchstens 10.000 Euro.

7.3.13. Sachsen

E-Business

> Zuschuss 50.000 Euro, 50% Förderquote
> Mit dem Programm E-Business unterstützt das Land Sachsen KMU bei der Umsetzung digitaler Vorhaben. Zuschüsse werden beispielsweise für die Planung, Konzipierung und Vorbereitung von Projekten, den Kauf von Software und dafür notwendiger Hardware oder die Einführung von entwickelten Lösungen gewährt. Dabei ist die Unterstützung durch externe Berater für die Planung, Konzipierung und Vorbereitung auf fünf Beratertage beschränkt mit einer maximalen Förderung von 450 Euro pro Tag.
> Weitere Informationen zum Förderprogramm "E-Business" befinden sich auf der Seite der Sächsischen Aufbaubank (SAB) oder im Flyer E-Business.

7.3.14. Sachsen-Anhalt

Digital Innovation

> Zuschuss 70.000 Euro, 70% Förderquote
> Mit dem Förderprogramm Digital Innovation unterstützt das Land Sachsen-Anhalt KMU bei der Konzeption und Umsetzung von Digitalisierungsprojekten. Das betrifft die Entwicklung von digitalen Produkten, Prozessen und Geschäftsmodellen, die Umsetzung digitaler Marketing- und Vertriebsstrategien und Ausgaben für die IT-Sicherheit.
> Weitere Informationen zu Digital Innovation des Landes Sachsen-Anhalt auf den Seiten der Investitionsbank Sachsen-Anhalt.

Digital Creativity

> Zuschuss 130.000 Euro, bis 90% Förderquote
> Mit dem Förderprogramm Digital Creativity fördert das Land Sachsen-Anhalt die Entwicklung und den Einsatz innovativer digitaler Medien in KMU. Dazu zählen u.a. audiovisuelle Medienproduktionen, Spiele, Apps und virtuelle Realitäten.
> Weitere Informationen zu Digital Creativity des Landes Sachsen-Anhalt auf den Seiten der Investitionsbank Sachsen-Anhalt

7.3.15. Thüringen

Digitalbonus Thüringen

> Zuschuss 15.000 Euro, 50% Förderquote
> Mit dem Digitalbonus unterstützt die Thüringer Aufbaubank die Digitalisierung von kleinen und mittelständischen Unternehmen. Schwerpunkte dabei sind die Digitalisierung von Betriebsprozessen,

Produkten, Dienstleistungen und Investitionen in die IT-Sicherheit. Die Förderung beträgt bis zu 50% der zuwendungsfähigen Ausgaben, höchstens jedoch 15.000 Euro

> Weitere Informationen zum Digitalbonus Thüringen auf der Webseite der Thüringer Aufbaubank.

Innovationsgutschein

> Ein weiteres Förderinstrument der Thüringer Aufbaubank ist der Innovationsgutschein. Damit werden Maßnahmen im Kontext Digitalisierung nur gefördert, wenn sie einen Bezug zu den folgenden Spezialisierungsfeldern haben:
  > Industrielle Produktion und Systeme
  > Nachhaltige und intelligente Mobilität und Logistik
  > Gesundes Leben und Gesundheitswirtschaft
  > Nachhaltige Energie und Ressourcenverwendung
> Weitere allgemeine Informationen und zur Förderhöhe auf der Webseite der Thüringer Aufbaubank.