Handbuch Unternehmens-Resilienz

Für kleine und mittelgroße Unternehmen

Erasmus+

CASSANDRA
KEEP YOUR BUSINESS GOING

Kopierschutz

Dieses Handbuch und die dazugehörigen Vorlagen wurden von Tournis Consulting LP in Zusammenarbeit mit allen Projektpartnern erstellt. Zusammen sind diese Dokumente ein Teilergebnis des CASSANDRA-Projekts, das mit Unterstützung der Europäischen Kommission finanziert wurde.

Sowohl das Handbuch, als auch die Vorlagen können heruntergeladen und kostenlos von jedem Unternehmen genutzt werden, das seine Resilienz verbessern möchte. Die Richtlinien des Programms Erasmus+ sind einzuhalten.

Das “Handbuch Unternehmens-Resilienz” ist Gegenstand der Lizenz:

Bildnachweis:
Bilder, die aus den Datenbaken von www.canva.com genutzt wurden:
Attention icon, ©icons8
Yellow bulb vector, ©Canva Layouts
Round Warning Sign, ©feelisgood
Wavy Flag, ©Canva
Whatsapp, ©Icon54
Green Book Vector, ©Canva
Green Logo Vektor, ©Canva

Haftungsausschluss

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung tragen allein die Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Die Verfasser dieses Handbuchs und der dazugehörigen Vorlagen sind in keinster Weise für die Nutzung oder die Umsetzung der darin enthaltenen Ideen, Methoden oder Ratschläge haftbar.

Gender

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

EIN ERGEBNIS DES **CASSANDRA** PROJEKTES

Erstellt durch TOURNIS CONSULTING LP

in Kooperation mit

CPMS, emcra GmbH, IBWF e. V., LVH und T-SOFT

MÄRZ 2017

„Wir müssen die Hoffnung aufgeben,
dass das Meer jemals ruhen wird.
Wir müssen lernen, trotz starkem Wind zu segeln.“

Aristoteles Onassis

CASSANDRA Projektpartner

emcra GmbH
Hohenzollerndamm 152,
14199 Berlin
Deutschland
Tel.: +49 30 31801330
E-Mail: info@emcra.eu

Tournis Consulting LP
Noti Botsari 9-11,
11741 Athen
Griechenland
Tel.: +30 2102526321
E-Mail: info@tournis-consulting.com

CPMS
Volonaki 14,
1045 Nikosia
Zypern
Tel.: +357 70003232
E-Mail: info@cpms.org.cy

T-SOFT
Novodvorska 1010/14,
14.201 Prag 4
Tschechien
Tel. +42 0261710561
E-Mail: info@tsoft.cz

IBWF e. V.
Potsdamer Str. 7,
10785 Berlin
Deutschland
Tel.: +49 171 2819194
E-Mail: info@ibwf.org

LVH
Mitterweg 7,
39.100 Bozen
Italien
Tel.: +39 0471323200
E-Mail: info@lvh.it

1. Inhaltsverzeichnis

Symbole

Definition

Informationen

Achtung!

Weiterführende Informationen

2. Das CASSANDRA Projekt

Dieses Handbuch ist ein Ergebnis des CASSANDRA-Projektes. CASSANDRA ist ein Akronym für „**C**ontinuity **a**nd **S**ecurity for **S**MEs **A**ctive in **N**eutralizing **D**angers and **R**isks affecting their **A**ctivities“. Ziel des zweijährigen Projektes (2015-2017), das durch das EU-Programm „Erasmus+“ gefördert wurde, war es, die Widerstandsfähigkeit von kleinen und mittleren Unternehmen (KMU) gegenüber Risiken oder Gefahren zu verbessern.

2.1. KMU

Das CASSANDRA-Handbuch wurde für KMU entwickelt, insbesondere für kleine Unternehmen, die unternehmensnahe Dienstleistungen anbieten. Hierzu zählen u. a. Rechtsanwälte, Steuerberater, Werbe- und Marketingagenturen, Personalberater, Grafik-Design und Druckdienstleistungen sowie Sicherheitsfirmen.

Der Gebrauch des Begriffes KMU in diesem Leitfaden bezieht sich auf dieses Marktsegment bzw. auf verwandte Dienstleistungsbereiche.

3. Einführung

Dieses Handbuch wurde speziell für die Bedürfnisse von KMU entwickelt. Es unterstützt diese beim Aufbau ihres Risikomanagements (einschließlich der Themengebiete „Informationssicherheit“ und „Sicherstellung des Geschäftsbetriebes“). Mit Hilfe dieses Handbuchs können KMU ihre Widerstands- bzw. Anpassungsfähigkeit individuell und bedarfsgerecht verbessern.

Die CASSANDRA-Methode hilft Inhabern bzw. Managern von KMU auf einfache, unkomplizierte und praktische Weise, sich für das Thema Risikomanagement zu sensibilisieren und die erforderlichen Kenntnisse zu erwerben. Sie verstehen, wie Sie die Anpassungs- bzw. Widerstandsfähigkeit Ihres Unternehmens nachhaltig und bedarfsgerecht verbessern können. Mit den zur Verfügung gestellten Materialien können Sie ein wirksames Risikomanagement aufbauen und unternehmensintern etablieren. Dabei berücksichtigen Sie die wichtigen Themenbereiche „Informationssicherheit“ und „Sicherstellung des Geschäftsbetriebes“. Auf dieser Basis werden fundierte und alltagstaugliche Entscheidungen möglich, die Ihr Unternehmen zukunftsfähig machen.

4. KMU und Risiken

4.1. Was ist Risiko?

Risiko ist ein Begriff, der im täglichen Leben regelmäßig benutzt wird. Er wird gewöhnlich als Kombination aus Eintrittswahrscheinlichkeit und Ausmaß bzw. Auswirkung beim tatsächlichen Eintreten eines Ereignisses verwendet. In diesem Handbuch definieren wir:

> Risiko ist aktuell eine Eventualität, die in Zukunft zur Realität werden kann. Wenn das geschieht, dann kann dies positive oder negative Auswirkungen bzw. Konsequenzen für Ihr Unternehmen haben.[1] [2]

Der Begriff Risiko kann unterschiedliche Bedeutungen haben. Es gibt z. B.:

- *Wahrscheinlichkeits-Risiko* („Die Wahrscheinlichkeit, dass unser Team heute das Spiel gewinnt, beträgt 30 %.“) (Zusatzfrage: Wie sicher sind Sie sich bei dieser Wahrscheinlichkeit?)
- *Unsicherheits-Risiko* bezüglich des Eintreffens und der Auswirkungen eines Ereignisses („Sollte es zu einem Erbeben kommen, könnte das Gebäude beschädigt werden.“)
- *Unsicherheits-Risiko* bezüglich des Ausmaßes, das ein eintretendes Ereignis haben kann („Durch den Streik könnten wir zwischen 20.000 € und 40.000 € verlieren.“)
- *Abweichungs*-Risiko gegenüber einer Planung („Wir haben mit Ausgaben in Höhe von 10.000 € gerechnet, der Rechnungsbetrag stieg jedoch auf 25.000 €.“)

Risiken können das Erreichen Ihrer Ziele im Privatleben und im Geschäftsbetrieb drastisch beeinflussen. Die Konsequenzen sind im besten Fall unerheblich, jedoch kann es auch passieren, dass sie die Existenz Ihres Geschäftsbetriebes bedrohen. Sie können Risiken in unterschiedliche Kategorien einteilen, z. B. finanzielle, operative, rufschädigende Risiken etc.

[1] ISO Leitfaden 73:2009, Risikomanagement, Definition 1.1.
[2] Principles of Risk Management, CRMI, The National Alliance for Insurance Education and Research, 2014.

4.2. „Und es ward Risiko“

Risiken sind überall – wenn Sie etwas tun, dann gehen Sie Risiken[3] ein. Und auch nichts zu tun, bringt vielfältige Risiken mit sich.

Das Leben birgt unzählige Risiken. Wir umgeben uns z. B. jeden Tag selbst beim Essen mit Risiken; wenn wir uns ungesund ernähren oder zu wenig bzw. zu viel essen, können wir krank werden. Bei der Arbeit lauern Risiken wie Arbeitsunfälle. Sport kann zu verbesserter Gesundheit führen, jedoch auch die Gesundheit gefährden, z. B. wenn man sich beim Trainieren verletzt. Keinen Sport zu treiben reduziert zwar das Verletzungsrisiko, erhöht aber ggf. das Risiko eines Herzinfarktes.

Jegliche Aktivität im Geschäftsbetrieb führt zu Risiken. Unzählige Investoren finanzieren jährlich neue KMU, während gleichzeitig eine Vielzahl schließen muss. Trotzdem investieren Inhaber vieler Unternehmen weiterhin als gäbe es keinerlei Risiken, ganz nach dem Motto: „Mir kann so etwas nicht passieren“.

Ein Risiko kann entweder auf Ihre eigenen Handlungen und Entscheidungen zurückgeführt werden (z. B. Preisänderungen, unzureichende Wartung Ihrer IT-Systeme etc.) oder aufgrund von externen Herausforderungen entstehen (Wettbewerber, finanzielle Unsicherheiten in Ihrem Land, Überschwemmungen etc.).

4.3. Positive und negative Risiken

Risiken können gleichzeitig positiv und negativ sein. Einen Geschäftsbetrieb zu starten, bringt die vielfältigsten Chancen und Risiken mit sich.

[3] Vgl. B. L. Cohen and I. S. Lee, “A Catalog of Risks”, in: Health Physics, 36 (6), S. 707-722, 1979.

POSITIVE RISIKEN (Chancen)	NEGATIVE RISIKEN (Verluste)
In diesem Fall rechnen Sie mit guten Erträgen, wenn Sie geschickt investieren und Ihr Unternehmen gut managen. Wenn z. B. ein direkter Wettbewerber sein Unternehmen aufgibt, dann stellt das ebenfalls ein positives Risiko bzw. eine Chance für Sie dar, allerdings nur wenn Sie in der Lage sind, neue, zusätzliche Kunden gut zu bedienen und Ihr Unternehmen sich an die geänderte Situation schnell anpassen kann. Sie müssen Ihre neuen Kunden ohne Qualitäts-einbußen versorgen können. Sollten Sie nicht ausreichend auf die neue Situation vorbereitet sein, dann besteht die Gefahr, dass Sie nicht nur den neuen Kunden nicht gerecht werden, sondern darüber hinaus auch Ihre bestehenden Kunden verlieren.	Negative Risiken wie Computer-ausfälle, Hackerangriffe, mensch-liches Versagen, überraschend starke Wettbewerber oder auch Naturkatastrophen wie Über-schwemmungen können bis zur Insolvenz führen, wenn Sie sich nicht proaktiv damit auseinandersetzen.

Jeder Geschäftsbetrieb muss in der Lage sein, mit seinen Risiken angemessen umzugehen, um ein möglichst gutes Gesamtergebnis für das Unternehmen zu erreichen. Das gilt sowohl für positive Risiken, weil Sie damit Ihren Erfolg maximieren können, als auch für negative Risiken. Hier kommt es darauf an, die schlimmsten Konsequenzen zu vermeiden. Auch neue Risiken oder potenzielle Umweltprobleme müssen immer wieder identifiziert und gemanagt werden.

Kurzgesagt müssen Unternehmen die Sicherstellung ihres Geschäftsbetriebes nachhaltig gewährleisten und ihre Widerstands- bzw. Anpassungsfähigkeit permanent verbessern.

4.4. Risiken unterscheiden nicht zwischen großen und kleinen Unternehmen

Kein KMU-Inhaber will aufgrund eines Feuers oder Erdbebens aufgeben müssen. Auch andere Risiken wie der Weggang eines wichtigen Mitarbeiters, der Verlust wichtiger Daten oder das Durchsickern von vertraulichen Informationen können bis zur Schließung führen, wenn das Unternehmen nicht darauf vorbereitet ist.
Unglücklicherweise hört man von den meisten Geschäftsinhabern eher folgende Aussagen, wenn es um das Thema Risiken geht:

- Also mir kann das nicht passieren!
- Bedrohung? Ich kann keine Bedrohung erkennen!
- Unser Unternehmen befasst sich nicht mit vertraulichen Informationen.
- Wir sind ein kleines Unternehmen. Risiken und Bedrohungen betreffen nur große Unternehmen!
- Warum sollte jemand mein Unternehmen gefährden wollen?
- Ich bin allem gewachsen!

Unternehmen sind Risiken und Bedrohungen ausgesetzt, egal wie groß sie sind, wo ihr Standort ist oder wie gut das Geschäft aktuell läuft. Durch diese Risiken können der Standort und die Mitarbeiter gefährdet, Kunden vertrieben, Umsätze beeinträchtigt, der Ruf zerstört und wie leider so oft in der Vergangenheit das Ende einer Unternehmung verursacht werden.

Sollte es zu Naturkatastrophen (Überschwemmungen, Erdbeben, Lawinen etc.) oder großen Bränden kommen, sind alle umliegenden Unternehmen, egal wie groß, betroffen. Auch ein Streik im Transportsektor kann zu lokalen oder sogar internationalen Blockaden von Gütern, Material und Menschen führen und dadurch sowohl KMU, als auch Großunternehmen betreffen.

Es kümmert die möglichen Risiken und Bedrohungen überhaupt nicht, ob Ihr Unternehmen groß oder klein ist. KMU können genauso wie Großunternehmen von Computerviren, Hackerangriffen, Verlust von Personal in Schlüsselpositionen, Bränden, Erdbeben oder jeder anderen Form von Ausfällen und Katastrophen betroffen sein. Fakt ist, dass KMU sogar noch viel gefährdeter sind, da es ihnen entweder am Bewusstsein für die Risiken in ihrer Umgebung mangelt („Ich kann keine Bedrohung erkennen."), sie dazu tendieren, viel zu optimistisch zu sein („Uns kann das nicht passieren.") oder sie wenige bzw. keine zusätzlichen Ressourcen haben, um Risiken aktiv entgegenzuwirken.

4.5. Wie sehr sind KMU Risiken und Bedrohungen ausgesetzt?

Um den Umfang der Risiken und Bedrohungen zu verstehen, denen KMU ausgesetzt sind, hat die Unternehmensberatungsgesellschaft PwC eine Umfrage zum Thema Informationssicherheit[4] durchgeführt, die Folgendes deutlich macht:

- Drei Viertel (76 %) der befragten KMU hatten im Jahr 2012 einen sicherheitsrelevanten Zwischenfall.
- Bei über der Hälfte handelte es sich dabei um schwerwiegende Zwischenfälle.
- Die Konsequenzen dieser Vorfälle bedeuteten für die Unternehmen einen Verlust von 21.000 € bis zu 42.000 €.

Fakten zu den beobachteten Sicherheitslücken:

- 46 % der KMU erlitten Systemabstürze und Datenbeschädigungen.
- 45 % der Zwischenfälle wurden von Mitarbeitern verursacht.
- Bei 41 % handelte es sich um externe Angriffe.

Die Konsequenzen, die außerplanmäßige Ausgaben von 21.000 € bis 42.000 € auf ein KMU haben können, sind erheblich. Ein Großunternehmen kann diesen Betrag im Normalfall leicht wegstecken, aber ein Kleinstunternehmen kann durch solche unerwarteten Kosten sogar zugrunde gehen.

[4] Vgl. Information Security Breaches Survey – Technical Report, PwC, 2012.

Im Jahr 2015 hat das „Business Continuity Institute“ eine Umfrage[5] durchgeführt, die als Ergebnis einige der Risiken und Bedrohungen auflistet, die Unternehmen am meisten fürchten:

ART DES RISIKOS ODER DER BEDROHUNG	EINTNRITTSWAHR-SCHEINLICHKEIT
Cyber-Angriff	82 %
IT- und Telekommunikationssysteme nicht verfügbar	81 %
Datenverlust	74 %
Versorgung mit Strom, Wasser etc. nicht verfügbar	57 %
Ungünstige Wetterbedingungen	52 %
Probleme in der Beschaffung	48 %
Sicherheitsvorfälle	48 %

Es kann zwischen diesen drei verschiedenen Kategorien von Bedrohungen unterschieden werden:

KATEGORIEN	**ERSTE**	In der ersten Kategorie finden sich die Risiken und Bedrohungen, die am meisten gefürchtet werden, sowie jene, die mit Informationssystemen, Sicherheit und IT zusammenhängen. Dabei kann es sich um Risiken in Verbindung mit Spezial-Anwendungen (z. B. Druckmaschinen-Software) oder mit Standardprogrammen (wie Textverarbeitungsprogramme, E-Mail, Internetbrowser) handeln. Obwohl nicht alle KMU komplett computerbasiert arbeiten, sind sie doch wie jeder andere Betrieb bis zu einem gewissen Grad von der Technologie abhängig. Sobald es zu E-Mail-Korrespondenz mit Kunden, Lieferanten oder Banken kommt, werden sich auf den Computern des Personals vertrauliche Informationen befinden (Bank-Konten von Lieferanten und Kunden, persönliche Daten der Kunden etc.). Daher ist es wenig überraschend, dass die PwC-Studie Cyber-Angriffe und Datenverluste zu den gefürchtetsten Risiken und Bedrohungen für KMU zählt.

[5] Vgl. Horizon Scan 2015 Survey Report, BCI, 2015.

VON BEDROHUNGEN	ZWEITE	Eine zweite wichtige Kategorie der Bedrohungen und Risiken für KMU ist die Verfügbarkeit von Netzwerken (IT- und Telekommunikationsnetzwerke etc.) und die Versorgung mit Strom, Wasser etc., um den täglichen Betrieb aufrecht zu erhalten. Diese Dienste nicht nutzen zu können, kann zum Stillstand des Betriebes führen. Daher benötigt man: (a) Alternative Möglichkeiten, um das operative Geschäft in so einem Fall aufrecht zu erhalten. (b) Kontinuierlichen Informationsaustausch mit den zuständigen Behörden bzw. Dienstleistern, um eine Ausfallzeit abschätzen zu können und dementsprechend zu handeln.
	DRITTE	Die dritte Kategorie der Risiken und Bedrohungen bezieht sich auf die Reduzierung oder den kompletten Verlust von Ressourcen, Vermögenswerten oder Dienstleistungen. Beispiele hierfür sind der Verlust von Büroräumlichkeiten aufgrund eines Erdbebens oder einer Überschwemmung, das Fernbleiben von Schlüsselpersonal, ungünstige Wetterbedingungen oder der Ausfall bzw. Tod des Inhabers. Es ist wichtig, Notfallpläne für solche Eventualitäten zu entwickeln.

4.6. Sind KMU auf Risiken und Bedrohungen vorbereitet?

Nur wenige KMU sind in der Lage, sich mit den oben genannten Problemen aktiv auseinanderzusetzen, und lediglich 30 % von ihnen haben einen Plan[6], wie sie auf diese Risiken, sollten sie tatsächlich eintreten, reagieren könnten. Das Fehlen eines solchen Plans liegt normalerweise daran, dass Unternehmen sich der Gefahren nicht bewusst sind oder deren Ausmaß nicht verstehen. Auch fehlende finanzielle Mittel, Ressourcen, Zeit und Know-how führen dazu, dass sich KMU nicht um einen Plan zur Sicherstellung ihres Geschäftsbetriebes kümmern.

KMU Inhaber und Geschäftsführer wissen meist nicht genau genug über alle möglichen Bedrohungen und Risiken Bescheid. Diese werden als zu komplex oder zu technisch angesehen und oft genug ignoriert, weil andere Aufgaben für das Überleben und das Wachstum des Geschäftsbetriebes auf den ersten Blick wichtiger erscheinen.

Statistische Erhebungen des europäischen Dienstleistungssektors[7] zeigen einerseits, dass sowohl die Anzahl, als auch die Umsätze der europäischen KMU stark gestiegen sind. Andererseits wird auch deutlich, dass eine beträchtliche Anzahl der Unternehmen insbesondere aus dem Dienstleistungssektor im Jahr 2015 den Markt aufgrund von Insolvenz wieder verlassen musste. Der Grund dafür ist recht einfach: KMU sind aus den zuvor genannten Gründen aktuell viel anfälliger gegenüber Risiken und Bedrohungen.

Hier eine Auswahl der unangenehmsten Konsequenzen aus Zwischenfällen in Unternehmen:

a) Produktionsausfall (über mehrere Tage oder Wochen nicht in der Lage sein, den Betrieb fortzuführen)

b) Kundenunzufriedenheit (Kunden wechseln zu anderen Dienstleistern)

c) Höhere Kosten (Gehälter steigen, Wiederaufbauarbeiten etc.)

d) Umsatzeinbußen (nicht in der Lage sein, Dienstleistungen anzubieten und daraus Einnahmen zu generieren)

[6] Vgl. Data Health Check Survey Results 2014, Databarracks, 2015.
[7] Vgl. Economic Outlook no.1220-1221 September-October 2015, Business Insolvency Worldwide, Euler Hermes, 2015.

Es ist relativ unwahrscheinlich, dass ein KMU zum Alltagsgeschäft zurückkehren kann, wenn es sich nicht intensiv und vorausschauend auf den Umgang mit den wahrscheinlichsten Risiken und Gefahren vorbereitet hat.

5. Was ist Resilienz?

Resiliente Unternehmen können sich anpassen und besitzen genügend Widerstandsfähigkeit, wenn z. B. Verluste auftreten. Sie lassen sich von Stress, zunehmender Komplexität, Chaos und sich ständig ändernden Rahmenbedingungen nicht unterkriegen.[8]

In diesem Handbuch definieren wir:

Resilienz-Management betrifft die Anpassungs- bzw. Widerstandsfähigkeit von KMU. Resiliente KMU sind in der Lage, potenzielle Risiken und Bedrohungen zu kontrollieren, sich auf den Umgang mit Fehlern, Katastrophen oder Krisen vorzubereiten bzw. sich von diesen zu erholen; sie können angemessen auf negative und auf positive Zwischenfälle, Umweltveränderungen und neue Chancen reagieren.

Veränderungen, egal ob plötzlich oder schleichend, haben vielfältige Gründe. Diese Veränderungen können reale oder potenzielle Konsequenzen für den Betrieb oder das Eigentum eines Unternehmens haben. Veränderungen können durch Risiken und Bedrohungen erzwungen werden oder durch neue Chancen entstehen. Die Gründe dafür können in internen und externen Ereignissen liegen, die einen lokalen, nationalen oder auch internationalen Hintergrund haben.

Resilienz ist kein Zustand, sondern eine nicht messbare, dynamische Fähigkeit, die sich ein Unternehmen aneignen kann. Jedes Unternehmen hat unterschiedliche Faktoren, die zur Verbesserung der Resilienz führen.

[8] Vgl. ISO/DIS 22316 Sicherheit und Resilienz - Resilienz von Organisationen - Grundsätze und Attribute.

Um die Resilienz eines Unternehmens zu verbessern, müssen mögliche Bedrohungen und Risiken aktiv angegangen werden. Das betrifft alle internen und externen Bereiche, unter anderem Arbeitsschutz, körperliche Sicherheit oder IT Sicherheit. Außerdem ist eine erhöhte Reaktionsfähigkeit bei unbekannten oder ungeplanten Zwischenfällen notwendig (z. B. Katastrophen, Ausfälle, Krisen etc.).

6. Verbessern Sie Ihre Resilienz mit CASSANDRA

6.1. Kann es jemals ein risikofreies Umfeld geben?

Unglücklicherweise nicht. Wir leben in einer sich ständig wandelnden Welt, in der Stillstand ein Fremdwort ist. Jede Veränderung, ob von Menschen gemacht oder umweltbedingt, schafft neue Risiken und ändert die potenziellen Auswirkungen von bestehenden Risiken.

Sie können die Risiken in Ihrem Umfeld deutlich reduzieren, indem Sie auf diese drei Punkte achten:

(a) Identifizieren Sie Ihre Risiken und arbeiten Sie kontinuierlich daran, sie unter Kontrolle zu behalten.

(b) Beobachten Sie Ihre Umgebung und passen Sie sich rasch an Veränderungen an.

(c) Verbessern Sie Ihre Fähigkeit, effektiv auf Zwischenfälle oder das plötzliche Eintreten von Risiken bzw. Krisen zu reagieren.

Dieses Handbuch und die CASSANDRA-Methode wurden entwickelt, um Ihr Unternehmen dabei zu unterstützen, die Kontrolle über mögliche Risiken zu erlangen. Der entscheidende Faktor dabei ist aber der Faktor Mensch. Sie müssen es auch tun!

6.2. Wie geht das CASSANDRA Projekt auf die Bedürfnisse von KMU ein?

CASSANDRA wurde eigens für KMUs entwickelt. KMU Inhaber und Manager benötigen professionelle Unterstützung in Sachen Resilienz-Management. Diese Unterstützung sollte **einfach**, aber trotzdem präzise sein, **praktisch**, aber auch umfassend, **orientiert an der tatsächlichen**

Umsetzung und auch speziell auf das Umfeld und die Bedürfnisse von KMU angepasst. Außerdem dürfen eine klare methodische Vorgehensweise und **praktische Schritt-für-Schritt-Anweisungen** nicht fehlen, die genau erklären, was getan werden muss, was dadurch erreicht wird und wie man effektiv vorgeht.

CASSANDRA bietet drei praxisnahe Instrumente: [9]

- Ein **Quick-Check**-Tool, das Ihnen einen ersten Überblick Ihrer aktuellen Risikosituation verschafft.
- Ein **Online-Kurs**, der Sie durch den gesamten Resilienz-Management-Prozess führt. Der Kurs verhilft Ihnen zu einem umfassenden Verständnis Ihrer Risiken und Bedrohungen, zeigt potenzielle Auswirkungen auf und dient als Wegweiser, damit Sie die besten Lösungen für Ihr Unternehmen finden. Das Beste daran ist, dass Sie den Online-Kurs arbeitsbegleitend nutzen können und Ihre Firma sofort von Ihren Lernfortschritten profitiert.
- **Dieses Handbuch**, das auch in Kombination mit dem Online-Kurs genutzt werden kann, bietet eine umfassende und informative Darstellung aller Themen, die KMU Inhaber und Manager verstehen sollten, bevor sie Resilienz-Management in ihrem Geschäftsalltag effektiv einführen können. Resilienz-Management wird mithilfe eines praxisnahen und strukturierten Ansatzes dargestellt und anhand von Beispielen, Methoden und Dokumenten-Vorlagen vertieft.

6.3. Ihre Vorteile („Was springt dabei für Sie heraus?“)

Die **Widerstandsfähigkeit** Ihres Unternehmens mithilfe von CASSANDRA zu erhöhen, bietet Ihnen jede Menge Vorteile. Hier haben wir ein paar davon aufgelistet:

- Verbessertes Bewusstsein und vernünftigere Entscheidungen von Inhabern, Managern und Mitarbeitern

[9] Vgl. www.cassandra-resilience.eu.

- Mehr Stabilität, um die Zukunft des Unternehmens zu gewährleisten
- Bessere Anpassungsfähigkeit an ein sich ständig wandelndes Umfeld
- Erhöhte Sicherheit für Mitarbeiter und Kunden
- Schutz Ihres Vermögens
- Reduzierte Versicherungskosten und geringere Gefahren durch Risiken und Bedrohungen
- Minimierung der Gefahr eines Betriebsstillstands
- Geringere Abhängigkeit von Mitarbeitern in Schlüsselpositionen
- Geringere Verzögerungen und Optimierung der derzeitigen Prozesse und Betriebsabläufe
- Besseres Verständnis Ihrer rechtlichen, behördlichen und versicherungstechnischen Anforderungen und dadurch u. a. weniger Rechtsstreitigkeiten
- Schutz Ihres guten Rufs und des Markenimages Ihres Unternehmens
- Besseres Management bei Krisen und eine schnellere Rückkehr zum Normalbetrieb; dadurch geringere ökonomische Einbußen
- Gesteigerte Erfolgschancen in der Zukunft
- Und vieles mehr!

7. Ein Resilienz-Projekt in Ihrem Unternehmen starten

7.1. Ihre Entscheidung

Die folgenden beiden Fragen bringen den Nutzen von CASSANDRA auf den Punkt und sollen Sie bei der Entscheidung unterstützen, ein Resilienz-Projekt in Ihrem Unternehmen zu starten:

- Möchten Sie, dass Ihr Unternehmen in Zukunft besser auf Risiken und unerwartete Zwischenfälle vorbereitet ist?
- Ist es Ihnen einige Stunden extra Aufwand wert, um im Ergebnis einen viel widerstandsfähigeren Geschäftsbetrieb zu haben?

Wenn Ihre Antworten JA lauten, **DANN HABEN SIE DEN WERT EINES RESILIENZ-PROJEKTES ERKANNT UND SICH DAZU ENTSCHLOSSEN ZU BEGINNEN**!

Wir können Ihnen zusichern, dass sich Ihre aufgewendete Zeit und die verwendeten Ressourcen definitiv bezahlt machen werden.

7.2. Wie nutzen Sie CASSANDRA, um ein Resilienz-Management in Ihrem Unternehmen einzuführen?

Wir empfehlen KMU Inhabern und Managern, den **Online-Kurs, den Quick-Check und dieses Handbuch** parallel zu verwenden.

Eine beliebte Vorgehensweise ist dabei die folgende:

1. **Nutzen Sie zuerst das Quick-Check-Tool**. Es wird Sie in nur wenigen Minuten mit einigen zentralen Fragestellungen des Risiko- und Resilienz-Managements vertraut machen.
2. **Konzentrieren Sie sich dann, wenn möglich, auf den Online-Kurs**. Jeder Abschnitt des Kurses bezieht sich auf ein bestimmtes Kapitel in diesem Handbuch, die **parallele Arbeit mit beiden Instrumenten** ist daher leicht und sehr empfehlenswert. Arbeiten Sie sich Schritt für Schritt durch den Kurs und legen Sie nach jedem Kapitel eine Pause ein, um die entsprechenden Inhalte in diesem Handbuch zu vertiefen. Im Handbuch finden Sie detaillierte Informationen, die im Online-Kurs so nicht beschrieben sind, sowie Grafiken und Tabellen, die Sie bei der praktischen Umsetzung unterstützen.
3. **Implementieren Sie das Resilienz-Management** in Ihrem Unternehmen am besten **berufsbegleitend und parallel zu Ihren Lernfortschritten**. Alternativ können Sie selbstverständlich auch zuerst den Kurs absolvieren und erst danach mit der Implementierung starten.

Falls Ihnen dieses Vorgehen aktuell zu aufwendig erscheint, können Sie auch erst einmal nur dieses Handbuch durcharbeiten und die hier in den kommenden Abschnitten dargestellten Schritte nacheinander umsetzen. Wichtig ist nur, dass Sie anfangen!

7.3. Wie viel Zeit benötigen Sie?

Für Ihre Entscheidung sind Zeit und Aufwand wesentliche Faktoren. Ein Resilienz-Projekt in einem KMU benötigt im Normalfall das Folgende:

1. **Viel Motivation und Begeisterung für eine bessere Zukunft** (von einer sichereren Zukunft für Ihr Unternehmen zu träumen, dauert nur wenige Sekunden).
2. **Ein paar Vorbereitungen** (diese dauern normalerweise wenige Minuten).
3. **Lernbereitschaft**, sowie ein einige Stunden, um das Projekt durchzuführen und z. B. das Handbuch zu lesen. Die benötigte Zeit können Sie über mehrere Wochen verteilen (im Normalfall 1-3 Stunden pro Woche für 4-5 Wochen – je nach Größe und Komplexität Ihres Unternehmens kann es auch mehr werden).
4. **Das Bestreben, die während des Projekts gefällten Entscheidungen tatsächlich umzusetzen** und die Bereitschaft, diese Umsetzung zu begleiten und zu kontrollieren. Der Arbeitsaufwand (insgesamt zwischen ein paar Stunden bis zu diversen Arbeitstagen) hängt stark von der Ausgangsposition Ihres Unternehmens ab. Dazu gehört z. B. die Zeit, die für den Kauf und die Installation von Anlagen und Software aufgewendet werden muss (beispielsweise Kauf eines Feuerlöschers für das Büro oder die Einrichtung eines Back-Up-Systems für Ihre IT bzw. der Kauf und die Installation eines Anti-Viren-Programms). Auch für die Erstellung eines Notfall-Plans und die Auswahl passender Versicherungen benötigen Sie ein entsprechendes Zeitbudget.
5. Sobald diese Schritte abgeschlossen sind, ist alle 3-4 Monate eine einstündige **Überprüfung** sinnvoll. Außerdem sollten Sie einmal im Jahr eine mehrstündige **umfassende Neubewertung** vornehmen.

Um die **Resilienz Ihres Unternehmens zu erhöhen** und alle Vorbereitungen zu treffen, sind im Normalfall bereits **wenige Stunden pro Woche über einen Zeitraum von einigen Wochen** ausreichend. Die Ergebnisse machen sich definitiv bezahlt.

7.4. Wer sollte das Resilienz-Management-Projekt unternehmensintern leiten?

Es ist wichtig, einen guten Überblick über den Geschäftsbetrieb zu haben. Am besten eignen sich für dieses Projekt daher die Inhaber oder Manager eines KMU.

Diese Schlüsselpersonen kennen die Geschichte des Unternehmens, die zukünftigen Ziele, Verpflichtungen, Risiken, Lieferanten- und Kundenbeziehungen, sowie das wirtschaftliche, soziale, politische und technologische Umfeld, in dem das Unternehmen agiert.

Natürlich sollten diese Personen auch betriebswirtschaftliche Fähigkeiten und Führungsqualitäten besitzen, insbesondere weil wichtige Entscheidungen getroffen werden müssen und die Umsetzung aller notwendigen Maßnahmen gewährleistet werden muss.

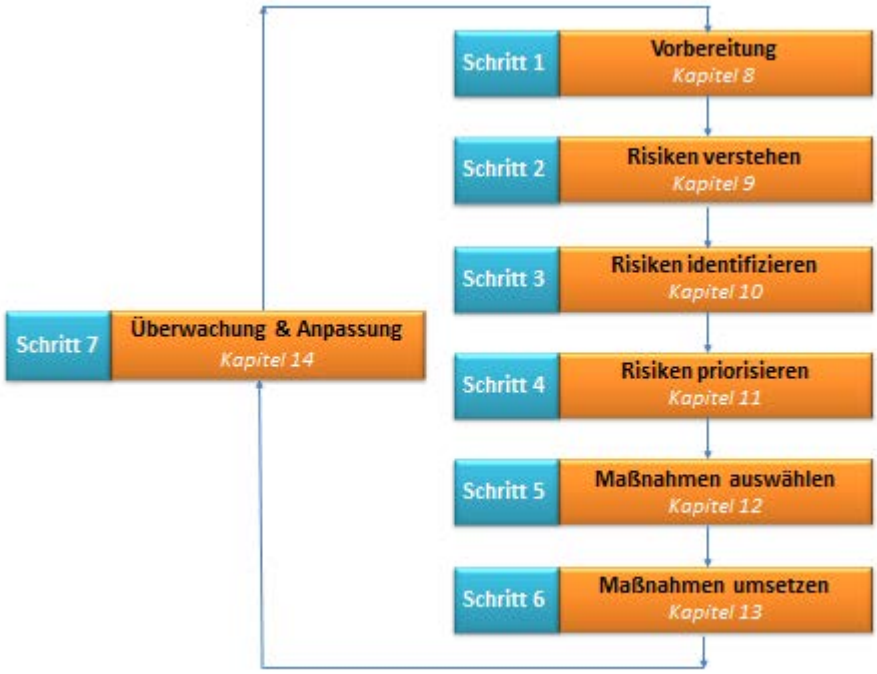
Auch die folgenden Fähigkeiten sind von Vorteil:

- Projekt-Management Know-how
- Gute Kommunikation (sowohl intern unter Mitarbeitern, als auch extern mit Dritten und relevanten Behörden)
- Grundlegende Management-Fähigkeiten wie Führungsqualität, Verlässlichkeit und Integrität

Es gibt keinerlei Einschränkungen, wenn weitere Mitarbeiter des Unternehmens etwas zum Projekt beitragen wollen. Es wäre sogar ideal, wenn alle Mitarbeiter teilhaben und ihren Input beisteuern können – von der Identifizierung der Risiken bis hin zur erfolgreichen Schadensminimierung.

7.5. Sieben Schritte zur Verbesserung Ihrer Resilienz

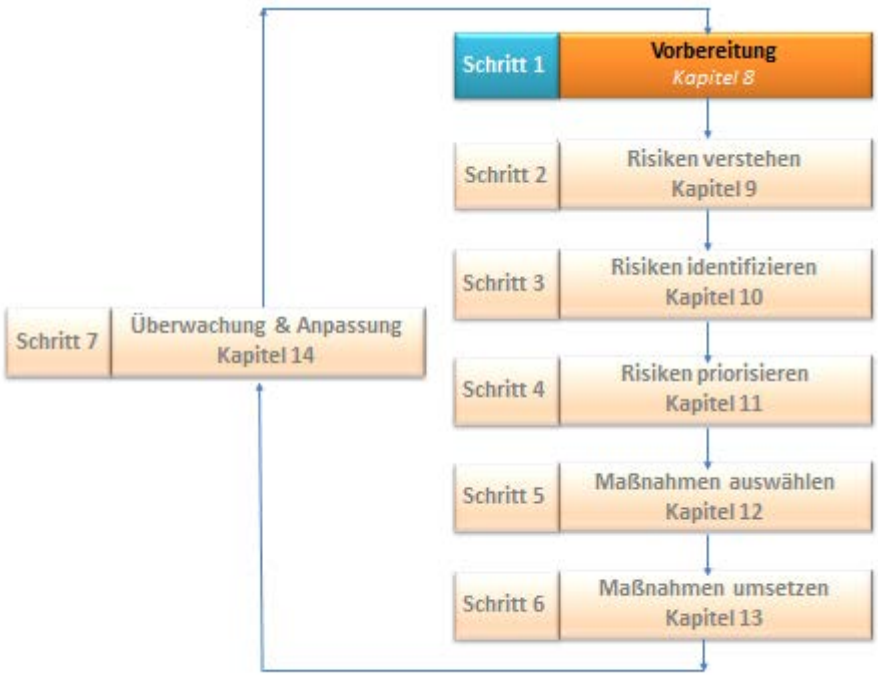
Wie Sie in der folgenden Grafik erkennen können, gehen wir zur Verbesserung der Widerstandsfähigkeit eines Unternehmens in sieben Schritten vor:



Schema 1 – Projektschritte zur Verbesserung der Resilienz – die CASSANDRA-Methode

Wir befassen uns mit jedem dieser Schritte in einem separaten Kapitel dieses Handbuchs. Zu jedem der sieben Schritte gibt es parallel einen entsprechenden Abschnitt im Online-Kurs.

8. Schritt 1 – Vorbereitung



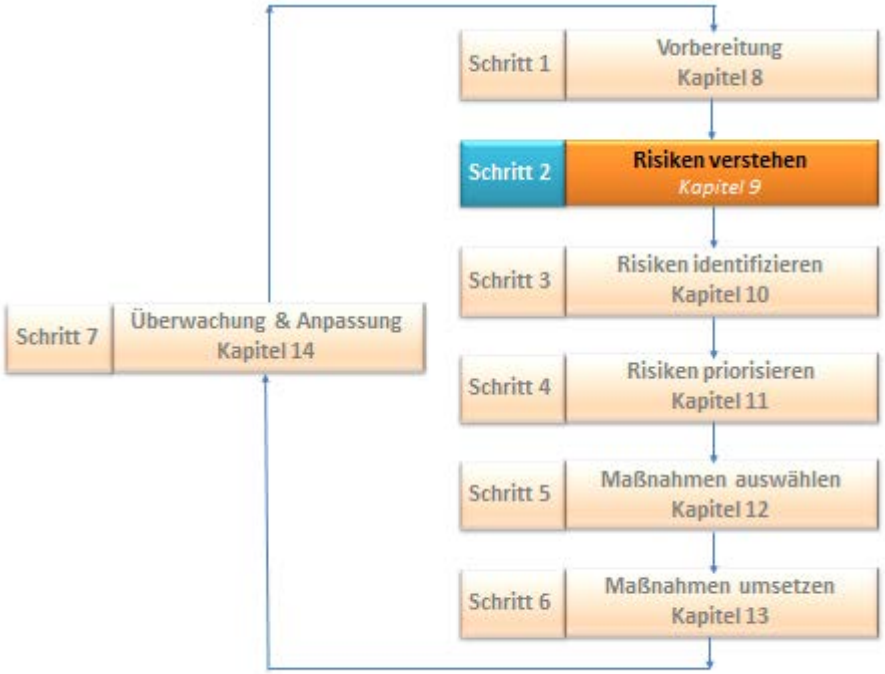
Dieser Schritt kann am einfachsten und schnellsten realisiert werden. Dazu arbeiten Sie sich durch diese Liste:

- Beschaffen Sie sich das Handbuch (bereits erledigt!).
- Bestimmen Sie einen Resilienz-Manager, der das Projekt in Ihrem Unternehmen durchführt (z. B. der Inhaber oder Manager des KMU; ggf. sind Sie das selbst).
- Planen Sie Zeit in Ihrem Kalender ein: 1-3 Stunden pro Woche für die nächsten 4-5 Wochen. Stellen Sie sicher, dass Sie in dieser Zeit nicht mit Unterbrechungen rechnen müssen.
- Informieren Sie alle Mitarbeiter bzw. Kollegen in Ihrem Unternehmen über das Projekt und betonen Sie, dass ihre Unterstützung benötigt und geschätzt wird.
- Stellen Sie Ihren Mitarbeitern oder Kollegen den Link zum Quick-Check-Tool zur Verfügung und erklären Sie ihnen, dass sie diesen Check bitte durchführen sollen.
- Schlagen Sie Ihren Mitarbeitern bzw. Kollegen außerdem den Online-Kurs vor, sofern Interesse besteht.

- Nehmen Sie Stift und Papier zur Hand, um sich Notizen zu machen und Ihre internen Projekt-Dokumente vorzubereiten. Sie sollten auch die Vorlagen verwenden, die wir Ihnen in Ergänzung zu diesem Handbuch zum Download zur Verfügung stellen.

Wir empfehlen Ihnen zur Erfassung der benötigten Arbeitszeit und zur Dokumentation Ihrer Projektergebnisse die einschlägigen Excel- oder Word-Anwendungen zu nutzen.

9. Schritt 2 – Risiken verstehen



Die möglichen Risiken für Ihr Unternehmen hängen stark davon ab, was die Besonderheiten Ihres Geschäftsbetriebes sind. Unternehmen der gleichen Größe, die sich im gleichen Sektor befinden, können zwar fundamentale Gemeinsamkeiten aufweisen, jedoch ist letzten Endes **jeder Betrieb einzigartig**. Außerdem gibt es viele externe Einflüsse, die eine Rolle spielen können.

Um den ersten Schritt in Richtung verbesserte Unternehmens-Resilienz zu gehen, sollten Sie die **Charakteristika Ihres Unternehmens und die des Umfelds, in dem Sie agieren, dokumentieren**. Notieren Sie alle Schlussfolgerungen Ihrer Beobachtungen, um damit das Fundament für Ihre nächsten Schritte zu legen.

Wenn Sie Ihren Unternehmenskontext analysieren, spielen sowohl interne, als auch externe Faktoren bzw. Herausforderungen eine wichtige Rolle. Wir vertiefen hier zuerst die externen Herausforderungen, und gehen danach auf die internen Herausforderungen ein.

Externe Herausforderungen sind Faktoren, die außerhalb der Kontrolle Ihres Unternehmens liegen. Diese können sowohl Ihre Leistungsfähigkeit beeinflussen, als auch die Fähigkeit, Ihre strategischen Ziele zu erreichen. Hier finden Sie Beispiele für externe Herausforderungen:

Soziale Heraus-forderungen	Von sozialen Herausforderungen spricht man, wenn ein großer Teil der Gesellschaft betroffen ist. Diese Themen haben im Normalfall unerwünschte Auswirkungen auf die Lebensqualität und betreffen z. B. Ihre Mitarbeiter, Geschäftspartner, Kunden oder sogar das gesamte Gebiet, in dem Sie tätig sind. Beispiele für entsprechende soziale Herausforderungen sind: • Kriminalität und Gewalt (eine hohe Kriminalitätsrate erfordert erhöhte Sicherheitsvorkehrungen) • Arbeitslosigkeit (niedrige Arbeitslosigkeit kann dazu führen, dass Mitarbeiter schneller kündigen und sich eine andere Position suchen) • Nicht genügend Experten oder Fachkräfte in Ihrem Tätigkeitsfeld • Armut • Öffentliche Sicherheit und Terrorismus • Epidemien und andere Gesundheitsprobleme • … Soziale Herausforderungen können sich auch auf andere Faktoren beziehen, z. B. Vorlieben, Interessen und Trends in der Gesellschaft. Die Veränderung der Interessen oder neue Trends, z. B. das Thema Digitalisierung[10], können Unternehmen zu einer Transformation Ihres Geschäftsmodells zwingen.

[10] Vgl. http://www.emcra.eu/projekte/digitalisation/.

Politische Heraus-forderungen	Politische Herausforderungen betreffen Aspekte wie die staatliche Ordnung, die Regierungsführung und die öffentliche Verwaltung. Bei politischen Herausforderungen besteht oft eine Verbindung zum politischen Klima in der Region, in der Ihr Unternehmen aktiv ist (national bzw. auch auf der Ebene der Europäischen Union) und zu der/den Region(en), die für Ihren Geschäftsbetrieb wichtig ist/sind. Politische Herausforderungen können enorme Auswirkungen auf ein Unternehmen haben, z. B. durch neue Gesetze bzw. Regulierungen oder durch höhere finanzielle Belastungen aufgrund zusätzlicher Steuern oder Abgaben. Beispiele für entsprechende politische Herausforderungen sind: • Staatliche Vorschriften (Genehmigungen) • EU-Beitritt oder -Austritt (z. B. BREXIT) • Rechtliche Angelegenheiten (z. B. Zugang zur Rechtsprechung und deren Kosten) • Steuerliche Herausforderungen • Copyright-Gesetze • Eigentums- und Mietrecht • Arbeits- und Handelsrecht • Krankenversicherung für Sie und Ihre Mitarbeiter • Umweltvorschriften • …

Wirtschaftliche Heraus-forderungen	Die wirtschaftlichen Rahmenbedingungen haben einen signifikanten Einfluss auf Unternehmen, da Nachfrage und Angebot von Gütern und Dienstleistungen davon direkt betroffen sind. Wirtschaftliche Herausforderungen, wie z. B. ein genereller Rückgang der Wirtschaftstätigkeit oder des Konsumentenvertrauens, können einem Unternehmen erheblichen Schaden zufügen. Faktoren, die hierbei berücksichtigt werden müssen, sind: • Das nationale wirtschaftliche Umfeld • Das lokale, regionale, nationale und internationale Wettbewerbsumfeld • Zugang zu Kapital • Zinskosten • Wechselkursschwankungen • Steuern • Gehälter • Inflation oder Deflation • …
Technologische Heraus-forderungen	Die Technologie ist einem ständigen Wandel unterworfen und verlangt von Unternehmen eine Entwicklung im Einklang mit dem technologischen Fortschritt. Es werden ständig Verbesserungen durch neue Technologien hervorgebracht, welche die Art und Weise verändern, wie Dienstleistungen erbracht und Produkte produziert werden, wie Angestellte arbeiten und wie Unternehmen ihr Angebot für potenzielle Kunden vermarkten. Die ständige Anforderung, das Unternehmen an ein sich rasch änderndes Umfeld anzupassen, ist für alle beteiligten Akteure eine große Herausforderung. Es bedarf darüber hinaus umfassender Investitionen, um mit dem technischen Wandel mitzuhalten, jedoch wären die Folgen fatal, wenn man die technologischen Veränderungen ignorieren

würde.

Beispiele für technologische Herausforderungen sind:

- Mobile Datennutzung (mobile Computernutzung, Tablets, Mobiltelefone, E-Mail etc.)
- Transformation des Arbeitsplatzes (z. B. Mitarbeiter, die von zu Hause aus arbeiten)
- Cloudbasierte Dienste
- Social Media (Menschen kommunizieren unglaublich viel in sozialen Netzwerken – besonders bei negativen Ereignissen!)
- Informationssicherheit (z. B. Viren, Malware, Datenverlust etc.)
- Neue Verkaufs- und Distributionskanäle für Dienstleistungen und Produkte
- Neue Gesetze zur Aufbewahrung und Nutzung von Daten
- …

Umwelt-Heraus-forderungen	Sowohl der geografische Standort eines Unternehmens, als auch die für Sie geltenden Umweltvorschriften stellen Umwelt-Herausforderungen für Ihr Unternehmen dar. Bei der Abwägung der Umweltthemen sollten Sie die folgenden Faktoren in Betracht ziehen: • Geografischer Standort • Kundennähe (u. a. im Zusammenhang mit der Lieferung von Produkten) • Klima und die natürliche und bauliche Umgebung Ihres Unternehmens • Wetterbedingungen (Kälte, Regen, Schnee, Hitze etc.) • Naturkatastrophen (Erdbeben, extreme Temperaturen etc.) • Energieanforderungen und -ausgaben (z. B. Kosten für Heizung oder Klimaanlage) • Verfügbarkeit und Qualität von Versorgungsbetrieben • Umweltvorschriften • Giftige oder gefährliche Materialien (z. B. in der Nähe Ihres Betriebes gelagert) • …

Interne Herausforderungen sind Faktoren, die vom Unternehmen selbst gesteuert bzw. beeinflusst werden können. Hier zeigt sich, wie ein Unternehmen arbeitet. Sie sind ausschlaggebend für den Erfolg. Beispiele für interne Herausforderungen sind:

Management bzw. Leitung: Organisations-struktur, Rollen und Verantwortlich-keiten	Beim Thema Management bzw. Leitung geht es um das gesamte Grundgerüst an Regeln, Vorschriften, Methoden, Prozessen und Kontrollelementen, auf dessen Basis das Unternehmen betrieben und gesteuert wird. Wird dabei alles richtig gemacht, kann das Unternehmen seine Ziele erreichen und erfolgreich agieren. Aspekte von gutem Management sind: • Organisationsstruktur und Effizienz • Klar definierte Rollen und Verantwortlichkeiten • Definierte Entscheidungsfindungsprozesse (für alltägliche und für grundsätzliche Entscheidungen) • Nachfolgeplanung (Ersatz) für Leitung und Personal • …
Strategie: Richtlinien und Zielsetzung des Unternehmens	Die Strategie eines Unternehmens basiert auf der Vision für die Zukunft der Organisation und der Richtung, die es einschlagen muss, um die langfristigen Ziele zu erreichen. Die Entscheidungen, die auf dem diesem Weg getroffen werden, spiegeln die zentralen Werte des Unternehmens wieder. Wichtige Aspekte sind: • Unternehmensziele, die in der Zukunft erreicht werden sollen • Vision • Geschäftsplan • Ressourcenverteilung • Übertragung und Dezentralisierung von Verantwortlichkeiten • Management-Systeme (Existenz von schriftlich fixierten Regeln, betrieblichen Prozessen und Vorschriften) • …

Standards	Die Standards eines Unternehmens beziehen sich auf die intern beschlossenen und etablierten Vorgehensweisen und Prozesse. Standards regeln z. B. die Dienstleistungserbringung und die internen Arbeitsabläufe, oft schriftlich spezifiziert in unternehmensinternen Richtlinien. Dazu gehört: • Standardisierung der Produktion und der Lieferung von Produkten und Dienstleistungen (um gleichbleibende Qualität zu sichern) • Schriftliche Richtlinien • Interne und externe Kommunikationsvorgaben (z. B. standardisiertes Briefformat, 24-Stunden-Service bei Beschwerden etc.) • …
Ressourcen und Fähigkeiten	Das Geschäftspotenzial eines Unternehmens hängt von den Faktoren Know-how, Expertise, Kapazitäten und Materialien ab. All das wird benötigt, damit die Kernfunktionen einer Unternehmung erfüllt werden können. Das Thema Ressourcen und Fähigkeiten betrifft alle Geschäftsbereiche, darunter Finanzen, Zeitmanagement, Personal, technische Systeme, Vertrieb und Lieferanten. Relevante Aspekte sind: • Das Know-how und die Expertise von Mitarbeitern und Management • Das Einstellen und Halten von qualifizierten Mitarbeitern • Kreativität und die Bereitschaft zur Innovation • Bestehende IKT-Systeme und Technologien (ausreichend, alt oder obsolet?) • Ausreichende Anzahl an Beschäftigten • Anzahl der Mitarbeiter, die bald in den Ruhestand gehen • Finanzielle Möglichkeiten • …

Informations-systeme	Ihre Informationssysteme sind eine wesentliche Grundlage für den Erfolg Ihres Unternehmens. Diese Systeme verarbeiten Ihre Geschäftsdaten und stellen Ihnen Informationen zur Verfügung, die Ihnen die Entscheidungsfindung erleichtern soll. Die Bedeutung des Informationssystems für Ihr Unternehmen hängt von vielen Aspekten ab, u.a. der Modernität Ihres IKT Systems, der Anzahl der Geschäftsprozesse, die von dem IKT System abgebildet werden, von Herausforderungen durch das Thema Informationssicherheit etc. Wichtige Aspekte in diesem Bereich sind: • Strategische IKT Planung (was erwarte ich von meinem IKT System und wird diese Erwartung aktuell erfüllt?) • IKT Regelungen und Verfahren • Support und Wartungsprobleme • Back-Up- und Notfallpläne • Informationssicherheit (Zugangsbeschränkung, Malware, Viren, Informationslecks etc.) • Informationsfluss und Verteilung von Informationen (an Mitarbeiter oder Kunden) • …

Interne und externe Stakeholder und andere Dritte	Stakeholder sind interne oder externe Gruppen bzw. Akteure, die ein Interesse am Erfolg des Unternehmens haben. Beispiele für interne Stakeholder sind: • Inhaber oder Aktionäre bzw. Anteilseigner • Investoren • Manager und Mitarbeiter Beispiele für externe Stakeholder sind: • Kunden • Geschäftspartner • Lieferanten • Auftragnehmer • Kommunalverwaltung und lokale Bevölkerung Wichtige Aspekte in Bezug auf Stakeholder sind: • Management der Beziehungen zu Stakeholdern • Wahrnehmung, Werte und Interessen der Stakeholder • Effektive Kommunikation und Zusammenarbeit mit Stakeholdern • …

All die genannten Herausforderungen und Faktoren haben einen Einfluss auf die Existenz, den Betrieb und die zukünftigen Erfolge und Misserfolge Ihres Unternehmens.

Jeder dieser Bereiche könnte Risiken und Chancen beinhalten, die für Sie relevant sind. Deshalb ist es notwendig, etwas Zeit zu investieren, um zu überlegen, welchen Einfluss der jeweilige Bereich auf Ihr Unternehmen haben kann.

Kommen wir zu ein paar Beispielen:

- Eine hohe Arbeitslosenrate in Ihrer Umgebung erleichtert Ihnen ggf. die Suche nach neuen Mitarbeitern, aber es kann trotzdem schwer sein, genau die passenden Fachkräfte für Ihr Unternehmen auf dem Arbeitsmarkt zu finden, z. B. wenn ein Mitarbeiter in Pension geht oder kurzfristig Ihr Unternehmen verlässt. Arbeitslosigkeit bzw. der lokale Arbeitsmarkt kann demnach ein positives Risiko (also eine Chance) darstellen, sich aber auch als negatives Risiko erweisen.
- Externe Herausforderungen und Risiken in Bezug auf lokale und globale Politik können Ihr Unternehmen stark beeinflussen. So kann zum Beispiel ein Terroranschlag den Tourismus in einer bestimmten Region reduzieren und lokalen Betrieben enormen Schaden zufügen.
- Ein weiteres Beispiel ist die Arbeit mit veralteter IKT Technologie. Dadurch können Sie Risiken ausgesetzt sein, wie:
    - Nicht genügend verfügbare IKT-Experten, die Sie bei technischen Problemen unterstützen können
    - Komplizierte und kostenintensive Wartung oder Reparatur, sobald ein IT Gerät ausfällt
    - Verminderte Produktivität (langsame IT Systeme, zu geringe Speicherkapazität etc.)
    - Erhöhte Gefährdung durch Viren und Hacking, da diese Systeme oft keine Updates gegen neue, aggressivere Computer-Viren erhalten
- Keine Datensicherung von wertvollen Daten und Informationen auf Ihren IKT Systemen (z. B. Laptops) zu machen, kann ein schwerwiegendes Risiko darstellen. Festplatten in IT Systemen geben normalerweise keinerlei Warnsignal, bevor sie versagen und Ihre Daten permanent unzugänglich sind.
- Es kann zu kritischen Situationen führen, wenn Ihr Unternehmen keinen Geschäftsplan und keine Jahresplanung hat. Schlechte Finanzplanung, unzureichende Ressourcenplanung und Planung der Personalkosten, unklare Gewinnziele und keine effektiven Mittel gegen plötzliche Marktumschwünge oder negative Zwischenfälle sind ein großes Risiko.

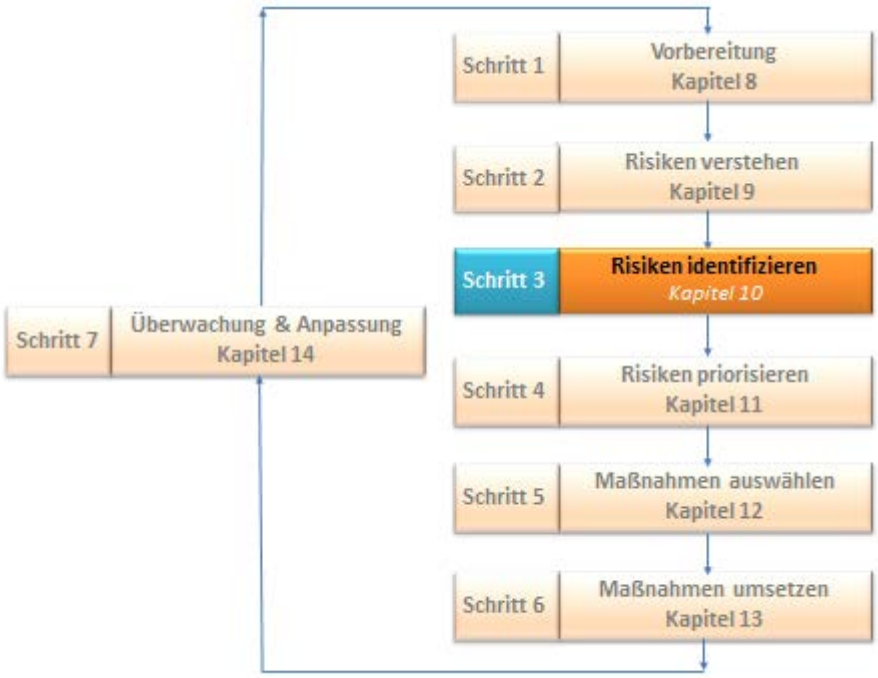
- Wenn es keine standardisierten Richtlinien und Prozesse für wichtige Aktivitäten gibt, könnte das unterschiedliche Servicequalität für Ihre Kunden bedeuten. Unzureichende Dokumentation kann katastrophale Folgen haben, wenn ein Mitarbeiter in einer Schlüsselposition das Unternehmen ohne Vorwarnung verlässt.
- Grippewellen oder saisonal bedingte Krankheiten können oftmals dazu führen, dass Mitarbeiter längere Zeit der Arbeit fernbleiben. Das Ergebnis könnte z. B. schlechter oder gar kein Kundenservice während der Hauptsaison sein. Das stellt ein äußerst hohes Risiko dar und ist besonders kritisch, wenn Ihr Unternehmen im personenintensiven Dienstleistungssektor arbeitet.
- Der geografische Standort Ihres Unternehmens spielt eine große Rolle, da es in gewissen Gebieten zu Wetterrisiken und Naturkatastrophen kommen kann (z. B. Gebiete in denen Schneestürme, eisige Winter oder Hitzewellen Standard sind). Sollte es einen nahegelegenen Fluss geben, der in den letzten Jahren häufig über die Ufer getreten ist, ist auch das definitiv ein Risiko, das man nicht unterschätzen darf. In Ländern wie Griechenland sollte man mit Erdbeben rechnen und sich überlegen, welche Konsequenzen eine solche Katastrophe auf das Unternehmen hat. Liegt Ihr Standort in der Nähe eines Waldes, so sollten Sie speziell in der mediterranen Gegend mit dem Risiko eines Waldbrandes rechnen. Außerdem könnten Risiken auftreten, wenn sich Ihr Unternehmen in der Nähe von gefährlichen Gütern (z. B. einer Tankstelle) oder in einer Gegend befindet, in der es öfters zu öffentlichen Demonstrationen kommt. Auch eine Umgebung mit schlechter Polizeiüberwachung kann kritisch sein.
- Schlechte Leistungen oder der Ausfall eines wichtigen Geschäftspartners oder Lieferanten ist ein enormes Risiko, das nicht auf die leichte Schulter genommen werden darf, besonders dann nicht, wenn ein maßgeblicher Teil Ihres Geschäftsbetriebes davon abhängt.
- Schlechte Auftragsklärung und Vertragsgestaltung (z. B. Unachtsamkeit bezüglich der Bedingungen, Voraussetzungen und Verpflichtungen eines Vertrages) kann zu schweren Verlusten führen und in extremen Fällen auch zur Schließung Ihres Unternehmens.

Es gibt noch unzählige weitere Beispiele für Risiken, denen Sie ausgesetzt sein könnten, jedoch haben wir uns für jene entschieden, die bei ganz normalen

Unternehmen häufig auftreten. Das Hauptziel dieses Kapitel war es, dass Sie Ihr gesamtes Unternehmensumfeld berücksichtigen, verstehen und analysieren. Sie sollten sowohl potenzielle interne, als auch externe Herausforderungen erkennen und verinnerlichen, welche Risiken daraus für Ihr Unternehmen entstehen können.

Jetzt haben Sie ein gutes Grundverständnis von Ihrem Unternehmensumfeld und sind bereit für den nächsten Schritt.

10. Schritt 3 – Risiken identifizieren



10.1. Alle Risiken identifizieren?

Dies ist einer der wichtigsten Schritte Ihres Projektes. Eventuell sogar der wichtigste, da keiner der folgenden Schritte umgesetzt werden kann, wenn Sie ein Risiko nicht zuerst einmal überhaupt identifizieren konnten. Dies ist besonders problematisch, da Sie einem Risiko, das Sie übersehen haben, weiter ausgesetzt sind und sobald es eintritt nicht wissen, wie Sie damit umgehen sollen.

Wir müssen jedoch auch akzeptieren, dass es nicht möglich ist, jedes einzelne Risiko und jede Gefahr ausfindig zu machen und zu identifizieren. Das liegt in der Natur des Menschen; alle unsere Bemühungen haben Grenzen.

Trotzdem gilt: Wenn Sie systematisch arbeiten und einer konkreten Methode wie CASSANDRA folgen, können Sie sicher sein, dass Sie alles in Ihrer Macht Stehende getan haben, um die für Ihr Unternehmen kritischen Risiken zu identifizieren. Mehr noch: Sie können darüber hinaus davon ausgehen, dass Sie Ihre wichtigsten Risiken tatsächlich alle identifizieren konnten.

Es ist auch gut zu wissen, dass die Identifizierung Ihrer Risiken wahrscheinlich etwas umfangreicher ausfallen würde, wenn sie sofort von einem Risikomanagement-Spezialisten durchgeführt würde. Wenn Sie Ihrem Resilienz-Projekt jedoch genügend Zeit und Aufmerksamkeit schenken, können Sie recht schnell zu einem Profi auf diesem Gebiet werden und sicher sein, dass Sie den Großteil Ihrer Risiken auch selbst identifizieren können.

Zu guter Letzt sollten Sie sich klarmachen, dass Ihnen die Identifizierung Ihrer Risiken immer nur einen Ist-Zustand liefert. Morgen, nächste Woche oder nächsten Monat könnten schon neue Gefahren für Ihr Unternehmen entstehen, da sich Ihr Geschäftsumfeld ständig ändert. Eine neue Steuerregelung oder ein Terroranschlag sind nicht langfristig vorhersehbar und können Ihre Risiko-Situation einschneidend ändern.

Das bedeutet nicht, dass Sie täglich Ihre Risiken neu identifizieren und die CASSANDRA-Methode laufend anwenden müssen. Durch eine gute erste Identifizierung erhalten Sie eine Liste mit allen wichtigen Risiken, die wahrscheinlich auch morgen noch genauso aktuell sein werden. Sie sollten sich täglich nur eine einzige wichtige Frage stellen: „Wenn man alle Aktivitäten, Änderungen und Entwicklungen in Betracht zieht; ist mein Unternehmen eventuell neuen, bisher nicht identifizierten Risiken ausgesetzt?“. Lautet die Antwort dazu ja, sollten Sie dieses neu identifizierte Risiko auf Ihre Liste setzen und separat bearbeiten. Sich darum zu kümmern, dauert im Normalfall nur ein paar Sekunden oder Minuten.

Zusammengefasst kann man empfehlen, dass Sie Ihre **Risikoliste mindestens einmal pro Jahr komplett überprüfen sollten um festzustellen, ob auch tatsächlich alle bisher registrierten Risiken noch gültig sind oder ob eventuell einige entfernt werden können. Auch neue Risiken können während dieser jährlichen Überarbeitung hinzugefügt werden**.

Obwohl Ihre Risikoliste nie komplett leer sein wird, kann Ihnen die CASSANDRA-Methode dabei helfen, sie so kurz wie möglich zu halten. Insgesamt wird Ihr Unternehmen möglichen Risiken in Zukunft definitiv weniger stark ausgesetzt sein.

10.2. Kategorisierung von Risiken

Um Ihre Risiken systematisch zu identifizieren, hilft es, verschiedene Risikokategorien bzw. Risikobereiche zu unterscheiden. Das ermöglicht es Ihnen, einzelne Bereiche Ihres Unternehmens separat und möglichst umfassend und tiefgehend zu analysieren. Risikobereiche können von Unternehmen zu Unternehmen unterschiedlich sein. Das hängt insbesondere von der Herangehensweise Ihres Risikomanagers (wahrscheinlich Sie selbst!) ab. Es gibt in der Literatur bzw. im Internet diverse brauchbare Ansätze – wir haben uns in diesem Handbuch dazu entschlossen, die folgenden sieben Risikokategorien zu nutzen, da sie unserer Meinung nach eine breite Analyse zulassen:

1. Unternehmens- und strategische Risiken
2. Operative Risiken und Risiken für die Sicherstellung des Geschäftsbetriebes
3. Finanzielle Risiken
4. IT- und Informationssicherheits-Risiken
5. Behördliche und rechtliche Risiken
6. Risiken im Personalbereich
7. Management-Risiken und Risiken durch Interessensvertreter

In den kommenden Absätzen bzw. Unterkapiteln analysieren wir jede dieser Kategorien nacheinander und geben Ihnen eine Fülle an Beispielen, um Sie dabei zu unterstützen, Ihre eigenen Risiken zu identifizieren. Sie werden feststellen, dass einige Risiken in mehreren Kategorien vorkommen können. Das stellt kein Problem dar, da im Endeffekt nur wichtig ist, möglichst alle Risiken zu identifizieren, egal in welche Kategorie sie einsortiert werden.

10.2.1. Unternehmens- und strategische Risiken

Diese Risiken beziehen sich auf:

(a) Den Geschäftsbereich und Markt (lokal oder international), in dem Ihr Unternehmen agiert

(b) Das allgemeine Geschäftsumfeld

(c) Die Strategien und die strategischen Ziele des Unternehmens

Um erfolgreich zu sein, benötigt jedes Unternehmen einen wohl durchdachten Geschäftsplan. Strategische Risiken bestehen, wenn dadurch Ihre Unternehmensstrategie beeinträchtigt werden könnte und die Erreichung Ihrer Ziele erschwert wird. Dies kann durch technologische Innovationen, durch neue Wettbewerber, eine veränderte Nachfrage, eine Erhöhung der gewohnten Kosten oder ähnlich weitreichende Veränderungen hervorgerufen werden.

Eine unvollständige Liste wichtiger Themen beinhaltet unter anderem:

- Marktrisiko (und Risiko in Ihrem spezifischen Geschäftsbereich)
- Politisches Umfeld
- Wettbewerb
- Öffentliche Sicherheit
- Nationale Wirtschaftslage
- Veränderung des Kundenverhaltens
- Veränderung bei der Nachfrage nach Dienstleistungen
- Arbeitsrecht (Veränderungen und aktuell gültiges Recht)
- Unternehmens-Fusionen und -Übernahmen
- Neue, die aktuelle Wirtschaftsweise stark verändernde Technologien
- Protektionismus
- Steigende Kosten für Personal und Materialien
- Investitionsrisiken
- Branding und Marketing/Kommunikation
- Risiken für den Ruf Ihres Unternehmens
- Betrug und Korruption
- Überaltertes geistiges Eigentum
- Unzureichende Qualitätssicherung
- Unzureichende Investitionen in Forschung und Entwicklung

10.2.2. Operative Risiken und Risiken für die Sicherstellung des Geschäftsbetriebes

Diese Risiken beziehen sich auf den operativen Geschäftsbetrieb, auf die angebotenen Dienstleistungen, auf alle Aktivitäten, um diese Dienstleistungen zu erbringen und auf die interne Verwaltung im Unternehmen. Außerdem gehören in diese Kategorie solche Risiken, die sich auf die Sicherstellung des Geschäftsbetriebes auswirken (z. B. im Zusammenhang mit Katastrophen oder negativen Zwischenfällen). Operative Risiken sind unerwartete Schwierigkeiten oder Fehler im alltäglichen Betrieb. Sie können u. a. eine technische Ursache haben oder auf menschliche Fehler zurückzuführen sein.

Eine unvollständige Liste wichtiger Themen beinhaltet u. a.:

- Schlechte Qualität Ihrer Dienstleistungen
- Schlechtes Projektmanagement
- Risiken im Bereich Logistik und Transport
- Geänderte Auflagen und der interne Umgang damit
- Vertragliche Risiken
- Umgang mit Versicherungen und Umfang der Absicherung
- Outsourcing
- Menschliches Versagen im operativen Betrieb
- Arbeitskonflikte und Streiks
- Fälschungen
- Betrug
- Epidemien, Grippepandemien
- Nachfolgeregelung oder Vertretung (Management und Personal)
- Wasserschäden, sanitäre Ausfälle
- Externe oder interne Stromversorgung
- Stromausfälle oder Spannungsspitzen

- Ausfall von Heizung, Lüftung oder Klimaanlage
- Ausfall von Maschinen
- Verlust oder Zerstörung von Eigentum
- Gefahrengüter: verschüttete Chemikalien und Kontaminierung (verbunden mit nahegelegener Produktion, Transport und Lagerung)
- Feuer in Ihren Geschäftsräumen: gravierend/wesentlich/gering
- Feuer in der Umgebung: gravierend/wesentlich/gering
- Staubstürme
- Erdbeben: gravierend/wesentlich/gering
- Überschwemmungen und Dürre
- Erdrutsche
- Hitzewellen
- Wirbelstürme, Taifune, Hurrikane
- Schnee- und Eisstürme
- Vulkane
- Gezeiten und Flutwellen
- Persönliche Sicherheit
- Zugang zum Unternehmensstandort nicht möglich
- Arbeitsschutzmittel fehlen
- Diebstahl oder Raub
- Bombendrohungen
- Entführungen
- Terroranschläge
- Verkehrsunfälle
- Zug-, Flugzeug-, Schiffs-Unfälle

Risiken für die Sicherstellung des Geschäftsbetriebes führen in der Regel zum Stillstand oder zu Unterbrechungen des Geschäftsbetriebes bzw. der operativen Tätigkeiten eines Unternehmens. Ursachen sind u. a. desaströse Zwischenfälle wie Brände, Erdbeben, Überschwemmungen etc.

Auch die Nichtverfügbarkeit von wichtigen Mitarbeitern, wesentlichen Lieferanten oder Dienstleistungen von Geschäftspartnern fallen in diese Kategorie. Da es sich hierbei um spezielle Risiken handelt, wird auch ein spezieller Ansatz benötigt – diesen besprechen wir ausführlich in einem späteren Kapitel in diesem Handbuch.

10.2.3. Finanzielle Risiken

Diese Risiken decken den gesamten Finanzbereich eines Unternehmens ab, also Kapital und Finanzierung, Finanzplanung, Fördermittel, Kosten und Preisfindung, Steuern und Abgaben etc.

Eine unvollständige Liste wichtiger Themen beinhaltet u. a.:

- Eigenkapital des Unternehmens
- Zahlungen an Lieferanten
- Forderungen gegenüber Kunden
- Betriebskosten
- Investitionen
- Budgetverwaltung
- Buchhaltung und Finanzmanagement
- Besteuerung
- Steuerzahlungen und Sozialversicherung
- Cash-Flow und Liquidität
- Kreditzugang und Kreditwürdigkeit
- Zinsrisiko
- Währungsrisiko

- Kostenkalkulation
- Umsatz und Preisstruktur
- Gewinnspannen

10.2.4. IT und Informationssicherheits-Risiken

Die Risiken in diesem Bereich beziehen sich auf alle technischen Installationen, die ein Unternehmen nutzt (z. B. Druckmaschinen bei Druckereiunternehmen, Computersysteme bei Steuer- oder Unternehmensberatern). Dieser Abschnitt ist etwas detaillierter, weil die hier diskutierten Risiken sehr vielfältig sind und es den meisten Personen in KMU an dem notwendigen IT-Know-how mangelt.

IKT Systeme werden von Unternehmen zur Unterstützung ihrer Kernaufgaben genutzt (z. B. Steuerberatungsunternehmen nutzen IKT Systeme, um die Konten aller Kunden zu erfassen, eine Anwaltskanzlei nutzt sie, um alle rechtlichen Dokumente eines Vorgangs zu speichern). Fast jedes Unternehmen nutzt IKT Systeme für betriebswirtschaftliche und für Management-Aktivitäten (egal ob es sich dabei um einen einzelnen Laptop, ein kleines Büro oder ein Computernetzwerk handelt).

10.2.4.1. Informationsbestände identifizieren

Um alle relevanten Risiken zum Thema IKT System identifizieren zu können, ist es wichtig, ein gutes Verständnis davon zu haben, was alles in die Kategorie „IKT Systeme“, oder anders ausgedrückt, was alles zu Ihren „Informationsbeständen“ gehört.

Da Informationen nicht immer elektronisch gespeichert werden, bezieht sich der Ausdruck „Informationsbestände“ auch auf jede andere Form von Informationen, z. B. auch auf Ausdrucke auf Papier.

Die folgende Tabelle soll Sie dabei unterstützen, Ihre Bestände zu identifizieren:

BEREICH	BESCHREIBUNG	BEISPIEL
IT Systeme	Wir nutzen den Begriff „System“, wenn wir von einer „Einheit“ sprechen, die Hardware, Software und Daten zur Verarbeitung von Information beinhaltet. Wenn wir z. B. von unserem „ERP System“ sprechen, meinen wir den Server, auf dem sich die ERP Anwendung befindet. Die Anwendung und die ERP Daten werden auf den Festplatten dieses Servers gespeichert. Auch ein Drucker ist ein IT System.	• Server • Computer • Laptops • Workstations • Backup-Systeme • Speichersysteme • Drucker • USB Sticks • CDs • Externe Festplatten • Smartphones • …

BEREICH	BESCHREIBUNG	BEISPIEL
Netzwerk	Alle Geräte, die benötigt werden, um das IT System eines Unternehmens aufzubauen. Ein Netzwerk beinhaltet alle Kabel, Router und Modems, um die netzwerkinterne Kommunikation zu ermöglichen.	• Verkabelung • Switches • Router • W-LAN
Kommunikation	Verbindungen zu anderen Telekommunikations- und Datennetzwerken, die von Telekommunikationsunternehmen zur Verfügung gestellt werden.	• Daten- und Internetleitungen • Telefonleitungen
Anwendungen	Hiermit sind Software-Anwendungen gemeint, die genutzt werden um Informationen zu verarbeiten. Sie werden innerhalb eines IT-Systems installiert.	• ERP • E-Mail • Internet Browser • Website • MS Office (Word, Excel etc.)
Systeme von externen Anbietern	Dabei handelt es sich um IT-bezogene Dienstleistungen, die von Dritten zur Verfügung gestellt werden, also Anwendungen, die Fremdeigentum sind, aber von unserem Unternehmen genutzt werden.	• Cloud Speichersysteme (Nutzung von Speichersystemen von Dritten, um unsere Daten zu sichern) • Cloud Anwendungen (Nutzung von Anwendungen, die cloudbasiert funktionieren. Eine Installation in unserem IT System ist nicht notwendig.)

BEREICH	BESCHREIBUNG	BEISPIEL
Andere Formen von gespeicherten Informationen	Beispiele dafür sind Papierunterlagen, das persönliche Know-how von Mitarbeitern, Ausdrucke etc.	• Lieferantenverträge • Arbeitsverträge • Antragsformulare (auf Papier) • Patente • Anmeldeformulare (auf Papier)

Wir empfehlen Ihnen die Nutzung der Tabelle „IT-Systeme – Software und Anwendungen – Büroausstattung – Produktionsanlagen – Kommunikationsleitungen“, die Sie in **Kapitel J**, **Paragraph J4b** „Wiederaufbauplan für Ihre Ressourcen“ des Anhangs **18.3 Vorlage Plan für die Sicherstellung des Geschäftsbetriebes** finden, um die Informationsbestände Ihres Unternehmens zu dokumentieren (weitere Informationen dazu auch in Kapitel **13.11.6 Aktivität 5: Bereiten Sie einen Wiederaufbau für einzelne Ressourcen vor**). Nutzen Sie die erste Spalte der Vorlage, um all Ihre Informationsbestände zu dokumentieren.

IKT Systeme sind speziellen Risiken ausgesetzt:

(a) Risiken im normalen Geschäftsbetrieb (z. B. geringe oder schlechte Leistung, Ausfälle, Leistungsabfälle etc.).

(b) Risiken im Zusammenhang mit dem Thema Informationssicherheit, für deren Identifizierung und Verständnis eine gewisse Expertise vorhanden sein muss.

Beide Risikobereiche diskutieren wir hier nacheinander. Darüber hinaus widmet sich ein gesonderter Abschnitt dem Spezialthema „Cyber Risiken“.

10.2.4.2. IT Infrastruktur und Risiken im normalen Geschäftsbetrieb

Diese Risiken beziehen sich auf das IKT System Ihres Unternehmens und die Art und Weise wie es (a) konzipiert, angeschafft und implementiert wurde, sowie (b) wie es aktuell arbeitet und administriert wird.

Wie identifiziert man diese Risiken? Am besten Sie nehmen die Liste Ihrer gesamten Informationsbestände zur Hand und sortieren die Risiken in vier Dimensionen:

(a) Organisatorische und betriebliche Dimension: (Risiken und Bedrohungen identifizieren, die sich darauf beziehen, wie Sie Ihre IKT Systeme und deren Betrieb verwalten).

Hier ein paar Beispiele:

- Die Qualität und Menge der bestellten und gelieferten Geräte wurde weder in der Vergangenheit, noch in der Gegenwart kontrolliert.
- Bestehende Anwendungen (ERP, Office-Anwendungen etc.) sind unzureichend für die Anforderungen des Unternehmens, da deren Spezifikationen bei der Beschaffung nicht genau festgelegt wurden.
- Die Anwendungen wurden ohne Benutzerleitfäden geliefert (sie wurden entweder nicht angefordert oder existieren nicht).
- Die Einarbeitung in die Nutzung der IKT Systeme ist unzureichend und daraus resultieren regelmäßige Anwendungsfehler. Neue Mitarbeiter werden nicht angemessen geschult.
- Die IKT Systeme werden nicht nach den Anweisungen des Herstellers gewartet.
- Da es keinen Problemlösungsprozess im Unternehmen gibt, wissen die Mitarbeiter nicht, wie sie technische Probleme beheben oder die Leistung ihrer IKT Systeme verbessern können.
- …

(b) Technische Dimension: (Risiken und Bedrohungen identifizieren, die sich auf die technischen Spezifikationen des IKT Systems und dessen Nutzung beziehen).

Hier ein paar Beispiele:

- Die gekauften IKT Geräte haben eine mindere Qualität.
- Datenkommunikationsleitungen (z. B. Internet) weisen eine schlechte Verbindungsqualität auf oder lassen nur eine niedrige Übertragungs-Geschwindigkeit zu, die nicht den Anforderungen des Unternehmens entspricht.
- Es fehlen ausreichende Kontrollfunktionen in der Software und Ihre Applikationen lassen eine automatische Überprüfung der Qualität der eingegebenen Daten nicht zu.
- Die Anschaffung von qualitativ minderwertigen Druckerpatronen führt dazu, dass Ihre Drucker Störungen aufweisen.
- …

(c) Physische Dimension: (Risiken und Bedrohungen identifizieren, die sich auf die physische Installation im Gebäude des Unternehmens beziehen).

Hier ein paar Beispiele:

- Server und wichtige IT Komponenten werden in unterschiedlichen Räumen des Gebäudes aufbewahrt.
- Die Seitenwände der Serverkästen werden nach der Wartung offengelassen. Sie werden so z. B. Staub oder Feuchtigkeit ausgesetzt.
- Netzwerkkabel werden ungeschützt und quer verstreut verlegt.
- …

(d) Menschliche Dimension: (Risiken identifizieren, die sich auf menschliche Beteiligung zurückführen lassen).

Hier sind ein paar Beispiele:

- Es passieren Fehler in der täglichen Arbeit als Ergebnis von unzureichend geschulten Mitarbeitern.
- Menschliche Fehler, z. B. Eingabe und Verarbeitung von inkorrekten Daten, Löschung von Daten oder nachlässiges Entsorgen von Papierdokumenten, Öffnen von virenbefallenen E-Mail-Anhängen etc.
- …

10.2.4.3. Informationssicherheits-Risiken

Das Thema Informationssicherheit betrifft den Schutz der Informationen und der Informationsbestände eines Unternehmens. Bespiele für Informationen und Informationsbestände sind elektronisch gespeicherte Daten, z. B. auf Datenträgern oder CD; IT Systeme, die Daten und Informationen speichern und verarbeiten; Kommunikationssysteme, die Daten zwischen Ihren Systemen übertragen; IT Anwendungen, wie beispielsweise ERP und E-Mail; Papierdokumente und Archive, die in Ihren Geschäftsräumen gelagert werden. Eigentumsrechte, Unternehmensgeheimnisse und Patente gehören ebenfalls dazu.

Um Ihre Informationsbestände zu schützen und Informationssicherheit zu gewährleisten, müssen Sie die folgenden drei elementaren Charakteristika kennen und sicherstellen:

- **Vertraulichkeit**: Informationen dürfen unbefugten Personen, Einrichtungen oder Geschäftsprozessen nicht zugänglich gemacht werden oder an diese weitergegeben werden.
- **Integrität**: Es muss sichergestellt sein, dass Informationen unverändert und vollständig zur Verfügung stehen, insbesondere der Schutz der Informationen vor unerlaubten oder unbemerkten Änderungen oder Löschungen.
- **Verfügbarkeit**: Schutz von Informationen und Sicherstellung, dass sie bei Bedarf verfügbar sind.

Informationssicherheit aufrechtzuerhalten bedeutet am Beispiel Ihrer ERP-Daten, dass die Vertraulichkeit der Daten erstens geschützt ist (keine Informationen werden an Unbefugte weitergegeben), zweitens die Integrität der Daten gewährleistet wird (keine absichtliche oder unabsichtliche Änderung oder Löschung ohne ordnungsgemäße Ermächtigung) und drittens die Verfügbarkeit der Daten gegeben ist (Daten und IT Systeme sollten jederzeit verfügbar sein, egal ob es zu Systemausfällen kommt oder ein Feuer Ihr Gebäude zerstört).

Informationssicherheits-Risiken und -Bedrohungen gefährden also die Vertraulichkeit, Integrität und Verfügbarkeit der Informationsbestände Ihres Unternehmens.

Um sich umfassend mit den Risiken und Schwachstellen Ihres IKT Systems auseinanderzusetzen, nutzen wir erneut die oben bereits skizzierten vier Dimensionen:

(a) Organisatorische und betriebliche Dimension: (Risiken und Bedrohungen identifizieren, die sich darauf beziehen, wie Sie Ihre IKT Systeme und deren Betrieb verwalten).

Hier ein paar Beispiele:

- Niemand in Ihrem Unternehmen ist für Sicherheitsprobleme Ihres Unternehmens zuständig.
- Es gibt keine Regelungen oder Entscheidungen Ihres Managements darüber, wer auf ERP- oder E-Mail-Anwendungen zugreifen darf.
- Niemand kümmert sich um die Löschung eines Benutzers oder die Löschung der Zugriffsrechte im ERP System, wenn ein Mitarbeiter das Unternehmen verlässt.
- Es hat noch nie eine Risikobewertung stattgefunden.
- Mitarbeiter werden nicht mit dem Thema Phishing vertraut gemacht bzw. wie sie damit umgehen sollen.
- Es wird kein Back-Up von IT Daten erstellt.
- Mitarbeiter teilen Kollegen ihre Passwörter mit, um so (ihres Erachtens) produktiver zu arbeiten.
- Es gibt keinen Plan zur Sicherstellung des Geschäftsbetriebes.
- …

(b) Technische Dimension: (Risiken und Bedrohungen identifizieren, die sich auf die technischen Spezifikationen des IKT Systems und dessen Nutzung beziehen).

Hier ein paar Beispiele:

- Einige veraltete Anwendungen sind weiter in Verwendung, was zu Sicherheitslücken führt.
- Das unternehmensinterne W-LAN ist für alle Mitarbeiter, Nachbarn, Besucher und Passanten ungeschützt verfügbar.
- Es werden keine Software-Updates durchgeführt.
- Back-Up Datenträger werden nicht verschlüsselt, bevor sie das Bürogebäude verlassen.
- Es gibt keinen Spam-Filter für eingehende E-Mails.
- Mitarbeiter haben Zugriff auf alle Websites, wie Online-Spiele, Online-Casinos und pornografische Inhalte.
- Jeder kann von zu Hause aus auf die Systeme des Unternehmens zugreifen.
- Es gibt keine Back-Ups, um unabsichtlich gelöschte Daten wieder-herzustellen.
- …

(c) Physische Dimension: (Risiken und Bedrohungen identifizieren, die sich auf die physische Installation im Gebäude des Unternehmens beziehen).

Hier ein paar Beispiele:

- Bildschirme von Computern oder Laptops werden nicht gesperrt. Sie befinden sich teilweise im Besucherbereich, sodass externe Personen Informationen auf den Bildschirmen einsehen können.
- Niemand weiß, welche Geräte zum IKT System des Unternehmens gehören. Es gibt kein Verzeichnis aller Geräte.
- USB Sticks werden ungeschützt im Besucherbereich liegen gelassen.

- Wichtige und vertrauliche Dokumente werden auf den Schreibtischen liegen gelassen, weil es keine Möglichkeit gibt, diese sicher aufzubewahren (z. B. verschließbare Schreibtischschubladen).
- Es gibt keinen Einbruchsalarm, der außerhalb der Geschäftszeiten für mehr Sicherheit sorgt.
- Alle (auch ehemalige) Mitarbeiter haben Schlüssel für Büroräume.
- Kabel liegen ungeschützt auf dem Boden, bzw. um Tische herum oder im Flur.
- …

(d) Menschliche Dimension: (Risiken identifizieren, die sich auf menschliche Beteiligung zurückführen lassen).

Hier ein paar Beispiele:

- Unehrliche Mitarbeiter und Betrug: Mitarbeiter stehlen Daten oder vertrauliche Informationen für persönliche Zwecke (z. B. für Wettbewerber).
- Mutwillige Änderung von Daten (auch Löschung oder das Hinzufügen von Daten).
- Illegale Datenmanipulation zum Beispiel, um Abmahnungen zu vermeiden. Ein weiteres Beispiel wäre die Änderung von Finanzberichten, um behördliche Bußgelder zu vermeiden.
- Mutwillige Installation von bedrohlichen oder illegalen Anwendungen im IT System des Unternehmens.
- Unbewusste oder unbeabsichtigte Offenlegung von vertraulichen Unternehmensdaten durch Mitarbeiter in Social-Media-Kanälen. Beispielsweise ein Mitarbeiter, der stolz Details über ein wichtiges Projekt, an dem er beteiligt war, mit seinen Freunden teilt.
- …

Manche Risiken passen in mehrere Dimensionen. Es reicht aus, sie einmal zu erfassen, solange sichergestellt ist, dass man sich später angemessen mit dem Risiko beschäftigt.

10.2.4.4. Spezifische Informationssicherheitsrisiken: Cyber Risiken

„Cyber Risiken“ sind Risiken, die auf den Ausfall oder eine Beeinträchtigung des IT Systems eines Unternehmens zurückzuführen sind. Die Folgen sind z. B. finanzieller Verlust, Störung/Unterbrechung des Betriebsablaufes oder negative Auswirkungen auf die Unternehmensreputation.

Das Internet, die Verfügbarkeit von öffentlichen Netzen, die Verbindungen von IKT Systemen, die Speicherung von persönlichen und wertvollen Informationen in IT Systemen, die wachsende Abhängigkeit der Unternehmen von IKT Systemen, die Nutzung der persönlichen Geräte Ihrer Mitarbeiter im unternehmensinternen Netzwerk (Smartphones, Laptops, Tablets), Globalisierung, Soziale Netzwerke und nicht zu vergessen Spiele wie Pokémon Go: Das alles erschafft eine Welt, die tagtäglich komplizierter wird und Informationssicherheit zu einer großen Herausforderung für Unternehmen jeder Größe macht. Unternehmen verlassen sich immer mehr auf cloudbasierte Lösungen, sie nutzen Websites für E-Commerce und E-Business oder Online-Dienstleistungen von anderen Unternehmen oder wickeln ihren Zahlungsverkehr elektronisch ab.

All diese Aspekte machen IKT Systeme so attraktiv für kriminelle Aktivitäten wie den Diebstahl von Daten, illegale Zugriffe auf Informationen, Betrug, Erpressung, Sabotage und viele andere Cyber-Verbrechen bis hin zur Lahmlegung ganzer Systeme. Dies alles geschieht durch „Hacker“.

„Hacker“ sind Menschen oder Programme, die nach Schwachstellen in Computersystemen oder Netzwerken suchen, um diese auszunutzen.

Ihre Motivation ist:

- Profit (Datendiebstahl, speziell von persönlichen Informationen; Geld; geistiges Eigentum; Erpressung von Unternehmen und deren Kunden; Spionage für Wettbewerber etc.)
- Protest („Hacktivisten“, die damit politische oder ideologische Ziele erreichen wollen)
- Ruhm (z. B. in das System der CIA einbrechen, um Bekanntheit zu erlangen)
- Nationale Interessen (Spionage durch ausländische Regierungen)

- Spaß
- Diverse weitere Beweggründe (darunter auch durchaus legale Motive, wie das absichtliche Eindringen in ein IT-System, um im Auftrag eines Unternehmens dessen Schwachstellen aufzuspüren)

Hacker nutzen viele verschiedene Werkzeuge und Methoden, u. a.:

- Malware bzw. bösartige Software: Dazu gehören Software-Codes wie Viren, Spyware, Trojaner, Würmer und Ransomware. Malware wurde entwickelt, um Daten zu stehlen oder zu zerstören, Benutzer auszuspionieren, Systeme kriminell auszubeuten oder Geld von ihren Opfern zu erpressen.
- Phishing: Hacker senden Betrugs-E-Mails, um persönliche und finanzielle Informationen vom Empfänger zu erlangen.
- Spear Phishing: Hierbei handelt es sich um eine gezieltere Form des Phishings mit Zielpersonen, die angegriffen werden, um persönliche oder finanzielle Informationen zu erbeuten.
- Denial of Service (DoS) Angriffe: Hacker greifen das Zielsystem an (normalerweise eine Website), blockieren das System und verursachen dadurch einen Stillstand.
- Software Sicherheitslücken: Sicherheitslücken bei einer Software als Ergebnis von Programmierung-Fehlern. Diese Schwachstellen können von Hackern ausgebeutet werden, um Zugriff auf ein System zu erlangen, Daten zu stehlen oder andere böswillige Aktivitäten umzusetzen.
- Änderung der Internet-Inhalte: Hacker greifen Websites an und ändern deren Inhalte, z. B. um den Ruf eines Unternehmens zu schädigen.
- Unangemessene oder böswillige Internet-Inhalte: Hacker greifen Websites an, um diese zu kontrollieren und für weitere Angriffe zu nutzen. Kompromittierte Websites können für Phishing-Attacken genutzt werden, z. B. um Malware oder andere unangemessene Inhalte zu verbreiten.

Es ist wichtig, sich bewusst zu machen, dass Cyber-Risiken nicht immer aus einer unbekannten Quelle stammen müssen. Risiken für das IKT System Ihres Unternehmens können genauso gut von vertrauten Personen oder Unternehmen bzw. von

den IKT Systemen Ihrer Geschäfts- oder Vertriebspartner ausgehen, ganz einfach, weil diese gehackt wurden.

Jedes Unternehmen, selbst wenn Sie nur einen einzigen PC benutzen, muss diese Risiken beachten.

10.2.4.5. Zusammenfassung

Dieses Kapitel folgte einem tiefergehenden, analytischen Ansatz, denn IT- und Informationssicherheitsrisiken sind Themen, bei denen es in normalen KMU an internem Know-how mangelt. Um sich damit angemessen auseinanderzusetzen, ist viel gesunder Menschenverstand notwendig und ggf. die externe Unterstützung durch einen IT-Experten, z. B. Ihr IT-Berater oder der Anbieter Ihres IKT-Systems. Wenn Sie einen externen IT-Berater hinzuziehen, dann seien Sie sich bewusst, dass diese Geschäftsbeziehung ebenfalls Abhängigkeiten und damit neue Risiken schafft.

Eine unvollständige Liste der wichtigsten Themen, die Sie während der Identifizierung Ihrer Risiken beachten sollten, beinhaltet u. a.:

- Unabsichtliches Löschen von Daten
- Falsche Erfassung von Daten
- Arbeitsplätze oder Computer, auf die ohne Passwörter zugegriffen werden kann
- Unzureichende oder nichtexistierende Software-Lizenzen
- Unzureichende Schulung von neuen oder befristeten Mitarbeitern
- Notwendigkeit, auf wichtige Dateien zuzugreifen, während ein Mitarbeiter abwesend ist und die Dateien nur auf dessen Computer zugänglich sind
- Den Nutzen verlorene oder falsch abgespeicherte Dateien
- Verlorene Mobilgeräte
- Versand eines PC zur Reparatur an Externe, obwohl auf der Festplatte interne Daten des Unternehmens gespeichert sind
- Unzureichende Dokumentation für Nutzer und Administratoren

- Abstürze von Anwendungen (durch Software- oder Hardware-Probleme, menschliches Versagen, etc.)
- Versagen von wichtigem Computerzubehör
- Kommunikationsprobleme z. B. aufgrund einer defekten Telefonanlage
- Hardware-Fehlfunktionen
- Negativer Einfluss von Stromausfällen auf Informationen und Daten
- Versagen von Geräten
- Verfälschte oder fehlerhafte Dokumente und Dateien durch neue bzw. aktualisierte Software
- Software-Probleme
- Eingeschränkte Verfügbarkeit von Programmen oder Daten aufgrund von Software Updates
- Kein Zugriff auf Dateien auf PC aufgrund von Festplattenfehlern
- Mangelhafte Back-Ups (z. B. Unsicherheit darüber, was gesichert wurde) oder gar keine Back-Ups
- Back-Ups, die nie überprüft werden
- Back-Up-Medien, die nie überprüft werden
- Back-Ups, die nur in den Geschäftsräumen aufbewahrt werden
- Schlechte Programmierung
- Systeme oder Geräte sind nicht verfügbar
- Nicht erlaubte Transaktionen werden durchgeführt
- Informationen sind für das Putzpersonal außerhalb der Geschäftszeiten offen zuganglich
- Geschäftsräume oder Informationen sind für ehemalige Mitarbeiter zugänglich
- Vertrauliche oder eingeschränkte Bereiche sind für unbefugte Parteien zugänglich
- Physische Offenlegung von vertraulichen Informationen

- Physisches Eindringen von Unbefugten
- Unzureichende Sicherheit am Arbeitsplatz
- Inkorrekter oder unangemessener Dateizugriff von Mitarbeitern
- Fälschung von Dokumenten, die zur Genehmigung übermittelt werden
- Betrügerische Programmierung, welche die Datenintegrität beeinflusst
- Zugriff auf böswillige Internetseiten
- Hacking
- Phishing
- Computerviren
- Berichte werden an unberechtigte oder unbeabsichtigte Parteien übermittelt
- Denial-of-Service Angriffe (auf die Website des Unternehmens)
- E-Mail Sicherheit
- Passwörter werden Kollegen mitgeteilt
- Vertrauliche Informationen werden während Diskussionen mitgeteilt
- Interner Diebstahl von Informationen
- Network Sniffing
- Cyber Angriffe
- Erbeutung von System-Benutzernamen und Passwörtern
- Vertrauliche Informationen werden zwischen Boten und Mitarbeitern ausgetauscht
- Vertrauliche Informationen werden von Boten übermittelt
- Offsite-Datenspeicherung ist nicht verschlüsselt und wird kompromittiert
- Unzureichende Firewall-Konfiguration
- Identitätsdiebstahl (in verschiedenen Formen: Kunden, Lieferanten, Mitarbeiter etc.)
- Informationen werden von ehemaligen Mitarbeitern verändert

- Inbetriebnahme von nicht genehmigten Software-Programmen, was zu schwerwiegenden Problemen im IT-System führt
- Versuche, das betriebsinterne Netzwerk zu zerstören oder zu sabotieren
- Mitnahme von vertraulichen Informationen außerhalb der Geschäftsräume
- IT-Dienstleister sind aufgrund interner Probleme nicht verfügbar
- Beim IT-System Abhängigkeit vom Know-how einzelner Personen
- Dritte (z. B. Händler), die Support für das IT-System zur Verfügung stellen, können auf vertrauliche Informationen zugreifen

10.2.5. Behördliche und rechtliche Risiken

Diese Risiken beziehen sich auf das behördliche und rechtliche Umfeld eines Unternehmens, sowie auf die Anforderungen, die ein Unternehmen aufgrund von Rechtsvorschriften einhalten muss. Risiken entstehen in diesem Fall normalerweise, wenn Regulierungsbehörden die derzeitige Gesetzeslage ändern oder neue Regeln einführen, die das Unternehmen negativ beeinflussen.

Eine unvollständige Liste wichtiger Themen, die Sie während Ihrer Identifizierung beachten sollten, beinhaltet u. a.:

- Einhaltung rechtlichen Vorschriften (in Ihrem Geschäftsbereich)
- Einhaltung behördlicher Vorschriften (in Ihrem Geschäftsbereich)
- Einhaltung der Arbeitsschutzgesetze (Feuerlöscher, Kennzeichnungen etc.)
- Vertragliche Risiken (Verträge mit Kunden und Lieferanten)
- Negative Gerichtsentscheidungen in laufenden Verfahren
- Pünktliche Erfüllung steuerlicher und staatlicher Anforderungen
- Änderungen von Verordnungen und Gesetzen

10.2.6. Risiken im Personalbereich

Diese Kategorie deckt alle Risiken ab, die sich auf den Personalbereich beziehen, also Themen wie Beschäftigung, Kompetenzen, Arbeitsschutz etc.

Eine unvollständige Liste wichtiger Themen, die Sie während Ihrer Identifizierung beachten sollten, beinhaltet u. a.:

- Die Verfügbarkeit von kompetenten Mitarbeitern im Unternehmen und auf dem Arbeitsmarkt
- Derzeitige Anzahl an Mitarbeitern
- Derzeitige Kompetenzen Ihrer Mitarbeiter
- Gesundheitsschutz und Sicherheit
- Unfälle am Arbeitsplatz
- Schutz bei Dienstreisen
- Mutterschutz
- Verlust von Mitarbeitern in Schlüsselpositionen (Krankheit, Kündigung etc.)
- Unangemessene oder unklare Beschäftigungsverhältnisse
- Unehrliche Mitarbeiter
- Vertretungsplanung (als Ersatz für nicht verfügbare Mitarbeiter)
- Gewalt am Arbeitsplatz
- Unzureichendes Training für die IKT Systeme des Unternehmens
- Unzureichendes Sicherheitstraining
- Unzureichendes Training bezüglich der Prozesse und Vorgänge im Unternehmen
- Grippepandemie
- Unzureichende Einhaltung von Sicherheitsvorschriften
- Kündigung oder (vorzeitiger) Ruhestand
- Streiks oder Arbeitsunruhen
- Geringe Arbeitsmoral oder Leistung

10.2.7. Management Risiken und Risiken durch Interessensvertreter

Diese Risiken beziehen sich auf:

(a) Die Art und Weise wie ein Unternehmen intern gemanagt und geführt wird.

(b) Die Art und Weise wie die Beziehungen mit Interessensvertretern bzw. Stakeholdern gemanagt werden (alle Akteure mit einem direkten oder indirekten Interesse an Ihrem Unternehmen, also Inhaber, Mitarbeiter, Kunden, Lieferanten, Behörden, lokale Bevölkerung, Medien, Banken oder andere Investoren oder Kreditgeber etc.).

Eine unvollständige Liste wichtiger Themen, die Sie während Ihrer Identifizierung beachten sollten, beinhaltet u. a.:

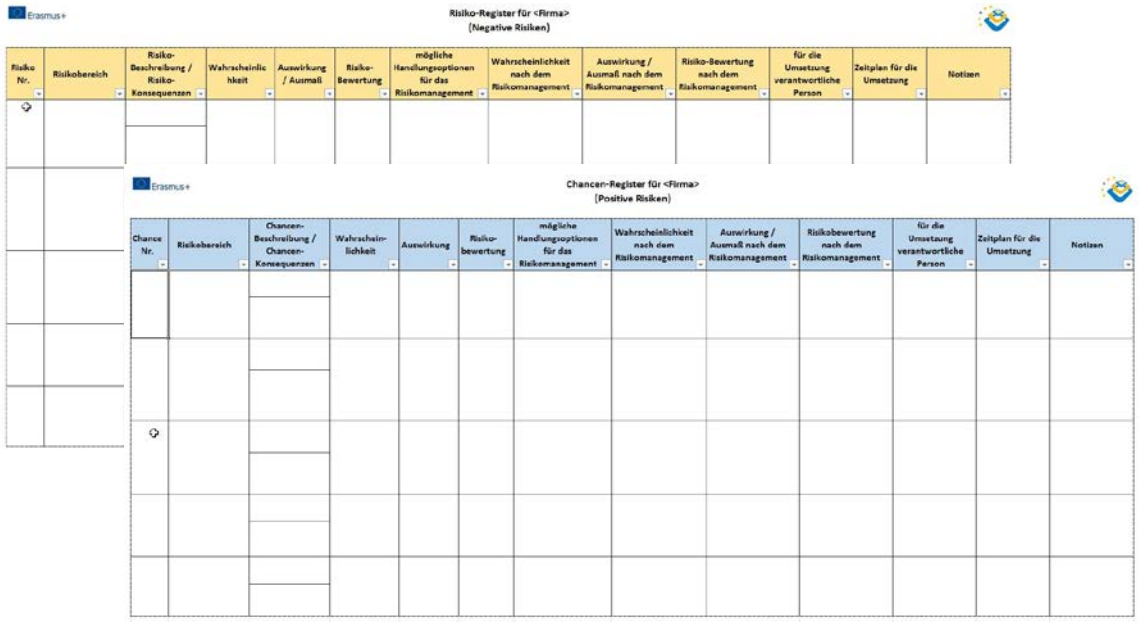
- Organisationsstrukturen und Organigramme
- Klare Rollen und Verantwortlichkeiten
- Management Wissen
- Management Fähigkeiten und Kompetenzen
- Genehmigungsprozesse (inklusive Zugriffsrechte auf die internen IKT Systeme)
- Schlechtes Management oder Mikro-Management
- Firmenpolitiken
- Fehlende Unternehmenswerte oder Prinzipien
- Bewertung und Management von Lieferanten und Händlern
- Interessen der Anteilseigner bzw. Aktionäre
- Interessen des Personals
- Kommunikation mit den Mitarbeitern
- Kundenverwaltung und -kommunikation (ggf. Abhängigkeit von einzelnen, wichtigen Kunden)
- Beziehungen zur lokalen Bevölkerung (insbesondere in der Nachbarschaft)

10.3. Systematisch und methodisch vorgehen

Um Ihre Risiken erfolgreich zu identifizieren, müssen Sie systematisch vorgehen und den einzelnen Schritten der CASSANDRA-Methode folgen. Wie Sie das am besten machen, erfahren Sie in den nächsten Kapiteln und Abschnitten.

10.3.1. Das wichtigste Dokument: Ihr Risikoregister

Sie benötigen ein Formular, in dem Sie alle Risiken dokumentieren können, die Sie identifizieren. Sie sollten dazu die Formularvorlagen (Excel) nutzen, die wir Ihnen in Ergänzung zu diesem Handbuch als Download zur Verfügung stellen.


Erasmus+

Risiko-Register für <Firma>
(Negative Risiken)

Risiko Nr.	Risikobereich	Risiko-Beschreibung / Risiko-Konsequenzen	Wahrscheinlichkeit	Auswirkung / Ausmaß	Risiko-Bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risiko-Bewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung	Notizen

Erasmus+

Chancen-Register für <Firma>
(Positive Risiken)

Chance Nr.	Risikobereich	Chancen-Beschreibung / Chancen-Konsequenzen	Wahrschein-lichkeit	Auswirkung	Risiko-bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risikobewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung	Notizen

In Ihrem Risikoregister erfassen Sie alle potenziellen Risiken, die Sie identifiziert haben. Das Register ermöglicht Ihnen, die Wahrscheinlichkeit und das Ausmaß bzw. die Auswirkungen für jedes einzelne Risiko zu erfassen und damit eine Gesamt-bewertung Ihrer Risiken vorzunehmen. Sie dokumentieren in der Tabelle darüber hinaus z. B. Ihre Handlungsoptionen, um die erkannten Risiken in Zukunft zu mindern oder am besten ganz ausschließen zu können.

In diesem Schritt nutzen Sie zunächst lediglich die ersten drei Spalten der Vorlage.

Spalte 1 = Risiko Nr.: jedes Risiko erhält eine laufende Nummer.

Spalte 2 = Risikobereiche bzw. -kategorien: die sieben Bereiche, die Sie bereits kennengelernt haben.

Spalte 3 = Risiko-Beschreibung/Risiko-Konsequenzen: dies ist die wichtigste Spalte. Hier beschreiben Sie das Risiko, das Sie identifiziert haben, in Ihren eigenen Worten und notieren alle Informationen, die in irgendeiner Weise wichtig sein könnten. Sie sollten darüber hinaus die angenommenen Konsequenzen, mit denen Ihr Unternehmen rechnen muss, dokumentieren, wenn das Risiko tatsächlich eintritt.

Sie können Ihre Risiken elektronisch oder handschriftlich erfassen. Drucken Sie die Vorlage gerne so häufig wie nötig aus. Wir empfehlen Ihnen jedoch, die elektronische Excel-Vorlage zu nutzen, da dies Ihre Arbeit in den folgenden Schritten sehr viel einfacher und angenehmer macht.

Sie wissen ja bereits, dass es negative UND positive Risiken gibt. Dementsprechend gibt es auch **zwei Risikoregister** – eines für die Erfassung der negativen Risiken (orange) und eines für die positiven Risiken bzw. Chancen (hellblau).

10.3.2. Zwischen Problemen und Risiken richtig unterscheiden

Bei der Identifizierung von Risiken kann es manchmal passieren, dass Sie aktuelle Probleme in Ihrem Unternehmen oder bereits bestehende Herausforderungen in Ihrem Betriebsalltag mit Risiken verwechseln.

Ein PROBLEM ist bereits aufgetreten und die damit verbundene Herausforderung ist Realität. Sie können die Auswirkungen auf die Ziele und die operative Arbeit Ihres Unternehmens bereits beobachten. Was schiefgehen konnte, ist also bereits schiefgegangen und verlangt nun nach einer Lösung, um die negativen Konsequenzen für Ihr Unternehmen zu reduzieren.

Ein RISIKO ist etwas, das in der Zukunft passieren könnte und einen Einfluss auf die Unternehmensziele und die operative Arbeit Ihres Unternehmens haben könnte. Es kann eintreten, muss aber nicht. Im Gegensatz zu einem bereits bestehenden Problem, können Sie für jedes Risiko einen Plan machen und Maßnahmen umsetzen, so dass dieses Risiko im besten Fall nicht mehr eintreten kann.

Anders ausgedrückt: Probleme sind bereits da und müssen gelöst werden. Risiken können vermieden werden und müssen nicht eintreten. Ein Risiko kann zu einem Problem für Ihr Unternehmen werden, aber ein Problem kann kein Risiko mehr sein, da es bereits Realität ist.

Die folgenden Sätze werden Sie bei der richtigen Identifizierung Ihrer Risiken unterstützen:

- **„Es besteht das Risiko, dass …….. . Falls das eintritt, ist die Konsequenz daraus ……. .“**
- **„Der Ausfall oder der Verlust des/von ……. wird folgende Konsequenz(en) haben: …….. .“**

z. B.

- Es besteht das Risiko, dass ein Feuer in unserem Bürogebäude ausbricht, wenn das Rauchen im Gebäude gestattet ist. Falls das eintritt, ist die Konsequenz daraus, dass das Gebäude niederbrennt und wir unsere Büros und unser gesamtes Inventar verlieren.
- Der Ausfall des IT Server Systems wird folgende Konsequenz(en) haben: unser gesamter Betrieb kommt zum Stillstand.

Sie müssen nicht immer den gesamten Satz aufschreiben. Notieren Sie einfach das Risiko und dessen Konsequenz(en):

RISIKO	**KONSEQUENZ(EN)**
Feuer im Büro wegen Rauchen im Gebäude	Verlust des Gebäudes und des Inventars; Stillstand des Betriebes
Versagen des IT Servers (z. B. aufgrund einer defekten Festplatte oder aufgrund eines Stromausfalls)	Kompletter Stillstand des Geschäftsbetriebes

10.3.3. Alleine arbeiten oder das Personal einbeziehen?

Obwohl Sie jetzt vielleicht denken, dass Sie Ihr Resilienz-Projekt mit der Unterstützung der CASSANDRA-Instrumente auch gut alleine umsetzen können, em-

pfehlen wir Ihnen sehr, Ihre Mitarbeiter in das Projekt mit einzubeziehen. Da Ihre Mitarbeiter über unterschiedliches Know-how und Spezialwissen verfügen, ist es fast sicher, dass sie einen wesentlichen Beitrag zur Identifizierung Ihrer Risiken leisten können. Außerdem ist es gut, die potenziellen Gefahren einzelner Risiken von mehreren Personen bewerten zu lassen. So vermeidet man eine Über- oder auch Unterschätzung der einzelnen Risiken bzw. Chancen.

Trotzdem können Sie sich (erst einmal) entscheiden, alleine weiter zu arbeiten, z. B. weil Sie schnell die ersten Fortschritte sehen möchten. Das ist völlig in Ordnung. Vielleicht sind Sie auch als Einzelperson (freiberuflich) selbständig. Alles was Sie hier erfahren, gilt auch für Ein-Personen-Unternehmen.

Wenn Sie aber Ihr Team einbeziehen möchten bzw. können, dann gehen Sie bitte folgendermaßen vor:

SCHRITT	BESCHREIBUNG	Erledigt
1	Organisieren Sie, wenn möglich, ein Kick-off-Meeting mit allen Mitarbeitern.	
2	Stellen Sie sicher, dass jeder Mitarbeiter das CASSANDRA Quick-Check-Tool genutzt hat (http://www.cassandra-resilience.eu/).	
3	Erklären Sie Risikomanagement und Resilienz mit Ihren eigenen Worten. Informieren Sie Ihre Mitarbeiter über die Ziele und die erwarteten Ergebnisse des Projekts: Ein widerstands- und anpassungsfähigeres Unternehmen, das für alle Beteiligten besser ist.	
4	Erklären Sie den Unterschied zwischen Risiken und bereits bestehenden Problemen (siehe oben), um gemeinsam effektiv und zeitsparend zu arbeiten.	
5	Stellen Sie kurz die sieben Risikokategorien bzw. -bereiche vor (siehe oben). Erklären Sie, dass Sie jede Kategorie separat nacheinander bearbeiten werden.	
6	Erklären Sie positive und negative Risiken.	
7	Zeigen (oder verteilen) Sie die beide Risikoregister.	

10.3.4. Beginnen Sie Ihre Risiken zu identifizieren

Brainstorming, egal ob alleine oder im Team, ist wahrscheinlich der beste Weg, um die Risiken Ihres Unternehmens systematisch zu identifizieren.

Fokussieren Sie sich auf jede einzelne Risikokategorie und bewerten Sie den Zustand Ihres Geschäftsbetriebes. Die folgenden Fragen können Ihnen helfen, Risiken zu identifizieren:

- Was könnte schiefgehen?
- Was könnte besser laufen?
- Was könnten wir falsch machen?
- Wo liegen unsere Schwachstellen?
- Welche Vermögenswerte müssen wir schützen?
- Wie könnte jemand unser Unternehmen bestehlen?
- Wie könnte jemand unseren Geschäftsbetrieb unterbrechen?
- Was könnte unseren Geschäftsbetrieb unterbrechen?
- Was passiert, wenn ich morgen nicht zur Arbeit kommen kann?
- Was passiert, wenn Mitarbeiter X das Unternehmen verlässt?
- Was passiert, wenn sich eine unserer Dienstleistungen extrem gut verkauft (weitaus besser, als wir uns bei der Planung erhofft hatten)?
- Auf welche Informationen und Informationssysteme sind wir am meisten angewiesen?
- Welche unserer Aktivitäten sind besonders wichtig? Was könnte diese beeinträchtigen?

Sie können sich z. B. auch auf jede einzelne Aktivität Ihres Unternehmens konzentrieren und überlegen, was schiefgehen oder verbessert werden könnte.

Risiken können darüber hinaus durch Vor-Ort-Besichtigungen identifiziert werden. Gehen Sie mit offenen Augen durch Ihr Bürogebäude, inspizieren Sie Ihre Umgebung und prüfen Sie, welche Risiken möglicherweise bestehen (Büro, Umgebung, benachbarte Gebäude etc.).

Falls Sie z. B. bereits eine SWOT-Analyse[11] für Ihre Dienstleistungen, Aktivitäten oder auch Ihre geschäftlichen Ziele durchgeführt haben, bieten die „Threats"- und die „Opportunities"-Spalten sehr gute Quellen für die Identifizierung von Risiken und von Chancen.

Eine weitere gute Quelle stellen diverse interne (Vertrags-)Dokumente dar. Interessant könnten u. a. die folgenden Unterlagen sein:

- (Miet-)Verträge für Anlagen/Gebäude sowie für outgesourcte Dienstleitungen
- Versicherungsverträge
- Dienstleistungsverträge mit Ihren Kunden
- Verträge mit wichtigen Geschäftspartnern und Lieferanten
- Dokumente über interne Richtlinien und Prozesse (z. B. ISO 9001 sofern vorhanden)

Nutzen Sie die beiden RISIKOREGISTER, um alle Risiken und Chancen zu dokumentieren, die Sie bis jetzt identifiziert haben (zu diesem Zeitpunkt nutzen Sie lediglich die ersten drei Spalten). Die Reihenfolge, in der Sie die Risiken und Chancen in den REGISTERN erfassen, spielt keine Rolle.

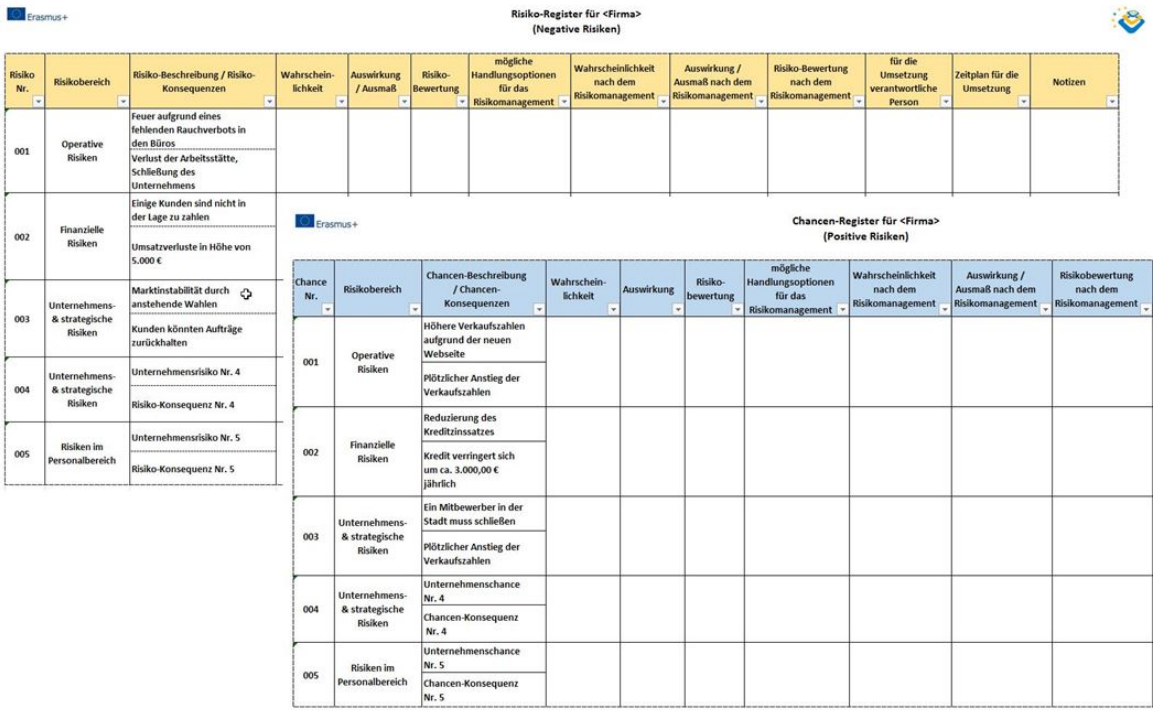
Sobald Sie fertig sind, werfen Sie noch einmal einen Blick auf Ihre Risiken und stellen sicher, dass Sie auch wirklich Risiken dokumentiert haben und keine bereits bestehenden Probleme (siehe oben). Ihre Risikoregister (sowohl positiv als auch negativ) sollten jetzt in etwa wie die untenstehenden Beispiele aussehen.

[11] Die SWOT-Analyse (engl. Akronym für Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen) und Threats (Bedrohungen)) ist ein Instrument der strategischen Planung.

Sie dient der Positionsbestimmung und der Strategieentwicklung von Unternehmen und anderen Organisationen. Identifiziert werden:

- Stärken: Merkmale vom Unternehmen, Projekten oder Produkten, die einen Vorteil gegenüber anderen darstellen
- Schwächen: Merkmale vom Unternehmen, Projekten oder Produkten, die einen Nachteil gegenüber anderen darstellen
- Chancen: Elemente im Umfeld vom Unternehmen, Projekten oder Produkten, die zum Vorteil genutzt werden können
- Bedrohungen: Elemente im Umfeld vom Unternehmen, Projekten oder Produkten, die zu Schwierigkeiten führen können

Mehr Informationen zum Thema SWOT-Analyse finden Sie z. B. hier: (https://de.wikipedia.org/wiki/SWOT-Analyse).



Risiko-Register für <Firma>
(Negative Risiken)

Risiko Nr.	Risikobereich	Risiko-Beschreibung / Risiko-Konsequenzen	Wahrschein-lichkeit	Auswirkung / Ausmaß	Risiko-Bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risiko-Bewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung	Notizen
001	Operative Risiken	Feuer aufgrund eines fehlenden Rauchverbots in den Büros Verlust der Arbeitsstätte, Schließung des Unternehmens										
002	Finanzielle Risiken	Einige Kunden sind nicht in der Lage zu zahlen Umsatzverluste in Höhe von 5.000 €										
003	Unternehmens- & strategische Risiken	Marktinstabilität durch anstehende Wahlen Kunden könnten Aufträge zurückhalten										
004	Unternehmens- & strategische Risiken	Unternehmensrisiko Nr. 4 Risiko-Konsequenz Nr. 4										
005	Risiken im Personalbereich	Unternehmensrisiko Nr. 5 Risiko-Konsequenz Nr. 5										

Chancen-Register für <Firma>
(Positive Risiken)

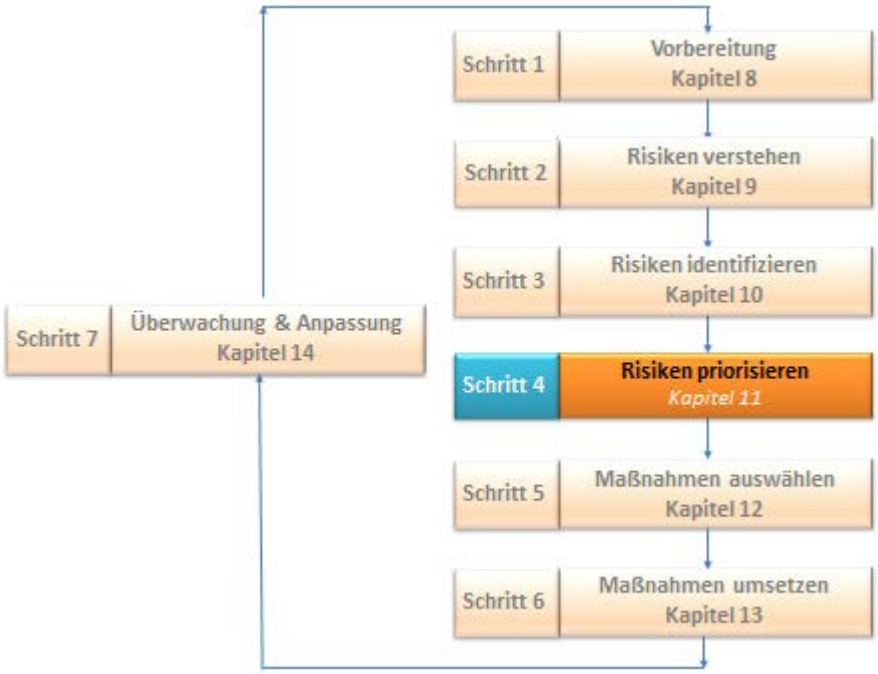
Chance Nr.	Risikobereich	Chancen-Beschreibung / Chancen-Konsequenzen	Wahrschein-lichkeit	Auswirkung	Risiko-bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risikobewertung nach dem Risikomanagement
001	Operative Risiken	Höhere Verkaufszahlen aufgrund der neuen Webseite Plötzlicher Anstieg der Verkaufszahlen							
002	Finanzielle Risiken	Reduzierung des Kreditzinssatzes Kredit verringert sich um ca. 3.000,00 € jährlich							
003	Unternehmens- & strategische Risiken	Ein Mitbewerber in der Stadt muss schließen Plötzlicher Anstieg der Verkaufszahlen							
004	Unternehmens- & strategische Risiken	Unternehmenschance Nr. 4 Chancen-Konsequenz Nr. 4							
005	Risiken im Personalbereich	Unternehmenschance Nr. 5 Chancen-Konsequenz Nr. 5							

10.3.4.1. Tipp zur Identifizierung von IKT- und Informationssicherheits-Risiken

Neben der bisher dargestellten Vorgehensweise zur Risikoidentifizierung sollten Sie bei der Identifizierung Ihrer IKT- bzw. Informationssicherheits-Risiken ggf. auch die folgenden Aspekte ergänzend berücksichtigen:

- Nutzen Sie die Auflistung Ihrer IKT Infrastruktur, die Sie in Kapitel **10.2.4 IT und Informationssicherheits-Risiken** erstellt haben.
- Identifizieren Sie Risiken, indem Sie die vier Dimensionen, die wir in den zwei Kapiteln „IT Infrastruktur und Risiken im normalen Geschäftsbetrieb“ und „Informationssicherheits-Risiken“ ausführlich diskutiert haben, für jede einzelne Anlage durchgehen.
- Nutzen Sie alle bereits zur Verfügung gestellten Listen mit den Beispielen möglicher Risiken, Bedrohungen und Schwachstellen.
- Analysieren Sie, welche Risiken die Vertraulichkeit, Integrität oder Verfügbarkeit Ihrer Informationsbestände gefährden.

11. Schritt 4 – Risiken priorisieren



Wenn Sie Schritt 3 abgeschlossen haben, steht Ihnen ein Risikoregister zur Verfügung, das bereits möglichst viele Ihrer Risiken beinhaltet. Das Dokument besteht normalerweise aus mehreren Seiten voll mit Risiken. Wenn Sie Ihr Risiko-register jetzt mit den Augen eines Managers ansehen, dann haben Sie bereits einen ersten guten Überblick Ihrer Risiken, vorerst jedoch, ohne dass die spezifischen Rahmenbedingungen Ihres Unternehmens berücksichtigt wurden.

Die Liste zeigt dem Management eines Unternehmens nicht,

- welches Risiko wichtig ist und welches nicht,
- welches Risiko mehr Aufmerksamkeit benötigt und welches eventuell übergangen werden kann und
- welches Risiko dringend ist und welches (erst einmal) aufgeschoben werden kann.

Wenn diese Fragen nicht beantwortet werden, können Sie nicht fundiert entscheiden, wie Sie auf Ihre Risiken reagieren sollen. Sollten Sie eher mit den ersten zehn Risiken beginnen, die Sie notiert haben, oder wäre es besser, die Risiken prioritär zu bearbeiten, die Sie persönlich für die wichtigsten halten? Und wie

gehen Sie mit der Tatsache um, dass Ihr Unternehmen normalerweise nicht über ausreichend finanzielle Mittel verfügt, um sich mit allen Risiken auseinander-zusetzen?

Sie werden wahrscheinlich schon erkannt haben, dass es unumgänglich ist, Ihre Risiken zu priorisieren. Nur so können Sie sich so schnell wie möglich um die wichtigsten Risiken kümmern und Ihre knappe Zeit und Ihre begrenzten Ressourcen sinnvoll einsetzen.

Für diese Priorisierung werden Sie zwei Faktoren eines jeden Risikos auswerten bzw. bestimmen: Die **Wahrscheinlichkeit**, dass ein Risiko tatsächlich eintritt, und das **Ausmaß bzw. die Auswirkungen**, wenn das Risiko eintritt.

11.1. Wahrscheinlichkeit

Die Wahrscheinlichkeit eines Risikos entspricht der angenommenen Häufigkeit eines Ereignisses in einem spezifischen Zeitraum.

Die Wahrscheinlichkeit des Auftretens eines negativen oder positiven Ergebnisses können wir normalerweise als statistischen Wert ausdrücken, der sich auf einen Zeitraum bezieht (z. B. die Wahrscheinlichkeit, dass ein bestimmtes Risiko innerhalb eines Jahres, innerhalb von 5 Jahren, 20 Jahren oder 100 Jahren auftritt).

Hier folgen einige Beispiele:

- Die Wahrscheinlichkeit eines Erdbebens mit der Stärke 5,5 oder höher auf der Richterskala liegt bei einem Erdbeben alle 20 Jahre in Athen, Griechenland.
- Die erwartete Anzahl von Überschwemmungen der Donau in Passau, Deutschland, liegt bei einer Überschwemmung alle 100 Jahre (auf Basis der historischen Daten von 1501 bis 2013).
- Auf Grundlage einer breiten Untersuchung von Computer-Laufwerken hat eine Studie von Google im Jahr 2007 ergeben, dass die jährlichen Ausfallraten

(geschätzte Wahrscheinlichkeit, dass ein Gerät oder eine Komponente während eines vollen Nutzungsjahres ausfällt) für einzelne Laufwerke zwischen 1,7 % für einjährige Laufwerke und über 8,6 % für dreijährige Laufwerke liegen.

Betrachtet man die Beispiele etwas genauer, dann fallen bei dieser Herangehensweise zwei Herausforderungen auf:

(a) Um die Wahrscheinlichkeiten korrekt berechnen zu können, werden teilweise umfassende statistische und historische Informationen benötigt. Große Unternehmen (wie z. B. international tätige Versicherungsunternehmen) sind selbstverständlich in der Lage, diese Informationen zu beschaffen, jedoch ist es eher unwahrscheinlich, dass ein Durchschnittsbürger, z. B. in der Person eines KMU Inhabers, Managers oder Angestellten den Zugang zu den entsprechenden Informationen hat bzw. die notwendigen Berechnungen statistisch korrekt durchführen kann.

(b) Statistisch gibt es einmal in 100 Jahren eine Überschwemmung in Passau:

1. Das schließt jedoch nicht aus, dass innerhalb der nächsten 100 Jahre zwei oder mehrere Überschwemmungen auftreten können.
2. Das bedeutet nicht, dass die nächste Überschwemmung erst in 99 Jahren auftritt, wenn die Donau im vergangenen Jahr über die Ufer getreten ist.

Es ist an dieser Stelle nicht Ihre Aufgabe, eine wissenschaftliche Analyse zu erstellen. Es muss reichen, wenn Sie Ihre Risiken einigermaßen fundiert priorisieren können. Sie werden weder Zugriff auf die statistischen Daten haben, die Ihnen 100 % Genauigkeit für Ihre Berechnungen versprechen, noch müssen Sie in der Lage sein, komplexe Wahrscheinlichkeitsberechnungen durchzuführen. Für Ihre Arbeit ist es in nahezu allen Fällen ausreichend, wenn Sie Ihren gesunden Menschenverstand nutzen, sowie gute Kenntnisse Ihres Geschäftsumfeldes besitzen und beides gemäß der im Folgenden präsentierten Herangehensweise anwenden.

Für eine brauchbare Risikopriorisierung ist es ausreichend, eine **Wahrscheinlichkeitsskala mit 3, 4, 5 oder mehr Abstufungen festzulegen**. Für die einzelnen Abstufungen der Skala können entweder Zahlenwerte und/oder Beschreibungen gewählt werden. Dies wird in der folgenden Tabelle verdeutlicht:

BEISPIEL FÜR EINE SKALA MIT 4 ABSTUFUNGEN

ABSTUFUNG		EINTRITTSWAHRSCHEINLICHKEIT
1	Unwahrscheinlich	Unter 7 % Nie aufgetreten oder könnte einmal in 15-20 Jahren auftreten
2	Möglich	Zwischen 8 % und 40 % Einmal alle 6-15 Jahre erwartet
3	Wahrscheinlich	Zwischen 41 % und 80 % Einmal alle 1-5 Jahre erwartet
4	Fast sicher	Über 80 % Mehr als einmal im Jahr erwartet

Alternativ

- Auf einer 3-Stufen Skala könnten die folgenden Werte genutzt werden:
  - 1 – Niedrig
  - 2 – Mittel
  - 3 – Hoch
- Auf einer 5-Stufen Skala könnten die folgenden Werte genutzt werden:
  - 1 – Fast unmöglich
  - 2 – Ziemlich unwahrscheinlich
  - 3 – Wahrscheinlich
  - 4 – Sehr wahrscheinlich
  - 5 – Nahezu sicher

In diesem Handbuch nutzen wir eine Skala mit 4 Abstufungen.

11.2. Ausmaß bzw. Auswirkung (Konsequenzen)

Das Ausmaß bzw. die Auswirkungen beziehen sich auf die voraussichtlichen Konsequenzen, die ein Risiko für das Unternehmen mit sich bringt, sollte es eintreten.

Die Konsequenzen für ein Unternehmen unterscheiden sich nicht nur in ihrem Ausmaß bzw. ihrer Auswirkung (z. B. hoch oder niedrig), sondern auch je nach betroffenem Geschäftsbereich:

- **Finanziell** (bedeutet finanziellen Verlust oder außerplanmäßige Kosten)
    - Umsatzverluste
    - Gewinneinbußen
    - Strafen und Bußgelder
    - Außerplanmäßige Kosten
    - Rückgang des Aktien- bzw. Anteilspreises
    - Verlust der Kreditwürdigkeit
    - Notwendigkeit zusätzlicher Kredite
    - …
- **Operativ** (bedeutet betrieblichen Stillstand von Teilen oder des gesamten Unternehmens):
    - Keine Möglichkeit, mit dem operativen Geschäft fortzufahren, oder Probleme, ausgewählte oder alle Dienstleistungen zu liefern
    - Geringe Leistung
    - Dienstleistungen mit niedriger Qualität werden erbracht
    - …
- **Arbeitsschutz** (betrifft die Gesundheit und Sicherheit von Mitarbeitern, Nachbarn, Kunden, Besuchern etc.):
    - Verletzung von Angestellten oder Besuchern

  - Unzureichende Sicherheitsbedingungen im Arbeitsumfeld
  - Geringes Wohlbefinden bei Mitarbeitern oder Besuchern
  - …
- **Renommee** (betrifft das Ansehen der Marke und die Reputation des Unternehmens):
  - Negative Berichte in den Medien
  - Hohe Anzahl von Kundenbeschwerden
  - Kunden verlieren das Vertrauen in die Dienstleistungen des Unternehmens
  - …
- **Rechtlich/Behördlich** (resultiert in der Unfähigkeit, behördlichen Anforderungen oder rechtlichen Vorschriften nachzukommen):
  - Rechtliches Vorgehen gegen das Unternehmen oder dessen Management
  - Verlust von Betriebsgenehmigungen oder Lizenzen
  - Ernstzunehmende Strafen
  - …
- **Personalwesen** (resultiert in Konsequenzen im Personalbereich):
  - Kündigungen
  - Niedrige Arbeitsmoral
  - Fehlende oder nicht verfügbare Mitarbeiter
  - …

Das Ausmaß bzw. die Auswirkungen eines eintretenden Risikos können nur einen Bereich (z. B. nur den Finanzbereich), eine Kombination aus mehreren Bereichen oder sogar alle Bereiche gleichzeitig betreffen.

Wie oben bei der Priorisierung ist es auch hier notwendig, eine **Auswirkungsskala festzulegen**, die 3, 4, 5 oder mehr Abstufungen aufweist. Für die einzelnen Abstufungen der Skala können entweder Zahlenwerte und/oder Beschreibungen gewählt werden. Dies wird in der folgenden **Beispieltabelle** verdeutlicht:

SKALA NEGATIVE RISIKOAUSWIRKUNG		
ABSTUFUNG		**AUSMASS bzw. AUSWIRKUNG (KONSEQUENZEN)**
1	Unerheblich	Arbeitsschutz: keine Auswirkung Finanziell: Verlust von weniger als 500 € Operativ: Betrieb für weniger als einen Tag unterbrochen Renommee: keine Auswirkung Behördlich/Rechtlich: keine Auswirkung
2	Gering	Arbeitsschutz: Erste Hilfe Behandlung notwendig Finanziell: Verluste zwischen 500 € und 2.500 € Operativ: Betrieb für 1-2 Tage unterbrochen Renommee: nur wenige unzufriedene Kunden Behördlich/Rechtlich: unerhebliche Nichteinhaltung von regulativen Anforderungen
3	Wesentlich	Arbeitsschutz: medizinische Behandlung benötigt Finanziell: Verluste zwischen 2.500 € und 10.000 € Operativ: Betrieb für 3-5 Tage unterbrochen Renommee: einige unzufriedene Kunden; geringe negative Berichterstattung in den Medien Behördlich/Rechtlich: signifikante Nichteinhaltung wichtiger regulativen Anforderungen; Klagen gegen den Inhaber bzw. gegen das Unternehmen
4	Gravierend	Arbeitsschutz: Tod oder schwerwiegende Verletzungen Finanziell: Verlust von mehr als 10.000 € Operativ: Betrieb für mehr als 5 Tage unterbrochen Renommee: viele unzufriedene Kunden; breitere negative Berichterstattung in den Medien Behördlich/Rechtlich: längerfristige bzw. permanente Nichteinhaltung wichtiger regulativen Anforderungen; Verlust der Betriebserlaubnis; multiple Klagen gegen den Inhaber bzw. gegen das Unternehmen

Die folgende Tabelle kann für die positiven Risikoauswirkungen verwendet werden:

SKALA POSITIVE RISIKOAUSWIRKUNG (MÖGLICHKEITEN)		
ABSTUFUNG		**AUSMASS bzw. AUSWIRKUNG (KONSEQUENZEN)**
1	Unerheblich	Arbeitsschutz: keine Auswirkung Finanziell: unerwartete Verkäufe oder Einsparungen unter 1.000 € Operativ: keine Auswirkung Renommee: keine Auswirkung Behördlich/Rechtlich: keine Auswirkung
2	Gering	Arbeitsschutz: keine Auswirkung Finanziell: unerwartete Verkäufe oder Einsparungen zwischen 1.000 € und 10.000 € Operativ: Arbeitsprozesse um 5 % verbessert (ermöglicht zusätzliche Umsätze) Renommee: positives Feedback von einigen Kunden Behördlich/Rechtlich: keine Auswirkung
3	Wesentlich	Arbeitsschutz: keine Auswirkung Finanziell: unerwartete Verkäufe oder Einsparungen zwischen 10.000 € und 30.000 € Operativ: Arbeitsprozesse um 20 % verbessert (ermöglicht zusätzliche Umsätze) Renommee: positives Feedback von mehreren Kunden; etwas Berichterstattung in Blogs; einige zusätzliche Umsätze und eine überschaubare Anzahl neuer Kundenkontakte Behördlich/Rechtlich: für neue Verträge mit Kunden ist rechtliche Unterstützung notwendig
4	Bedeutend	Arbeitsschutz: keine Auswirkung Finanziell: unerwartete Verkäufe oder Einsparungen von über 30.000 € Operativ: Arbeitsprozesse um 70 % verbessert (ermöglicht zusätzliche Umsätze) Renommee: positives Feedback von vielen Kunden; umfassende Berichterstattung in den Medien; beträchtliche zusätzliche Umsätze und eine große Anzahl neuer Kundenkontakte Behördlich/Rechtlich: für neue Verträge mit Kunden ist umfassende rechtliche Unterstützung notwendig

In diesem Handbuch nutzen wir eine Skala mit vier Abstufungen und die obenstehende Tabelle.

11.3. Risiko-Bewertung

Jetzt wenden wir uns wieder den beiden Risikoregistern zu. Bitte bestimmen Sie vor dem Hintergrund der eben diskutierten Themen jetzt die Wahrscheinlichkeit und die potenzielle Auswirkung bzw. das Ausmaß für jedes Ihrer identifizierten Risiken.

Ihre positiven und negativen Risikoregister sollten danach ungefähr so aussehen:

Erasmus+

Risiko-Register für <Firma>
(Negative Risiken)

Risiko Nr.	Risikobereich	Risiko-Beschreibung / Risiko-Konsequenzen	Wahrschein-lichkeit	Auswirkung / Ausmaß	Risiko-Bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risiko-Bewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung	Notizen
001	Operative Risiken	Feuer aufgrund eines fehlenden Rauchverbots in den Büros Verlust der Arbeitsstätte, Schließung des Unternehmens	2	4								
002	Finanzielle Risiken	Einige Kunden sind nicht in der Lage zu zahlen Umsatzverluste in Höhe von 5.000 €	3	3								
003	Unternehmens- & strategische Risiken	Marktinstabilität durch anstehende Wahlen Kunden könnten Aufträge zurückhalten	2	2								
004	Unternehmens- & strategische Risiken	Unternehmensrisiko Nr. 4 Risiko-Konsequenz Nr. 4	1	4								
005	Risiken im Personalbereich	Unternehmensrisiko Nr. 5 Risiko-Konsequenz Nr. 5	3	2								

Erasmus+

Chancen-Register für <Firma>
(Positive Risiken)

Chance Nr.	Risikobereich	Chancen-Beschreibung / Chancen-Konsequenzen	Wahrschein-lichkeit	Auswirkung	Risiko-bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkun Ausmaß nach Risikomanage
001	Operative Risiken	Höhere Verkaufszahlen aufgrund der neuen Webseite Plötzlicher Anstieg der Verkaufszahlen	3	3				
002	Finanzielle Risiken	Reduzierung des Kreditzinssatzes Kredit verringert sich um ca. 3.000,00 € jährlich	2	2				
003	Unternehmens- & strategische Risiken	Ein Mitbewerber in der Stadt muss schließen Plötzlicher Anstieg der Verkaufszahlen	2	4				
004	Unternehmens- & strategische Risiken	Unternehmenschance Nr. 4 Chancen-Konsequenz Nr. 4	2	3				
005	Risiken im Personalbereich	Unternehmenschance Nr. 5 Chancen-Konsequenz Nr. 5	2	4				

Sie bewerten Ihre Risiken, indem Sie den Wert für die Wahrscheinlichkeit mit dem Wert für die Auswirkung multiplizieren:

Risiko-Bewertung = Wahrscheinlichkeit x Ausmaß bzw. Auswirkung

Nehmen Sie bitte wieder Ihre beiden Risikoregister zur Hand und dokumentieren die Ergebnisse dieser Multiplikation. Ihr Ergebnis sieht nun so aus:

Erasmus+

Risiko-Register für <Firma>
(Negative Risiken)

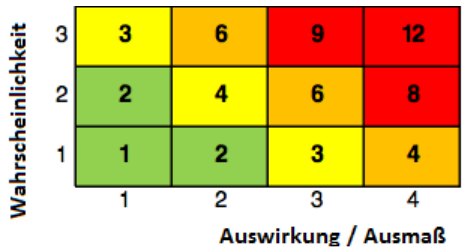
Risiko Nr.	Risikobereich	Risiko-Beschreibung / Risiko-Konsequenzen	Wahrschein-lichkeit	Auswirkung / Ausmaß	Risiko-Bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risiko-Bewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung
001	Operative Risiken	Feuer aufgrund eines fehlenden Rauchverbots in den Büros Verlust der Arbeitsstätte, Schließung des Unternehmens	2	4	8						
002	Finanzielle Risiken	Einige Kunden sind nicht in der Lage zu zahlen Umsatzverluste in Höhe von 5.000 €	3	3	9						
003	Unternehmens- & strategische Risiken	Marktinstabilität durch anstehende Wahlen Kunden könnten Aufträge zurückhalten	2	2	4						
004	Unternehmens- & strategische Risiken	Unternehmensrisiko Nr. 4 Risiko-Konsequenz Nr. 4	1	4	4						
005	Risiken im Personalbereich	Unternehmensrisiko Nr. 5 Risiko-Konsequenz Nr. 5	3	2	6						

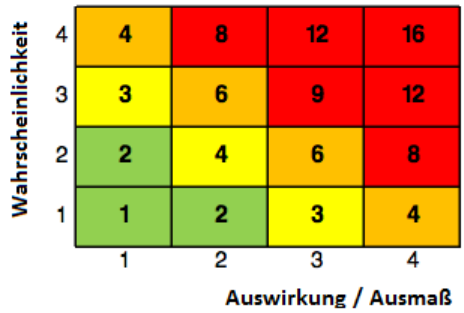
Erasmus+

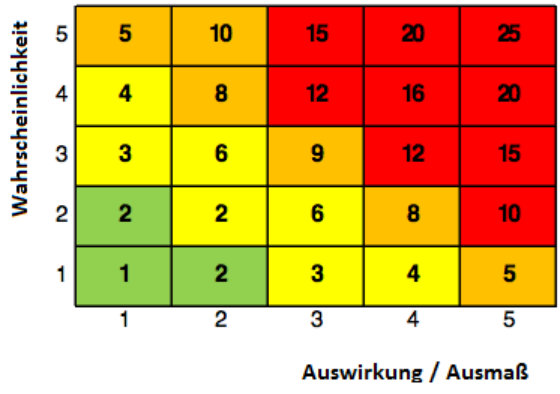
Chancen-R
(Posi

Chance Nr.	Risikobereich	Chancen-Beschreibung / Chancen-Konsequenzen	Wahrschein-lichkeit	Auswirkung	Risiko-bewertung	mögliche Handlungsoptione für das Risikomanagemen
001	Operative Risiken	Höhere Verkaufszahlen aufgrund der neuen Webseite Plötzlicher Anstieg der Verkaufszahlen	3	3	9	
002	Finanzielle Risiken	Reduzierung des Kreditzinssatzes Kredit verringert sich um ca. 3.000,00 € jährlich	2	2	4	
003	Unternehmens- & strategische Risiken	Ein Mitbewerber in der Stadt muss schließen Plötzlicher Anstieg der Verkaufszahlen	2	4	8	
004	Unternehmens- & strategische Risiken	Unternehmenschance Nr. 4 Chancen-Konsequenz Nr. 4	2	3	6	

11.4. Risikomatrix







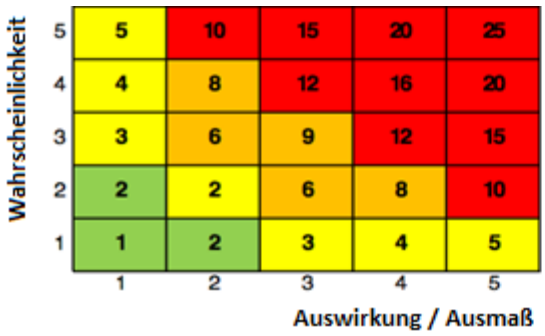
Eine Risikomatrix ist ein Raster in Anlehnung an das **Ampelsystem.** Die Matrix wird verwendet, um die Bewertung von Risiken besser zu visualisieren. Die Farben der Ampel zeigen die Relevanz der Risiken und vereinfachen dadurch Ihre Priorisierung. Die Skala geht von **Grün** (geringstes Risiko) bis **Rot** (schwerwiegendstes Risiko).

- **Rot** = Signifikante Risiken, die behandelt werden müssen (Hoch)
- **Orange** = weniger signifikante Risiken, die behandelt werden sollten (Moderat)
- **Gelb** = Mittlere Risiken, die eventuell behandelt werden (Niedrig)
- **Grün** = Unerhebliche Risiken, für die keine Ressourcen verwendet werden müssen, solange sie unverändert bleiben (Sehr niedrig)

Die Matrix ist eine Kombination aus der Wahrscheinlichkeits- und der Auswirkungsskala. Die Größe Ihrer Risikomatrix hängt ganz davon ab, wie groß die ursprünglichen Skalen sind, die Sie heranziehen. In den oben gezeigten Beispielen sehen Sie als erstes eine Risikomatrix mit einer dreistufigen Wahrscheinlichkeits-Skala kombiniert mit einer vierstufigen Auswirkungs-Skala. Beispiel zwei zeigt eine vierstufige Wahrscheinlichkeits-Skala kombiniert mit einer ebenfalls vierstufigen Auswirkungs-Skala. Im dritten Beispiel haben beide Skalen fünf Stufen.

Wenn wir uns die Matrix ansehen, können wir erkennen, dass die wichtigsten Risiken jene sind, die **sowohl eine hohe Eintrittswahrscheinlichkeit, als auch gravierende Auswirkungen aufweisen. Diese Risiken befinden sich in der oberen rechten Ecke der Matrix.**

Bitte beachten Sie: Risiken mit jeweils nur einem hohen Wert bei der Wahrscheinlichkeit (oberste Reihe) oder bei der Auswirkung (rechte Spalte) sind ebenfalls wichtig und erfordern Ihre Aufmerksamkeit.



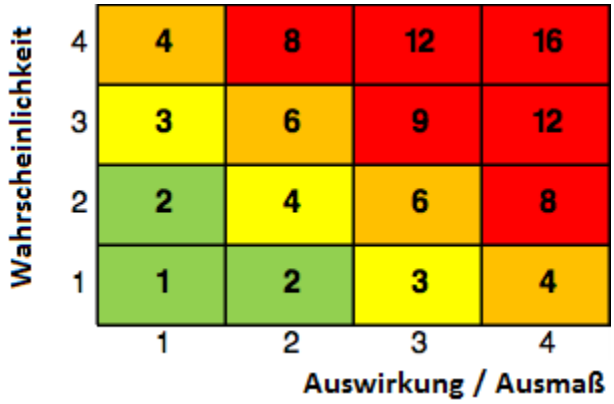
Je nach Ihrer individuellen Risikobereitschaft können Sie:

a) Auf Nummer Sicher gehen und wie im Beispiel oben links bereits Risiken ab einer Risiko-Bewertung von 10 als rot markieren.

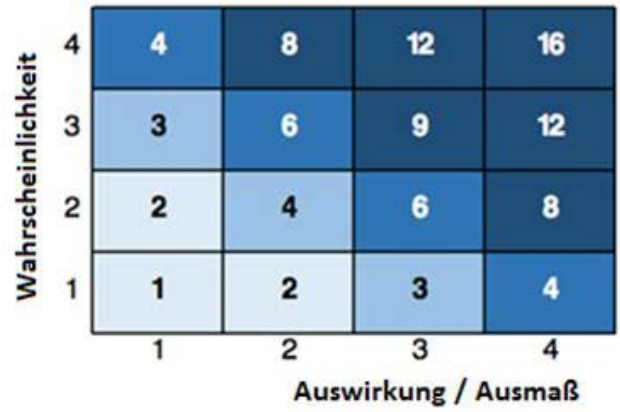
b) Die Sache wie im rechten Beispiel etwas entspannter angehen und eine höhere Risikobereitschaft zeigen, indem Sie alle Risiken mit einer Risiko-Bewertung von 3 oder geringer als unerheblich klassifizieren und erst ab einer Risikoeinstufung von 15 oder höher ein Risiko als rotes, also signifikantes Risiko kennzeichnen.

11.5. Risikopriorisierung

In diesem Handbuch nutzen wir eine 4 x 4 Risikomatrix, aufbauend auf den Skalen aus den vorherigen Kapiteln:



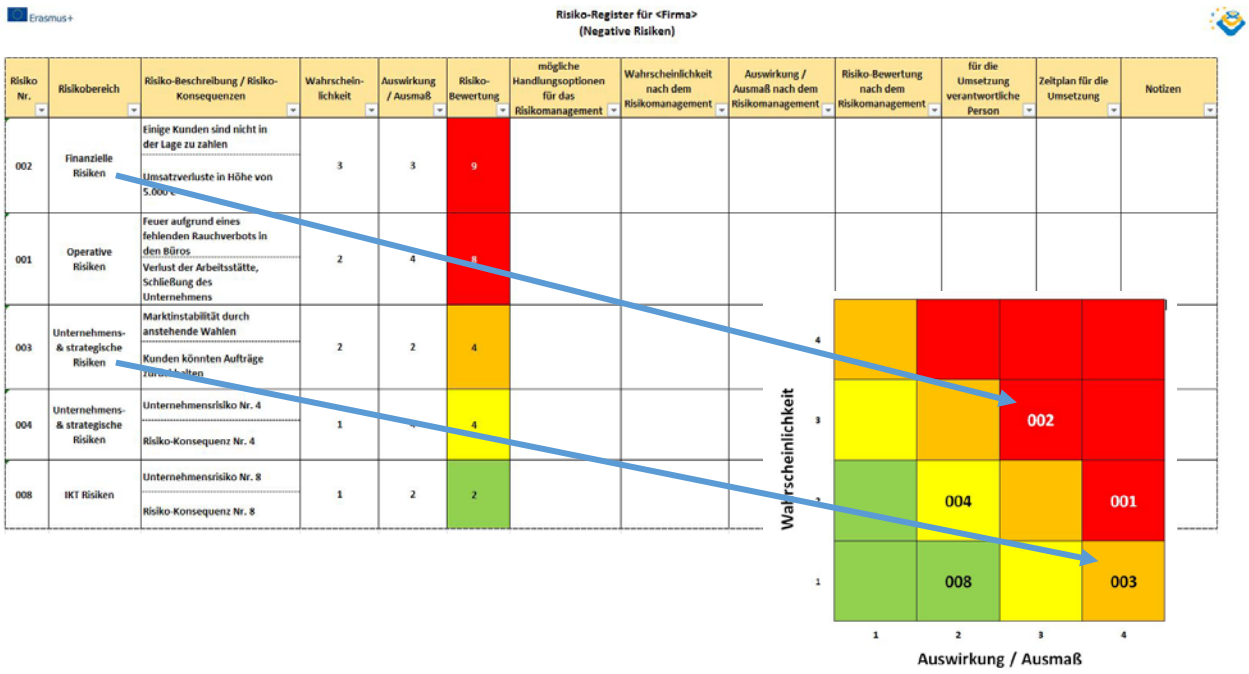
Unsere Risikobereitschaft ist nicht besonders hoch und darum kennzeichnen wir eine Risiko-Bewertung von 8 oder höher als rot. Grün sind die Risiken mit einer Bewertung von 1 oder 2.



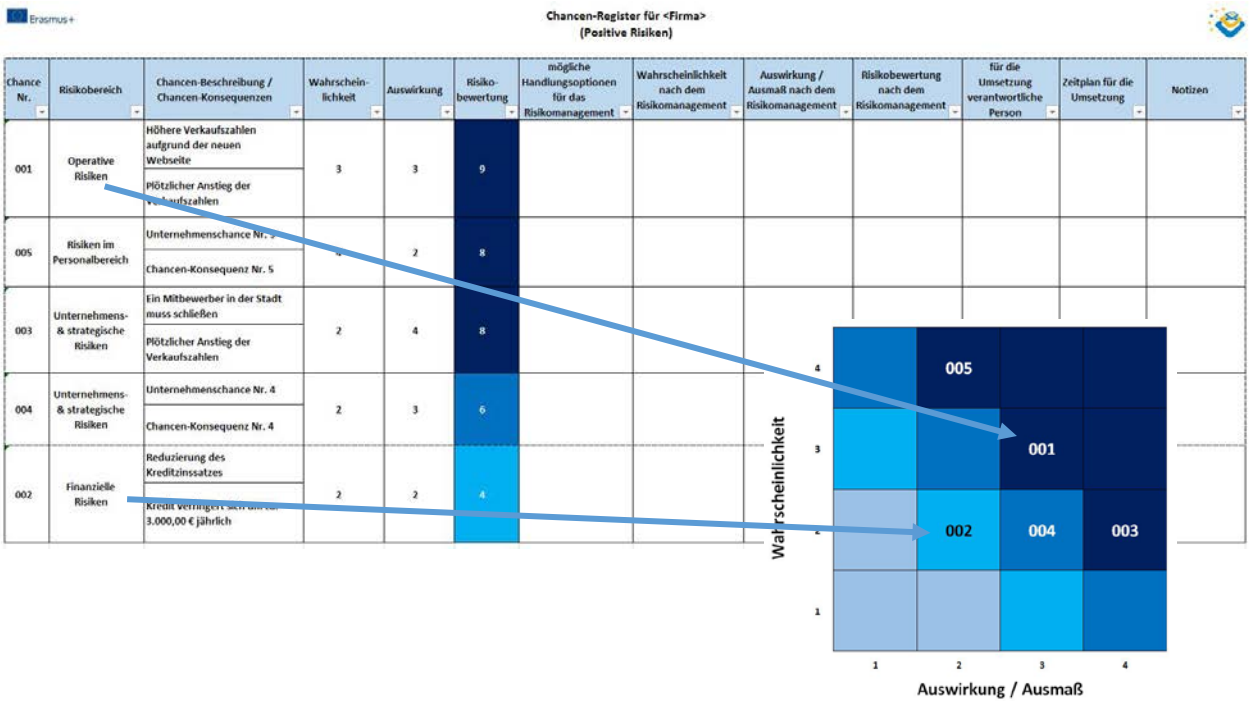
Das gleiche Vorghensweise wenden wir analog bei der positiven Risikomatrix an.

Gehen Sie nun zurück zu Ihren beiden Risikoregistern und wenden Sie das Ampelsystem in der Spalte der Risiko-Bewertung an. Sie erhalten ein eindeutiges Abbild Ihrer wichtigsten Risiken. Mithilfe der Excel-Tabelle können Sie Ihre Liste so anpassen[12], dass die Werte in der Spalte mit der Risiko-Bewertung nach der Größe sortiert werden. Die wichtigsten Risiken und Chancen erscheinen ganz oben in der Tabelle und Sie wissen sofort, mit welchen (positiven oder negativen) Risiken Sie sich zuerst befassen sollten. Das Ergebnis für die negativen Risiken wird in etwa so aussehen:

[12] Hierbei ist die Excel-Vorlage eine große Hilfe. Die Sortierung dauert nur wenige Sekunden.

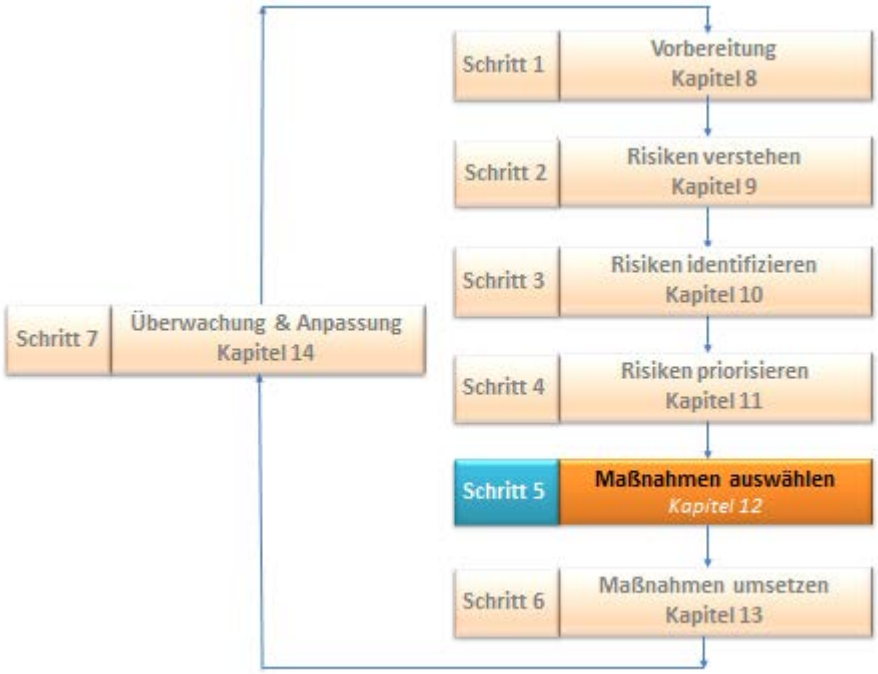


Für die positiven Risiken wird Ihre Risikomatrix und das dazugehörige Chancenregister wie folgt aussehen:



Wie Sie erkennen können, bietet die Risikomatrix-Ansicht ein übersichtliches Bild Ihrer Priorisierung.

12. Schritt 5 – Maßnahmen auswählen



Behalten Sie während Ihres gesamten Resilienz-Projektes Ihr Ziel im Hinterkopf: Die Reduzierung der Risiken Ihres Unternehmens, um damit sicherzustellen, dass der Geschäftsbetrieb aufrechterhalten und Ihre unternehmerischen Ziele erreicht werden können. Das Ergebnis soll kontinuierliches und profitables Wachstum sein.

Bislang haben Sie zwei sehr wichtige Schritte abgeschlossen. Sie haben:

(a) die Risiken identifiziert, mit denen Ihr Unternehmen konfrontiert ist und

(b) diese Risiken priorisiert, indem Sie sie nach Dringlichkeit bzw. Gefährdungspotenzial sortiert haben.

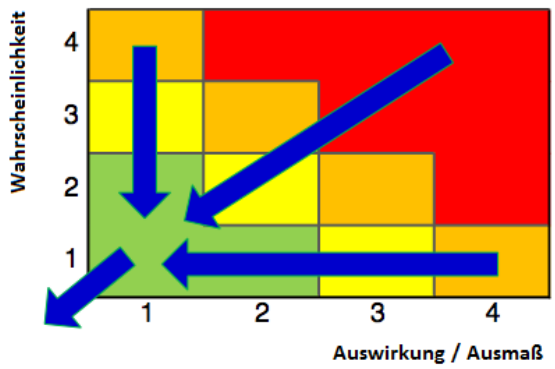
Der nächste Schritt hilft Ihnen dabei zu entscheiden, welche Maßnahmen und Vorgehensweisen die besten sind, um aktiv mit den Risiken in Ihrem Unternehmen umzugehen und diese zu minimieren.

12.1. Ein guter Umgang mit Risiken

Unser **Ansatz zum Umgang mit Risiken** in diesem Handbuch ist einfach:

Verbessern Sie die Position jedes Risikos in Ihrer Matrix, so dass es entweder in den grünen Bereich verschoben werden kann, oder versuchen Sie, das Risiko gleich vollständig aus der Matrix zu entfernen, so dass es für Ihr Unternehmen nicht mehr existiert.

Das bedeutet, dass Sie jedes Risiko einzeln bearbeiten müssen. Nachdem Sie die notwendigen Maßnahmen ergriffen haben, wird Ihre aktualisierte Risiko-Bewertung dementsprechend niedriger sein. Ihre Risiken bewegen sich wie folgt in Ihrer Matrix:



- vom roten Bereich in den orangen, gelben bzw. grünen Bereich oder
- von Orange nach Gelb bzw. Grün oder
- von Gelb nach Grün oder
- am besten komplett aus der Matrix und aus Ihrem Risikoregister.

12.1.1. Ab wann ist ein Risiko akzeptabel?

Die **Entscheidung, ab wann ein Risiko akzeptiert werden kann**, hängt von diversen Rahmenbedingungen ab:

(a) Die Risiko-Bewertung für ein Risiko ist bereits niedrig genug, also die Eintrittswahrscheinlichkeit und die potenziellen Auswirkungen werden insgesamt als gering eingeschätzt.

(b) Der Aufwand, der betrieben werden muss (z. B. Einsatz von Personal oder externe Kosten), um das Risiko zu reduzieren oder zu minimieren, übersteigen die negativen Auswirkungen, sollte dieses Risiko eintreten.

(c) Es gibt nachvollziehbare Gründe, warum es gegenwärtig nicht möglich ist, geeignete Maßnahmen zu ergreifen, um die Risiko-Bewertung zu senken.

Risiken mit den dargestellten Merkmalen befinden sich im besten Fall bereits im grünen Bereich Ihrer Risikomatrix. Ansonsten müssen Sie das Risiko, egal in welchem Bereich der Risikomatrix es sich aktuell befindet, fürs erste akzeptieren, wenn Sie es nicht vermeiden, mindern oder anderweitig reduzieren können.

In solch einem Fall müssen Sie **das Risiko als AKZEPTABEL bewerten**. Behalten Sie es aber auf alle Fälle zur weiteren Beobachtung im Ihrem Risikoregister.

12.1.2. Was wird mit den akzeptablen Risiken gemacht?

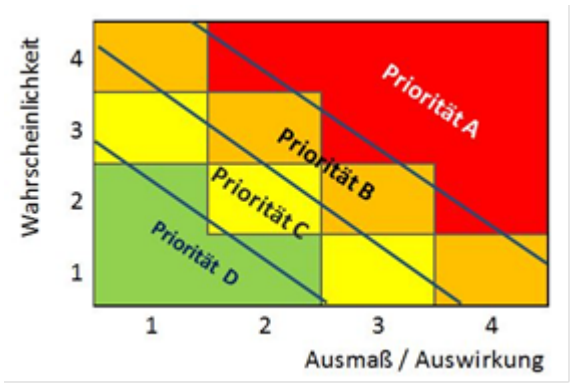
Ein Risiko, das Sie als akzeptabel eingestuft haben, wird entweder nicht weiter beachtet oder man erstellt einen kurzen Plan bzw. eine Handlungsanweisung für den Fall, dass es eintritt. Diesen Plan haben Sie dann zur Hand, wenn Sie ihn benötigen. Das Ziel ist, möglichst schnell wieder ohne Beeinträchtigung weiterarbeiten zu können.

12.1.3. Was wird mit den nicht akzeptablen Risiken gemacht?

Die meisten Risiken werden Sie nicht akzeptieren können. Diese Risiken haben eine hohe Eintrittswahrscheinlichkeit und/oder zu große negative Auswirkungen, damit also eine mittlere bzw. hohe Risiko-Bewertung. Sie befinden sich in den roten, orangen oder gelben Bereichen der Matrix und sind nicht tolerierbar, weil die negativen Konsequenzen für Ihr Unternehmen zu weitgehend wären.

Gegen diese Risiken können Sie vorgehen, indem Sie eine der weiter unten dargestellten Strategien zum Umgang mit Risiken einsetzen.

Beachten Sie, dass **jedes Risiko einzigartig** ist. Sie werden daher **eines nach dem anderen** bearbeiten müssen. Auch die von Ihnen gewählten Maßnahmen müssen dementsprechend passgenau ausgewählt werden.



Es gibt kein Risiko-Management von der Stange. Dazu ist Ihre Unternehmens-situation zu einzigartig. Sie müssen sich mit jedem einzelnen Risiko sehr individuell auseinandersetzen.

Dabei sollten Sie mit den Risiken der Priorität A (siehe Schaubild) beginnen und sich dann über B und C nach D vorarbeiten.

12.2. Die möglichen Strategien zum Umgang mit Risiken

Um den hier empfohlenen **Ansatz zum Umgang mit Risiken** umzusetzen, können Sie eine, mehrere oder auch alle der **folgenden Strategien** für jedes Ihrer Risiken anwenden:

(a) RISIKO VERMEIDEN

- **Vermeiden Sie ein Risiko**, so dass davon für Ihre Firma keine Gefahr mehr ausgehen kann, indem Sie die Aktivität einfach gar nicht beginnen oder nicht weiter fortführen, die zur Entstehung des Risikos führen kann bzw. geführt hat.

  z. B. können Sie das Risiko, dass ein neues Produkt, für das Sie im Einkauf viel investieren müssten, viel zu schlechte Verkaufszahlen aufweist, vermeiden, indem Sie es zum gegenwärtigen Zeitpunkt nicht einführen.

Die Vermeidungs-Strategie wird oft genutzt, wenn eine Aktivität oder eine Situation ein hohes Risiko beinhaltet und kein anderer Ansatz angewandt werden kann. Ein Risiko kann verglichen mit den angenommenen Vorteilen für ein Unternehmen einfach zu hoch sein. Außerdem ist es möglich, dass sich die absehbaren Kosten für eine Minderung des Risikos nicht rentieren oder trotz eines hohen (finanziellen) Aufwandes die mindestens notwendige Risikoreduzierung nicht zu erreichen ist.

Also muss die Entscheidung getroffen werden, eine riskante Aktivität nicht zu beginnen oder nicht weiter darin involviert zu sein.

(b) RISIKO MINDERN

- **Den Ursprung des Risikos beheben**:

  z. B. durch Ersetzen eines defekten Kabels, das zu Verbindungsproblemen mit dem Internet führt. Der Ursprung des Risikos wird entfernt, also besteht kein Risiko mehr, dass die Verbindung in einem kritischen Moment unterbrochen wird.

In solch einem Fall investiert das Unternehmen (ein wenig) Geld und Zeit, um die Ursache des Risikos komplett zu entfernen. Die Entfernung unterscheidet sich von der Vermeidung. Wenn ein Risiko gemindert wird, verbleibt es trotzdem im Risikoregister, wird aber neu eingestuft. Wird es entfernt (s. o. Vermeidung), dann ist das Risiko für das Unternehmen nicht mehr vorhanden.

- **Mindern der Eintrittswahrscheinlichkeit eines Risikos**:

  z. B. (1) indem Sie das Rauchen in den Räumlichkeiten Ihres Unternehmens verbieten, können Sie das Risiko eines Brandes reduzieren.

  (2) Auch der Umzug Ihrer Geschäftsräume aus der Nähe eines Waldgebietes in eine Stadt vermindert die Brandgefahr.

Sie können im Normalfall die Eintrittswahrscheinlichkeit eines Risikos reduzieren, indem Sie seine Quelle überwachen bzw. kontrollieren. Beispielsweise können Sie für alle schriftlichen Berichte, die Ihr Unternehmen an Kunden sendet, das 4-Augen-Prinzip als Qualitätskontrolle einführen und so die Wahrscheinlichkeit, dass ein Schriftstück mit zu geringer Qualität Ihr Haus verlässt, nachhaltig mindern.

- **Mindern der Auswirkungen eines Risikos:**

  z. B. (1) indem Sie einen Plan zur Sicherstellung Ihres Geschäftsbetriebes für den Fall vorbereiten, dass Sie von einer Überschwemmung getroffen werden, mindern Sie die Auswirkungen, sollte ein naheliegender Fluss tatsächlich über die Ufer treten. Sie werden in Ihrem Plan Vorkehrungen treffen, die es Ihnen erlauben, Ihren Geschäftsbetrieb fortzusetzen, obwohl Ihr Bürogebäude ernsthaft in Mitleidenschaft gezogen wurde. Sie können die Auswirkungen eines Flutschadens darüber hinaus mindern, indem Sie eine Versicherung abschließen, die im Schadensfall die Kosten übernimmt (siehe dazu auch unten „Risiko übertragen“).

(2) Wenn Sie ein automatisches Feuerlöschsystem installieren, dann werden Sie die Auswirkungen eines Brandes reduzieren.

Die Minderung der Auswirkungen eines Risikos verlangt häufig nicht nur nach der Umsetzung ganz bestimmter Maßnahmen. Immer wieder werden Sie (a) **das Risiko an Dritte übertragen** (siehe unten) und (b) einen **Notfallplan bzw. einen Plan zur Sicherstellung Ihres Geschäftsbetriebes** erstellen müssen. Beides sind alternative Vorgehensweisen, um sicherzustellen, dass Ihr Geschäftsbetrieb fortgeführt werden kann. Das Risiko selbst wird dadurch nicht verändert, aber Sie reduzieren die Auswirkung, **wenn es eintreten sollte**. Ausführliche Informationen über die Erstellung eines Notfallplans bzw. des Plans zur Sicherstellung des Geschäftsbetriebes finden Sie in den folgenden Kapiteln dieses Handbuches.

- **Mindern der Eintrittswahrscheinlichkeit und der Auswirkungen:**

  z. B. wählen Sie zwei Maßnahmen und setzen diese gleichzeitig um: (a) Sie verbieten das Rauchen in Ihren Räumlichkeiten und (b) Sie installieren ein automatisches Feuerlöschsystem. Damit werden beide Risikofaktoren vermindert.

Dies ist also eine Kombination aus beiden oben dargestellten Vorgehensweisen.

(c) <u>RISIKO ÜBERTRAGEN</u>

- **Übertragen des Risikos an Dritte:**

  z. B. können Sie das Risiko, Ihr gesamtes Betriebsvermögen durch ein Feuer zu verlieren, verringern, indem Sie dieses Risiko mit einem Versicherungsunternehmen „teilen“.

Ein Risiko zu übertragen ist in gewisser Weise auch ein Weg der Risikoverminderung (siehe oben (b)). Risiken werden meist wie folgt übertragen:

(a) Versicherungsschutz für besonders existenzgefährdende Risiken: Eine Versicherung zahlt Ihnen einen Geldbetrag für Ihren erlittenen Schaden, z. B. für zerstörte Räumlichkeiten, Güter oder Ausrüstungen bzw. auch bei Personenschäden oder bei Haftungsrisiken.

(b) Outsourcen oder Unterauftragsvergabe an Dritte: Eine Dienstleistung oder eine (interne) Aktivität kann Ihrer Meinung nach von Dritten besser erbracht werden, weil Sie ein besseres Ergebnis erwarten oder Dritte mehr Kapazitäten in Bereichen haben, in denen es Ihnen an Expertise, Fähigkeiten oder finanziellen Ressourcen fehlt (z. B. Outsourcing Ihrer Buchhaltung an einen Steuerberater, anstatt Einstellung eines betriebsinternen Buchhalters).

Die folgenden **beiden Punkte sind sehr wichtig,** wenn Sie überlegen, eines oder mehrere Ihrer Risiken zu übertragen:

(a) Das Outsourcing oder das Abschließen einer Versicherung kann, obwohl es gewisse Risiken reduziert, gleichzeitig neue Risiken mit sich bringen, die Sie im Zuge Ihres Vertragsmanagements mit Ihrem externen Dienstleister oder einer Versicherungsgesellschaft ebenfalls unter Kontrolle behalten müssen (z. B. das Risiko, dass ein Versicherungsunternehmen nicht zahlt oder ein von Ihnen beauftragtes Unternehmen plötzlich Konkurs anmelden muss).

(b) Obwohl Sie das Risiko übertragen haben, ist Ihr Unternehmen gegenüber den eigenen Interessensvertretern bzw. Stakeholdern weiter voll verantwortlich (u. a. Kunden, Anteilseigner, Behörden).

(d) RISIKO AKZEPTIEREN

- **Das Risiko akzeptieren** (siehe auch oben): Diese Strategie wiederholen wir hier in dieser Auflistung bewusst, weil insbesondere für kleine und Kleinst-Unternehmen bei diversen Risiken kurz- oder mittelfristig keine andere Vorgehensweise in Frage kommt, u. a. weil es an den nötigen zeitlichen oder finanziellen Ressourcen mangelt. Trotzdem ist eine informierte und bewusste Entscheidung über die (hoffentlich) nur zeitlich befristete Akzeptanz von Risiken immer noch besser, als Risiken ganz zu vergessen, zu ignorieren oder gar nicht zu identifizieren.

(e) RISIKO VERSTÄRKEN (NUR FÜR POSITIVE RISIKEN/CHANCEN)

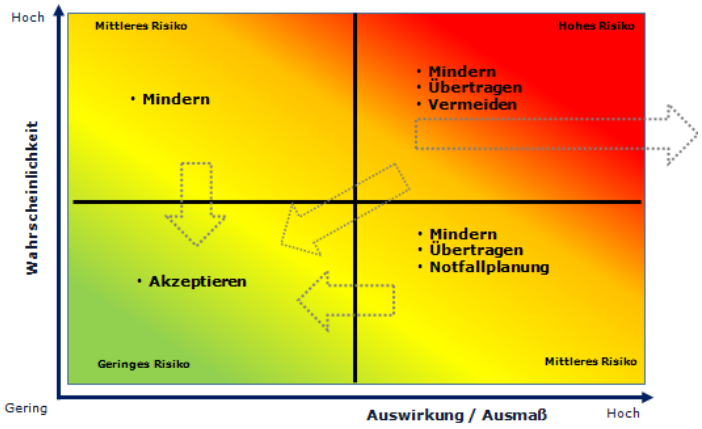
- **Das Risiko nutzen und/oder verstärken**, um eine sich bietende Chance zu nutzen.

z. B. ist es denkbar, dass eine Dienstleistung für einen Kunden schneller und damit mit weniger Aufwand fertiggestellt werden kann, als ursprünglich geplant. Wenn dies geschieht, sparen Sie ggf. Kosten ein. In so einem Fall konzentriert man sich darauf, die Wahrscheinlichkeit einer rascheren Fertigstellung zu erhöhen, man verstärkt also das positive Risiko.

Diese Strategie ist **einzig und allein für positive Risiken** geeignet: Ein Risiko kann verstärkt werden, indem die Eintrittswahrscheinlichkeit oder die möglichen Auswirkungen erhöht werden. Es sollten alle notwendigen Maßnahmen ergriffen werden, um sicherzustellen, dass das Risiko eintritt und das Unternehmen durch die entstandene Chance so weit wie möglich profitiert.

12.2.1. Welche Strategie passt zu welcher Risiko-Bewertung?

Da jedes Risiko für sich gemanagt wird, müssen die jeweils verantwortlichen Personen einige wichtige Aspekte in ihrem Entscheidungsprozess berücksichtigen.



Obwohl einige Risiken dieselbe Risiko-Bewertung haben (z. B. Risiko A hat die Wahrscheinlichkeit 2 und die Auswirkung 4 und damit die gleiche Bewertung wie Risiko B mit der Wahrscheinlichkeit 4 und der Auswirkung 2), werden Sie unterschiedliche Strategien im Umgang mit diesen Risiken anwenden.

Ein Risiko kann, abhängig von der Bewertung seiner Wahrscheinlichkeit und seiner Auswirkung, in vier Kategorien unterteilt werden (siehe Grafik). Für jede Kategorie gibt es bevorzugte Strategien zum Umgang mit einem Risiko, die im Normalfall Anwendung finden. Selbstverständlich können Sie auch andere Vorgehensweisen wählen, wenn diese besser geeignet sind. Wir zeigen Ihnen hier nur die geläufigsten Strategien:

(a) Risiken mit **hoher Eintrittswahrscheinlichkeit** und **hoher Auswirkung** (rechts oben in Ihrer Risikomatrix)

Diese Risiken sind absolut inakzeptabel. Ihre hohe Eintrittswahrscheinlichkeit bedeutet, dass sie sehr wahrscheinlich oder fast schon sicher eintreten. Wenn das geschieht, ist die Auswirkung, die sie auf das Unternehmen haben können, sehr bedrohlich. Es muss unbedingt gehandelt werden, um diese Risiken auf eine akzeptable Stufe zu senken. Die folgenden Strategien können Sie anwenden:

(1) Vermindern Sie das Risiko, indem Sie Maßnahmen ergreifen, um die Eintrittswahrscheinlichkeit oder die Auswirkungen zu reduzieren.

(2) Übertragen Sie das Risiko:

- Outsourcing oder Vergabe eines Untervertrages, um das Risiko an externe Dritte zu übertragen. Diese Übertragung senkt das Risiko auf ein akzeptableres Level.
- Abschluss einer Versicherung, um den potenziellen Verlust zu mindern.

(3) Vermeiden Sie das Risiko komplett, indem Sie bestimmte Aktivitäten oder Dienstleistungen nicht weiter fortführen bzw. anbieten.

(b) Risiken mit **hoher Eintrittswahrscheinlichkeit** und **geringer Auswirkung** (oben links in Ihrer Risikomatrix)

Diese Risiken treten recht häufig auf. Da die Auswirkungen im Normalfall recht niedrig oder unerheblich sind, **scheint** zuerst einmal kein großes Problem vorzuliegen. Das ist jedoch nicht richtig, da die Auswirkungen durch das regelmäßige Auftreten kumuliert auch recht hoch bzw. inakzeptabel sein können.

Diese Risiken haben ihre Ursache häufig in nachrangigen Problemen im Zusammenhang mit internen Prozessen, Prozeduren, Aktivitäten oder Ihrer Ausrüstung. Meist reichen ganz konkrete und überschaubare Maßnahmen, um diese Risiken ganz in den Griff zu bekommen oder die durch sie verursachten Störungen zu minimieren. Ein typisches Beispiel dafür sind Geräte, wie z. B. ein zu alter Drucker, der oftmals Störungen aufweist. Hier lohnt es sich, ggf.

schneller ein neues Gerät anzuschaffen. Das Thema Qualitätssicherung gehört auch häufig in diesen Bereich. Dieses Risiko kann z. B. durch die Anwendung des Vier-Augen-Prinzips (Thema Rechtschreibung) vor dem Aussenden von Dokumenten an einen Kunden weitestgehend behoben werden.

Die typische Strategie für solche Risiken ist:

Vermindern Sie das Risiko, indem Sie Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit ergreifen.

(c) Risiken mit **niedriger Eintrittswahrscheinlichkeit** und **hoher Auswirkung** (unten rechts in Ihrer Risikomatrix)

Diese Risiken treten zwar selten auf, jedoch können die Auswirkungen, die sie auf Ihr Unternehmen haben, gewaltig sein. Typische Beispiele dafür sind Naturkatastrophen (Überschwemmungen, Erdbeben etc.), Brände oder der Verlust bzw. Ausfall Ihres gesamten IKT-Systems und der IT-Infrastruktur.

Der hohe potenzielle Schaden dieser Risiken (z. B. Stillstand des Geschäftsbetriebes, beträchtlicher finanzieller Verlust, zerstörte Räumlichkeiten etc.) bedeutet, dass diese Risiken gemanagt werden müssen.

Typische Strategien für diese Risiken sind:

(1) Vermindern des Risikos, indem passende Maßnahmen ergriffen werden, um die Auswirkungen abzuschwächen, falls dieses Risiko tatsächlich eintritt.

(2) Übertragen des Risikos:

- Outsourcing einer bestimmten Aktivität, um das Risiko an externe Dritte zu übertragen. Die Übertragung senkt das Risiko auf eine akzeptablere Stufe.
- Eine Versicherung abschließen, um den potenziellen Verlust zu mindern.
- Erstellen eines Notfallplans, um die operativen Tätigkeiten fortführen zu können und um sicherzustellen, dass die Fortführung des Geschäftsbetriebes gewährleitet ist, falls das Risiko eintritt (mehr Informationen dazu folgen in einem späteren Kapitel).

(d) Risiken mit **niedriger Eintrittswahrscheinlichkeit** und **niedriger Auswirkung** (unten links in Ihrer Risikomatrix)

Diese Risiken können akzeptiert werden und benötigen häufig keine weiteren Aktivitäten zu ihrer Minderung. Es ist sehr unwahrscheinlich, dass diese Risiken eintreten und selbst wenn dies geschieht, sind die Auswirkungen (sehr) gering.

Die typische Strategie für solche Risiken ist:

Akzeptieren Sie das Risiko, aber bewerten Sie es regelmäßig neu, um erkennen zu können, wenn sich die potenziellen Folgen negativ verändern.

12.2.2. Umgang mit IT-Risiken

Um die richtigen Maßnahmen für den Umgang mit IT- bzw. Informationssicherheits-Risiken zu identifizieren, hilft Ihnen die folgende Vorgehensweise:

- Arbeiten Sie in zwei Bereichen:
  (1) Strategischer bzw. unternehmerisch, operativer Bereich
  (2) Technischer Bereich
- Wenden Sie für diese beiden Bereiche folgende zwei Vorgehensweisen an:
  (1) Wählen Sie die besten Maßnahmen aus, die Ihnen zur Verfügung stehen, um das Risiko zu mindern. Stellen Sie sicher, dass Sie das Risiko auch wirklich verstehen. Fragen Sie sich z. B.: „Welche Daten oder Informationen könnten in Sachen Vertraulichkeit oder Integrität verletzt werden?“ oder „Wie könnte diese Manipulation dieser Daten stattfinden?“
  (2) Denken Sie für den Fall, dass das Risiko eintritt, immer auch an weitere alternative Handlungsoptionen oder Vorbereitungen, selbst wenn Sie bereits Maßnahmen zur Minderung des Risikos umgesetzt haben (weitere Back-Ups, Notfallpläne etc.).

12.2.2.1. Strategischer bzw. unternehmerisch, operativer Bereich

Hier geht es um die folgenden Maßnahmen und Aktivitäten:

1. Identifizieren Sie die bestmögliche IKT-Strategie für die Technologie- und Kommunikationssysteme Ihres Unternehmens.

   Die strategischen Entscheidungen, die Sie in Bezug auf Ihre IT-Systeme treffen, sind von herausragender Bedeutung. Die folgenden Fragen sollen Sie dabei unterstützen, die richtigen Entscheidungen zu treffen:

   - Sollten wir eine ERP-Softwarelösung anschaffen oder können wird das outsourcen?
   - Sollten wir unsere Daten in der Cloud speichern oder eigene Server kaufen?
   - Stellen wir einen Mitarbeiter ein, der IKT-Kenntnisse besitzt und/oder beauftragen wir einen externen Berater?
   - Welchen Berater wählen wir für die Wartung und den Support unserer Systeme? Ist eine Einzelperson ausreichend, oder sollten wir uns für ein Unternehmen entscheiden?
   - Sollen wir Microsoft-, UNIX- oder Apple-Betriebssysteme nutzen?

   Nehmen Sie sich hier die notwendige Zeit und entscheiden Sie sehr bewusst.

   Einige Beispiele, die Ihnen ggf. schon bekannt vorkommen:

   - **Die Anschaffung eines eigenen Servers oder das Hosting Ihrer Anwendungen bzw. Daten in der Cloud.** Die Cloud minimiert das Risiko eines Serverausfalls verbunden mit dem Risiko des Datenverlusts. Für die Cloudlösung benötigen Sie aber einen unterbrechungsfreien Internetzugriff, wenn Sie permanent mit Ihren Daten arbeiten müssen. Diese Verbindung kann z. B. auch von Hackern angegriffen werden.
   - **Gemeinsames Speichern aller Dateien (z. B. Word, Excel etc.) auf einem zentralen Dateiserver oder Speichern durch jeden Mitarbeiter separat auf den persönlichen Computerfestplatten**. Beide Optionen haben Vor- und Nachteile: Wenn Ihr Dateiserver gehackt wird, sind alle Dateien auf einmal gefährdet, allerdings ist das Back-Up Ihres gesamten Datenbestands viel einfacher, wenn diese auf einem zentralen Server gesichert werden.

- **Anschaffung einer Buchhaltungssoftware oder komplettes Outsourcing an ein Steuerberatungsunternehmen**. Wenn Sie Ihre Buchhaltungs- und Steuerinformationen auf Ihrem eigenen Server verwalten, sollten Sie sich der potenziellen technischen Probleme bewusst sein, die mit Servern, Software und Back-Ups auftreten können. Positiv ist, dass die Daten dann unter Ihrer Kontrolle bleiben. Wenn Sie eine externe Lösung wählen, geben Sie die Kontrolle über sensible Daten aus der Hand. Sie sollten sich daher mit den Sicherheitsstandards Ihres externen Dienstleisters (Wie und wo speichert Ihr Steuerberater Ihre Daten ab?) beschäftigen und auch eruieren, was passieren kann, wenn diese Speicherung gehackt wird.

Da diese Themen äußerst komplex sind, wird Ihr persönliches Know-how oftmals nicht ausreichen. Es ist dann geboten, einen externer IT-Berater hinzuzuziehen, der gemeinsam mit Ihnen die Vor- und Nachteile der diversen Optionen bewertet. Die endgültige Entscheidung kann Ihnen dieser Berater jedoch nicht abnehmen. Finden Sie wirklich eine passende Lösung für Ihr Unternehmen und fällen Sie Ihre Entscheidungen nur dann, wenn Sie die Konsequenzen wirklich verstanden haben. Sie müssen mit dem Ergebnis Ihrer Entscheidungen voraussichtlich über einen längeren Zeitraum arbeiten.

2. <u>Wählen Sie Ihre IKT-Dienstleister sehr sorgfältig aus</u>

Bei der Auswahl Ihrer IKT-Dienstleister müssen Sie nicht nur darauf achten, dass der Dienstleiter eine hohe Kompetenz aufweist. Um Ihr Risikopotenzial zu minimieren, achten Sie bitte besonders auf die folgenden Kriterien:

NR.	KRITERIUM ZUR RISIKOSTEUERUNG	ERLEDIGT
1	Prüfen Sie die Vertrauenswürdigkeit. Sie müssen sicherstellen, dass sich Ihre IT-Infrastruktur und Ihre Daten in den richtigen Händen befinden.	
2	Schließen Sie einen Vertrag, der jede einzelne Dienstleistung detailliert beschreibt, die das Unternehmen für Sie bereitstellt. Achten Sie darauf, dass auch der Servicelevel explizit definiert ist (z. B. die Reaktionszeit, falls ein Gerät ausfällt). Auch die Verpflichtung zur Vertraulichkeit und zum Datenschutz der Daten Ihres Unternehmens muss ein fester Bestandteil dieses Vertrages sein.	
3	Stellen Sie sicher, dass Sie genau wissen, welche Zugriffsrechte Sie dem externen Unternehmen (und seinen Angestellten) gewährt haben (z. B. Büroschlüssel, Passwörter für einige oder alle Systeme, Fernwartung etc.). Vergessen Sie nicht, diese Zugriffsrechte bei Beendigung einer Kooperation wieder zu entziehen.	
4	Überprüfen Sie regelmäßig, ob die vertraglich festgelegten Regeln auch eingehalten werden. Nutzen Sie Vertragsstrafen.	

3. Legen Sie interne Regeln und Prozesse fest, die bestimmen, wie Ihre IKT-Systeme genutzt und administriert werden sollen.

   Auf diesem Gebiet gibt es für Ihr Unternehmen jede Menge Arbeit – allerdings mehr im Hinblick auf die Qualität als auf die Quantität. Sie finden untenstehend eine Liste mit ausgewählten Maßnahmen, die sich auf Ihre IKT-Systeme und das Thema Informationssicherheit beziehen und die Ihnen im Umgang mit Ihren Risiken helfen können. Wir empfehlen Ihnen, dass Sie diese Liste Schritt für Schritt gemeinsam mit Ihrem IKT-Berater durcharbeiten:

   - **Geben Sie jemandem in Ihrem Unternehmen die Zuständigkeit für das Thema Sicherheit** (das könnten Sie selbst sein, ein Manager, der Inhaber

oder ein zuverlässiger Mitarbeiter). Diese Person sollte sicherstellen, dass alle Sicherheitsbestimmungen umgesetzt und dauerhaft eingehalten werden.

Dieselbe Person sollte auch dafür verantwortlich sein, dass alle wichtigen Informationen aktualisiert, sicher gelagert oder gespeichert werden und bei Bedarf zur Verfügung stehen (z. B. die Liste mit allen Zugriffsrechten auf Ihr IKT-System und die jeweiligen Berechtigungen für die Nutzer, Ihre Mitarbeiter und für Dritte).

- **Klassifizieren Sie Informationen**. Manche Informationen oder Dokumente können für jeden zugänglich sein, andere wiederum nur für eine ausgewählte Nutzergruppe. Setzen Sie eine Klassifizierung fest, indem Sie z. B. das Wort „VERTRAULICH“ auf allen vertraulichen elektronischen oder ausgedruckten Dokumenten notieren lassen. Bewahren Sie diese Dokumente in Schließfächern und verschließbaren Schreibtischschubladen auf, für die Sie den Zugriff steuern können.
- **Organisieren und kontrollieren Sie Zugriffsrechte**. Nutzen Sie ein internes Dokument, dass Sie ebenfalls als VERTRAULICH einstufen, um folgendes festzulegen:
    - Wer hat Schlüssel für die Räumlichkeiten des Unternehmens?
    - Wer hat Zugriff auf welches System und mit welchen Rechten (z. B. Zugriff nur auf Bereiche, wo Dateien für den jeweiligen Arbeitsbereich aufbewahrt werden oder als Systemadministrator Zugriffsmöglichkeiten auf das gesamte System)?
    - Wer hat Zugriff auf E-Mail-Konten? Listen Sie die unterschiedlichen E-Mail-Konten auf!
    - Wer hat Internetzugang?
    - Wer hat Zugriff auf Schließfächer mit vertraulichen Dokumenten?
- **Organisieren Sie die Kontrolle Ihrer Geräte und Ausrüstungsgegen-stände**.
    - Erstellen Sie eine Liste aller Ihrer IKT-Geräte (ALLE Geräte, nicht nur die wichtigen – auch USB Sticks).

  - Stellen Sie sicher, dass es für jedes Gerät einen Verantwortlichen gibt und notieren diese Verantwortlichkeiten schriftlich. Z. B. könnte jeder Mitarbeiter für seinen PC oder Laptop verantwortlich sein – jeder muss sicherstellen, dass der Rechner nicht verloren geht oder gestohlen wird.
  - Auch die Schlüssel zu Ihren Geschäftsräumen sind wichtig. Kontrollieren und dokumentieren Sie auch, wer Ersatzschlüssel hat bzw. wo diese aufbewahrt werden.

- **Organisieren Sie den Prozess, wenn ein Mitarbeiter das Unternehmen verlässt oder ihm gekündigt wird:** Rückgabe aller Geräte, die zur Verfügung gestellt wurden; Beendigung der Zugriffsrechte auf Ihre IKT-Systeme; Deaktivierung des E-Mail-Kontos etc.
- **Stellen Sie sicher, dass jeder Mitarbeiter vertraglich verpflichtet ist**, die unternehmensintern geregelten Zugriffsrechte auf Betriebsinformationen und Daten sowie alle Sicherheitsvorschriften einzuhalten. Sie werden in diesen Fragen ggf. Ihren Rechtsberater um Unterstützung bitten.
- **Regeln Sie den Umgang mit Passwörtern**. Es sollte kein einziges System in Ihrem Unternehmen geben, für das kein Passwort benötigt wird. Stellen Sie sicher, dass die Passwortlänge ausreichend ist und die Mitarbeiter ausreichend komplexe Passwörter nutzen (z. B. ein Passwort, das Kleinbuchstaben, Großbuchstaben, Zahlen und verschiedene Zeichen beinhaltet). Legen Sie fest, wie häufig Mitarbeiter die Passwörter für jedes System aktualisieren müssen. Verbieten Sie, dass Mitarbeiter Passwörter untereinander austauschen.
- **Dokumentieren Sie alle Abläufe und Prozesse Ihres Unternehmens**.
- **Bereiten Sie einen Back-Up Plan vor**.
- **Ziehen Sie einen Supportvertrag für Ihre EDV-Geräte und Ihre Software in Betracht**, um sicherzustellen, dass Probleme und Ausfälle zeitnah und möglichst kostengünstig gelöst bzw. beendet werden können, sowie dass die Geräte, wenn nötig, rasch ersetzt werden.

- **Bereiten Sie einen Plan zur Sicherstellung Ihres Geschäftsbetriebes und einen Wiederaufbauplan** vor, um beim Verlust von Geräten oder der Zerstörung Ihrer Geschäftsräume reagieren zu können.
- **Bereiten Sie einen Plan zum Umgang mit Störfällen vor**, um bei derartigen Ereignissen und Vorfällen schnell handeln zu können (inklusive sicherheitsrelevante Themen wie Verlust oder Diebstahl von Passwörtern).
- **Stellen Sie sicher, dass es einen Kommunikations- und Benachrichtigungsplan gibt** (z. B. an wen wenden Sie sich und was müssen Sie mitteilen, wenn Kundendaten gehackt wurden?).
- **Führen Sie mindestens einmal im Jahr eine Risiko- und Schwachstellenanalyse** für Ihre IKT-Systeme und IKT-Infrastruktur durch.
- …

4. Erhöhen Sie durch Mitarbeiterschulungen das Bewusstsein zum Thema Informationssicherheit und zum richtigen Umgang mit den IKT-Systemen in Ihrem Unternehmen.

   Dies ist wahrscheinlich die wichtigste Maßnahme! Indem Sie Ihre Mitarbeiter informieren und aktiv einbeziehen, können Sie die Risiken und Bedrohungen für Ihr Unternehmen nachhaltig vermindern und gleichzeitig das Auftreten von negativen Zwischenfällen reduzieren.

   Veranstalten Sie Diskussionsrunden bzw. kurze Schulungseinheiten mit Ihrem IKT-Berater oder einem Sicherheitsexperten. Diese Einheiten sollten die folgenden Themen behandeln:

   - Die Bedeutung des Themas Informationssicherheit allgemein
   - Spezielle Themen, wie:
     - E-Mail Nutzung
     - Webseiten und Webseiten-Zugriff
     - Spam, Phishing und Online-Betrug
     - Nutzung von Social-Media-Kanälen und der Schutz von Unternehmensinformationen

- Identifizierung von Anzeichen, dass die Systeme Ihres Unternehmens möglicherweise gehackt wurden
- Vorgehensweise bei sicherheitsrelevanten Vorfällen
- Abläufe und Prozesse in Ihrem Unternehmen (z. B. Zugriffsrechte)
- Schutz der unternehmenseigenen Anlagen und Geräte
- Verschlüsselung von Daten
- …

Ihre Mitarbeiter müssen keine Experten auf diesem Gebiet werden, aber „gute und aufgeklärte Nutzer“ sollten sie sein. Schulungen sollten auch für neue Mitarbeiter angeboten werden und Ihre internen Diskussionsrunden sollten in regelmäßigen Intervallen wiederholt werden. In den Diskussionsrunden sollten bereits eingeführte Maßnahmen und Lösungen vorgestellt werden, sodass Ihre Mitarbeiter eine klare Vorstellung davon erhalten, was sie zu tun bzw. zu lassen haben.

Ihre Mitarbeiter müssen unbedingt verstehen, wie wichtig das Thema Sicherheit für Ihr Unternehmen ist. Mögliche Verletzungen oder Verstöße können nicht nur extreme Auswirkungen auf den Geschäftsbetrieb haben, sondern auch zu (disziplinar-)rechtlichen Verfahren gegen das Unternehmen oder gegen die Mitarbeiter selbst führen.

12.2.2.2. Technischer Bereich

Dieser Bereich konzentriert sich auf die Auswahl und die Spezifikationen Ihrer unternehmensinternen technischen Lösungen. Das Ziel ist, negative Zwischenfälle jeglicher Art möglichst auszuschließen. Es folgt eine Liste mit Beispielen, um Sie direkt zu unterstützen:

- Installieren Sie ein Alarmsystem, um jeden unerlaubten Zutritt bzw. das physische Eindringen in Ihre Räumlichkeiten zu überwachen. Installieren Sie eine Überwachungskamera inkl. Aufnahmefunktion.
- Nutzen Sie Anti-Virus oder Anti-Malware Software für die IKT-Systeme Ihres Unternehmens. Stellen Sie sicher, dass diese Anwendungen permanent aktualisiert werden.

- Installieren Sie eine Firewall (ein System, um den ein- und ausgehenden Datenverkehr zu überwachen und zu steuern).
- Aktualisieren Sie regelmäßig Ihre Software. Stellen Sie sicher, dass regelmäßig Patches[13] installiert werden. Verlangen Sie, dass Ihre IKT-Dienstleister regelmäßige Updates und Patches liefern.
- Installieren Sie Stromaggregate, USV[14] und Netzfilter, um so die Auswirkung zu reduzieren, die ein Stromausfall auf Ihr Netzwerk und die Leistung Ihres IKT-Systems haben kann.
- Implementieren Sie Verschlüsselungssysteme, um Ihre gespeicherten Daten zu schützen. Das gilt sowohl für Dateiserver, Laptops, USB Sticks, als auch für externe Festplatten, die Sie nutzen, um Dateien zu übertragen und zu kopieren. Es ist besonders wichtig, dass Sie genau wissen, wer Zugriff auf diese Verschlüsselungscodes hat, und dass Sie Kopien davon an einem sicheren Ort aufbewahren (falls die Codes vergessen werden oder verloren gehen).
- Entscheiden Sie, ob Sie W-LAN nutzen wollen. W-LAN Netzwerke können sehr praktisch sein, da man schnell und einfach darauf zugreifen kann, jedoch sind sie auch weitaus anfälliger für Hacking-Angriffe. Sollten Sie ein W-LAN Netzwerk aufsetzen, ändern Sie regelmäßig das Passwort und steuern Sie den Zugriff durch die Nutzer.
- Nutzen Sie Softwarelösungen und Tools, um Ihr System und Ihr Netzwerk laufend zu überwachen (besonders wichtig für 24/7 E-Commerce Webseiten).
- Steuern Sie den Internetzugriff Ihrer Mitarbeiter. Genehmigen Sie keinen Zugriff auf Online-Casinos, „Erwachsenen“-Seiten, Spiele oder ähnlich risikoreiche Webseiten.
- Nutzen Sie einen separaten und abgeschlossenen Raum mit funktionierender Klimaanlage als Serverraum für Ihr IKT-System.

[13] Ein Patch ist eine Korrekturauslieferung für Software oder Daten, um Sicherheitslücken zu schließen, Fehler zu beheben oder bislang nicht vorhandene Funktionen nachzurüsten.

[14] USV = Unterbrechungsfreie Stromversorgung. Siehe dazu auch Kapitel 16: Ausgewählte Begriffe und Abkürzungen.

Für den Umgang mit Ihren IT-Risiken empfehlen wir Ihnen die Zusammenarbeit mit einem externen IKT-Berater, um die sichersten und besten Maßnahmen zur Risikominimierung zu identifizieren.

12.2.3. Erarbeiten eines umfassenden „Plans zur Sicherstellung des Geschäftsbetriebes“

Einige nicht akzeptable Risiken und Gefahren können nicht weiter oder weit genug minimiert werden. Es bleibt ein Restrisiko bestehen, z. B. weil ein Unternehmen seinen Standort aus einem erdbebengefährdeten Gebiet nicht verlegen kann oder will. Vorausschauende Unternehmen planen deshalb die Sicherstellung ihres Geschäftsbetriebes für den Fall, dass es zu einer wesentlichen Störung mit sehr negativen Auswirkungen kommt. Dieses Vorgehen, das auch als betriebliches Kontinuitätsmanagement bezeichnet wird, plant den Umgang mit einschneidenden negativen Störungen oder Katastrophen in den folgenden Bereichen: Infrastruktur, Räumlichkeiten, eigene Dienstleistungen, operative Tätigkeiten, Personal, Zulieferer, Geschäftspartner, Kunden, Märkte, Markenauftritt und Renommee etc.

Um die Sicherstellung Ihres Geschäftsbetriebes planen zu können, müssen Sie sich überlegen, welche Handlungsmöglichkeiten Sie im Falle störender oder zerstörerischer Ereignisse haben (z. B. Verlust von Geräten und Räumlichkeiten oder im Hinblick auf immaterielle Werte wie den Verlust Ihres wichtigsten Kunden). Dieser Plan muss sofort in dem Moment umsetzbar sein, wenn das negative Ereignis eintritt. Ein Plan zur Sicherstellung des Geschäftsbetriebes kann alle oder einige der folgenden Risiken abdecken:

- **Notfall- und Evakuierungsplan** (um die Auswirkung zu mindern, die Risiken wie Feuer oder die Zerstörung Ihres Bürogebäudes auf Personen in Ihren Räumlichkeiten haben)
- **Geschäftsräume oder Arbeitsplätze nicht nutzbar** (Home-Office als Alternative in Betracht ziehen)
- **Versagen oder Ausfall von IKT-Systemen** (entweder kompletter Ausfall, Datenverlust oder beides)

- **Verlust von Dateien und Archiven** (elektronisch oder auf Papier)
- **Ausfall der Kommunikationstechnik** (Datenleitungen und/oder Sprachleitungen, z. B. Telefonanlage)
- **Keine Leistungserbringung für Kunden möglich** (aus unterschiedlichen Gründen wie z. B. umfangreicher Schaden am Betriebsgebäude, ausgefallene IKT-Systeme, Streik der Mitarbeiter etc.)
- **Verlust, Schaden oder Fehlfunktion von Produktionsanlagen**
- **Personal nicht verfügbar** (z. B. aufgrund von Grippepandemien oder Unfall)
- **Plötzliche Insolvenz oder Unterbrechung des Geschäftsbetriebes** (aufgrund einer Katastrophe) **bei einem wichtigen Zulieferer** (der wichtige Dienstleistungen oder Produkte zur Verfügung stellt) **oder bei einem Geschäftspartner** (an den eine wichtige Aktivität outgesourct wurde)
- **Verlust eines wichtigen Kunden**, der über 40 % des Umsatzes eingebracht hat
- …

Im Kapitel **13.3 Vorbereitung von Plänen und Umsetzung von Lösungen** werden Sie mehr über die Vorbereitung dieser Pläne für Ihr Unternehmen erfahren.

12.2.4. Ein Risiko geht, ein anderes kommt …

Oftmals führt die Minderung oder Eliminierung eines Risikos zur Entstehung eines neuen Risikos für Ihr Unternehmen. Das ist leider nicht zu vermeiden.

Zum Beispiel:

(1) Um das Risiko zu vermeiden, dass ein neues Produkt nicht genügend Kunden findet, könnten Sie sich dazu entschließen, das Produkt gar nicht erst einzuführen. Damit entsteht das Risiko, dass Ihr Unternehmen eine Marktchance verpasst, ein Wettbewerber diese Chance ergreift, das Produkt erfolgreich anbietet und die Position Ihres Unternehmens am Markt geschwächt wird.

(2) Die Anschaffung von Feuerlöschern vermindert die Auswirkung eines möglichen Brandes, jedoch kann sie dazu führen, dass (a) Mitarbeiter durch den Löschschaum

der Feuerlöscher verletzt werden und/oder (b), dass die Feuerlöscher nicht ordnungsgemäß gewartet werden und im Notfall unbrauchbar sind.

> Sie müssen sehr vorsichtig bei der Auswahl Ihrer Maßnahmen sein, um Ihr Unternehmen nicht neuen, ggf. nicht beachteten Risiken auszusetzen, deren potenzielle negative Auswirkungen eventuell sogar noch größer sein können als die des ursprünglichen Risikos.

12.2.5. Mehrere Handlungsoptionen für den Umgang mit Risiken können richtig sein

Für jedes Risiko in Ihrem Risikoregister kann es mehr als eine passende Handlungsoption geben. Entweder Sie wählen die beste Option aus oder wenden die verschiedenen Optionen aufeinander abgestimmt parallel an.

Es ist sehr ratsam, in diesen Fällen auch den Rat von externen Experten oder von Ihren Kollegen einzuholen. Auch das Internet bietet eine gute Quelle für weitere Informationen.

Brainstorming ist ein geeigneter Weg, um möglichst viele Lösungsoptionen zu identifizieren. In Ihrem Risikoregister sollten Sie aber nur die Handlungsoptionen erfassen, die wirklich dabei helfen, das Risiko zu mindern und von Vorteil für Ihr Unternehmen sind. Beurteilen Sie jede einzelne Idee mit Hilfe der folgenden Kriterien:

(a) Der Lösungsansatz ist umsetzbar und passt zu Ihrer Unternehmensgröße und zu Ihrem Unternehmenskontext.

(b) Die Methode wird das Risiko definitiv soweit mindern, dass es für das Unternehmen akzeptabel wird.

(c) Der Lösungsansatz schafft kein neues Risiko, das eine noch größere Gefahr für Ihr Unternehmen bedeutet.

(d) Die Kosten für die Umsetzung Ihres Lösungsansatzes sind nicht höher als die Kosten des Risikos, sollte dieses eintreten (Ausnahme sind Risiken des Arbeits- und des Gesundheitsschutzes, da der Wert des menschlichen Lebens und der Gesundheit nicht mit normalen Geschäftsrisiken gleichgesetzt werden kann).

12.2.6. Dokumentieren Sie Ihre Handlungsoptionen

Dokumentieren Sie in Ihrem Risikoregister alle Handlungsoptionen, die Sie für jedes Risiko identifiziert haben. Dazu nutzen Sie die Spalte „**mögliche Handlungs-optionen für das Risikomanagement**“.

Erasmus+

Risiko-Register für <Firma>
(Negative Risiken)

Risiko Nr.	Risikobereich	Risiko-Beschreibung / Risiko-Konsequenzen	Wahrschein-lichkeit	Auswirkung / Ausmaß	Risiko-Bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risiko-Bewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung	Notizen
002	Finanzielle Risiken	Einige Kunden sind nicht in der Lage zu zahlen Umsatzverluste in Höhe von 5.000 €	3	3	9	Verluste akzeptieren Gerichtliche Schritte einleiten Ausgaben reduzieren						
001	Operative Risiken	Feuer aufgrund eines fehlenden Rauchverbots in den Büros Verlust der Arbeitsstätte, Schließung des Unternehmens	2	4	8	Rauchen verbieten Notfallplan vorbereiten						
003	Unternehmens- & strategische Risiken	Marktinstabilität durch anstehende Wahlen Kunden könnten Aufträge zurückhalten	2	2	4	bessere Zahlungs-bedingungen anbieten Ausgaben reduzieren						
004	Unternehmens- & strategische Risiken	Unternehmensrisiko Nr. 4 Risiko-Konsequenz Nr. 4	1	4	4	Risikomanagement Nr. 4						
008	IKT Risiken	Unternehmensrisiko Nr. 8 Risiko-Konsequenz Nr. 8	1	2	2	Risiko akzeptieren						

Erasmus+

Chancen-Regi
(Positiv

Chance Nr.	Risikobereich	Chancen-Beschreibung / Chancen-Konsequenzen	Wahrschein-lichkeit	Auswirkung	Risiko-bewertung	mögliche Handlungsoptionen für das Risikomanagement
001	Operative Risiken	Höhere Verkaufszahlen aufgrund der neuen Webseite Plötzlicher Anstieg der Verkaufszahlen	3	3	9	auf Überstunden einstellen neue Mitarbeiter einstellen
005	Risiken im Personalbereich	Unternehmenschance Nr. 5 Chancen-Konsequenz Nr. 5	4	2	8	Risikomanagement Nr. 5
003	Unternehmens- & strategische Risiken	Ein Mitbewerber in der Stadt muss schließen Plötzlicher Anstieg der Verkaufszahlen	2	4	8	neue Mitarbeiter einstellen
004	Unternehmens- & strategische Risiken	Unternehmenschance Nr. 4 Chancen-Konsequenz Nr. 4	2	3	6	Risikomanagement Nr. 4
002	Finanzielle Risiken	Reduzierung des Kreditzinssatzes Kredit verringert sich um ca. 3.000,00 € jährlich	2	2	4	Risiko akzeptieren

12.2.7. Beispiele für mögliche Strategien zur Risiko-Minderung

Am Ende dieses Handbuches finden Sie in **Anhang 18.2** auf ca. 20 Seiten eine umfangreiche Liste mit **Beispielen für mögliche Strategien und Maßnahmen zur Risiko-Minderung**.

Diese Beispiele dienen Ihnen als Fundgrube für Ihre Entscheidungsfindung. Es ist keine vollständige Liste und es ist zu beachten, dass nicht alle Maßnahmen oder Strategien in jedem Unternehmen angewandt werden können.

12.3. Bewertung der Handlungsoptionen und Entscheidungsfindung

Sobald Sie alle Handlungsoptionen gesammelt haben, ist es an der Zeit zu entscheiden, welche der Möglichkeiten Sie umsetzen wollen.

Eine „**Kosten-Nutzen-Rechnung**“ bzw. die **Gegenüberstellung der Vor- und Nachteile**[15] wird Ihnen helfen, die beste Handlungsoption auszuwählen. Faktoren, die Sie berücksichtigen sollten, sind: Zeit, Aufwand, Komplexität, Risiko der Umsetzung, Vorteile, Nachteile etc.

Bei der Auswahl Ihrer bevorzugten Maßnahme sollten Sie darauf achten, dass die Risiko-Bewertung nach der Umsetzung der Maßnahme für das jeweilige Risiko so gering wie möglich wird.

Ein Beispiel:

Für ein bestimmtes Risiko mit einer Einstufung von 12 (Eintrittswahrscheinlichkeit 4 x Auswirkung 3) gibt es zwei Handlungsoptionen: A und B.

- Wenn Sie sich für Option A entscheiden, beträgt die neue Risiko-Bewertung 2 (Eintrittswahrscheinlichkeit 2 x Auswirkung 1). Dabei handelt es sich um eine akzeptable Risikoeinstufung (siehe Kapitel 12.2. (d) „RISIKO AKZEPTIEREN“).
- Wenn Sie sich für Option B entscheiden, beträgt die neue Risikoeinstufung 4 (Eintrittswahrscheinlichkeit 2 x Auswirkung 2). Dies ist keine akzeptable Risiko-Bewertung.

Sie würden in diesem Beispiel, vorausgesetzt die Kosten sind im Rahmen, Option A wählen, weil die Risiko-Bewertung besser ist.

Vergessen Sie auch nicht, dass Sie ein Risiko auch einfach „akzeptieren“ können. Sie können sich dazu entscheiden, Risiken zu akzeptieren und nichts dagegen zu unternehmen, sofern Sie diese Entscheidung wohl überlegt und auf der Basis ausreichender Informationen getroffen haben (hauptsächlich bei Risiken im grünen Bereich der Matrix, seltener bei Risiken im gelben und orangenen Bereich der Matrix). Mehr dazu können Sie in Kapitel 12.2. (d) nachlesen.

Nachdem Sie Ihre Entscheidungen getroffen haben, enthält Ihr Risikoregister alle von Ihnen ausgewählten Handlungsoptionen für jedes einzelne Risiko.

[15] Folgendes Vorgehen für die „Kosten-Nutzen-Rechnung“ bzw. die „Gegenüberstellung der Vor- und Nachteile“ ist möglich: Erstellen Sie eine Tabelle mit drei Spalten. Die Zeilen der ersten Spalte beinhalten Ihre unterschiedlichen Optionen, Lösungen oder Ideen, die verglichen werden sollen. Die zweite Spalte enthält die unterschiedlichen Kosten, Schwierigkeiten und Nachteile des Kaufes, der Umsetzung und der Ausführung der Alternativen aus Spalte 1. In der dritten Spalte stehen die Vorteile und Risiko-Bewertungen der Alternativen aus der ersten Spalte. Die Tabelle wird es Ihnen leichter machen, eine gute Entscheidung zu treffen.

12.4. Finanzierung Ihres Risikomanagements

Kein Unternehmen hat unendliche Ressourcen oder Finanzen zur Verfügung. Ein typisches KMU hat normalerweise sogar nur sehr wenige Ressourcen zur Verfügung, wenn es um Ausgaben geht, die nicht direkt mit dem operativen Geschäft zu tun haben. Ressourcen, ob Finanzen, Mitarbeiter, Zeit etc., sind im Normalfall immer knapp und ihre Umschichtung (oder die Beschaffung von zusätzlichen Mitteln) zu Gunsten anderer Aktivitäten wie dem Umgang mit Risiken verlangt von den verantwortlichen Akteuren jede Menge Energie und schwierige Entscheidungen.

Wenn Unternehmen sich entscheiden, ihre Risiken aktiv anzugehen, dann erhalten sie im ersten Schritt ein langes Risikoregister mit einer Vielzahl von Risiken. Es sollte beim Thema Kosten des Risikomanagements aber nicht vergessen werden, dass dabei auch eine beträchtliche Anzahl an Chancen identifizieren werden, und sich das Risikomanagement zumindest in Teilen selbst „finanzieren“ kann. Da der Umgang mit Ihren negativen Risiken fast immer Geld kosten wird, müssen Sie die Priorisierung Ihrer Risiken im zweiten Schritt vor dem Hintergrund Ihrer finanziellen Mittel bewerten.

Wir haben hier einige Punkte zusammengestellt, die Sie bei Ihrer Entscheidungsfindung unterstützen sollen:

A. Verstehen und akzeptieren Sie, dass die Risikobehandlung in Ihrem Unternehmen Zeit braucht. Auch wenn Sie alle nötigen Ressourcen zur Verfügung haben, werden Sie für die Umsetzung aller ausgewählten Handlungsoptionen einen längeren Zeitraum einplanen müssen.

B. Legen Sie Ihr verfügbares Budget fest, bevor Sie mit der Handlungsplanung beginnen.

C. Nutzen Sie die Liste der Handlungsoptionen, um das benötigte Budget für jede Handlungsoption vor der Umsetzung festzulegen.

D. Die Ergebnisse Ihrer bereits durchgeführten Priorisierung sind weiter relevant: Rote Risiken müssen dringender angegangen werden, als orange und gelbe.

E. Wählen Sie Dringlichkeit als Kriterium: Manche Risiken können nicht warten und haben einen bestimmten zeitlichen Rahmen (z. B. Fristen, die eingehalten werden müssen). Die dringendsten Risiken sind außerdem häufig diejenigen, die mit dem Schutz von Leben und Gesundheit zu tun haben.

F. Verschaffen Sie sich „leichte und schnelle Erfolge“: Es gibt normalerweise jede Menge Risiken, die nur einen geringen Aufwand und wenig Ressourcen benötigen. Nutzen Sie das zum Vorteil Ihrer Firma und als Ansporn für sich persönlich, um auch am Ball zu bleiben, wenn es schwieriger wird.

G. Überlegen Sie auch, ob Sie andere Projekte ggf. verschieben können. Vergleichen Sie deren Bedeutung mit dem Vorteil, ein bedeutendes Risiko für Ihre Firma eliminieren zu können (z. B. die Anschaffung eines neuen Autos könnte weniger wichtig sein, als die Vorbereitung eines Plans zur Sicherstellung des Geschäftsbetriebes im Bereich Ihrer IT-Systeme).

12.5. Aktualisieren Sie Ihr Risikoregister

Dokumentieren Sie in Ihrem Risikoregister, für welche Behandlungen Sie sich entschieden haben und welche Risiko-Bewertungen die Risiken danach aufweisen.

(a) Fügen Sie Ihre Handlungsoptionen in die Spalte „**mögliche Handlungsoptionen für das Risikomanagement**“ ein. Kennzeichnen Sie die von Ihnen ausgewählte Option eindeutig.

(b) Berechnen Sie die niedrigere, angepasste **Risiko-Bewertung nach dem Risiko-management** (neue Wahrscheinlichkeit und neue potenzielle Auswirkung nach der Umsetzung der ausgewählten Handlungsoption).

(c) Bestimmen Sie für jedes Risiko eine **für die Umsetzung zuständige Person**.

(d) Legen Sie einen **Zeitplan für die Umsetzung** der Maßnahme(n) fest.

Erasmus+

Risiko-Register für <Firma>
(Negative Risiken)

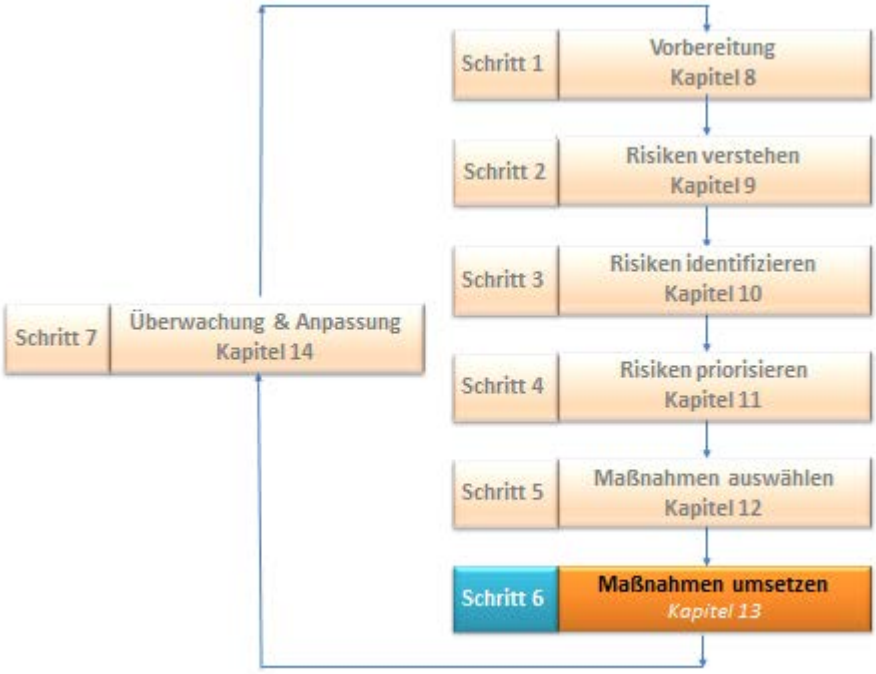
Risiko Nr.	Risikobereich	Risiko-Beschreibung / Risiko-Konsequenzen	Wahrschein-lichkeit	Auswirkung / Ausmaß	Risiko-Bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risiko-Bewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung	Notizen
002	Finanzielle Risiken	Einige Kunden sind nicht in der Lage zu zahlen Umsatzverluste in Höhe von 5.000 €	3	3	9	Verluste akzeptieren Gerichtliche Schritte einleiten Ausgaben reduzieren	2	2	4	Panayiotis P.	Start 1/8/2016 Ende 10/8/2016	
001	Operative Risiken	Feuer aufgrund eines fehlenden Rauchverbots in den Büros Verlust der Arbeitsstätte, Schließung des Unternehmens	2	4	8	Rauchen verbieten Notfallplan vorbereiten	1	4	4	Alexandros S.	Start 10/7/2016 Ende 15/9/2016	
003	Unternehmens- & strategische Risiken	Marktinstabilität durch anstehende Wahlen Kunden könnten Aufträge zurückhalten	2	2	4	bessere Zahlungs-bedingungen anbieten Ausgaben reduzieren	1	2	2	Michael K.	Start 1/5/2016 Ende 5/5/2016	
004	Unternehmens- & strategische Risiken	Unternehmensrisiko Nr. 4 Risiko-Konsequenz Nr. 4	1	4	4	Risikomanagement Nr. 4	1	1	1	Heike K.	Start 1/7/2016 Ende 3/7/2016	
008	IKT Risiken	Unternehmensrisiko Nr. 8 Risiko-Konsequenz Nr. 8	1	2	2	Risiko akzeptieren	1	2	2	-	-	

Erasmus+

Chancen-Register für <Firma>
(Positive Risiken)

Chance Nr.	Risikobereich	Chancen-Beschreibung / Chancen-Konsequenzen	Wahrschein-lichkeit	Auswirkung	Risiko-bewertung	mögliche Handlungsoptionen für das Risikomanagement	Wahrscheinlichkeit nach dem Risikomanagement	Auswirkung / Ausmaß nach dem Risikomanagement	Risikobewertung nach dem Risikomanagement	für die Umsetzung verantwortliche Person	Zeitplan für die Umsetzung	Notizen
001	Operative Risiken	Höhere Verkaufszahlen aufgrund der neuen Webseite Plötzlicher Anstieg der Verkaufszahlen	3	3	9	auf Überstunden einstellen neue Mitarbeiter einstellen	3	4	9	Pierre-Etienne M.	Start 1/6/2016 Ende 15/6/2016	
005	Risiken im Personalbereich	Unternehmenschance Nr. 5 Chancen-Konsequenz Nr. 5	4	2	8	Risikomanagement Nr. 5	3	2	6	Monika K.	Start 1/5/2016 Ende 5/5/2016	
003	Unternehmens- & strategische Risiken	Ein Mitbewerber in der Stadt muss schließen Plötzlicher Anstieg der Verkaufszahlen	2	4	8	neue Mitarbeiter einstellen	3	4	12	Boje D.	Start 1/8/2016 Ende 10/8/2016	
004	Unternehmens- & strategische Risiken	Unternehmenschance Nr. 4 Chancen-Konsequenz Nr. 4	2	3	6	Risikomanagement Nr. 4	2	8	8	Michael K.	Start 7/2016 Ende 30/10/2016	
002	Finanzielle Risiken	Reduzierung des Kreditzinssatzes Kredit verringert sich um ca. 3.000,00 € jährlich	2	2	4	Risiko akzeptieren	2	2	4	-	-	

13. Schritt 6 – Maßnahmen umsetzen



13.1. Umsetzungsplan

Manche Maßnahmen und Entscheidungen sind relativ einfach und benötigen daher keine detaillierte Planung. Bei anderen müssen Sie ggf. etwas anschaffen bzw. installieren (z. B. Feuerlöscher), Prozesse schriftlich festhalten oder Ihr Personal schulen etc. Diese Maßnahmen oder Aktivitäten müssen im Normalfall nur einmal umgesetzt werden. In einigen Fällen sind auch periodische Überprüfungen notwendig.

Für die komplexeren Maßnahmen empfehlen wir Ihnen, intern jeweils ein Projekt durchzuführen. Planen Sie für diese Projekte mindesten die folgenden Aspekte:

- Wer ist verantwortlich für die gesamte Projektumsetzung?
- Klar festgelegte Ziele.
- Ein detaillierter Handlungs- und Zeitplan.
- Eine Zusammenfassung der benötigten Ressourcen für die Projektumsetzung: Finanzierung, Ausrüstung, beteiligte Personen sowie Verantwortlichkeiten für die jeweiligen Ressourcen etc.

- Ein Kommunikationsplan, der die wichtigsten Interessenvertreter und Stakeholder auflistet und Möglichkeiten benennt, diese miteinzubeziehen etc.
- Eine Berechnung der erwarteten Risiko-Bewertung, die NACH der Umsetzung des Projektes erreicht werden soll (Restrisiko).

Der gesamte **Umsetzungsplan** muss vom Management genehmigt werden, da nur die Leitungsebene die notwendigen Ressourcen zur Verfügung stellen kann. Er wird ggf. separat dokumentiert werden.

13.2. Umsetzung von Maßnahmen und Lösungen im Bereich Informationssicherheit

Wie bereits diskutiert, differenziert man Maßnahmen und Lösungen im Bereich Informationssicherheit in zwei Bereiche (siehe Kapitel 12.2.2. Umgang mit IT Risiken).

Diese Maßnahmen und Lösungen umzusetzen, verlangt dagegen nach einer Einteilung in drei Bereiche (!):

- Umsetzung von Maßnahmen im strategischen bzw. unternehmerisch, operativen Bereich
- Umsetzung von Maßnahmen im technischen Bereich
- Kontrolle der Maßnahmen und Lösungen, die genutzt werden

(a) <u>Umsetzung von Maßnahmen im strategischen bzw. unternehmerisch, operativen Bereich</u>

1) <u>IKT-Strategien des Unternehmens</u>

Die meisten IKT-Strategien folgen einem standardisierten Umsetzungsprozess: Auswahl einer technologischen Lösung, die dann in Verbindung mit unternehmensinternen Schulungen implementiert wird.

Ihr Technologie-Dienstleister kann Sie bei der Überwachung der Umsetzung unterstützen. Stellen Sie sicher, dass Sie eine klare Vorstellung davon haben, was Sie geliefert bekommen und dass Sie alle relevanten Dokumentations-Unterlagen erhalten (z. B. Anleitungen, Netzwerkpläne etc.).

2) Auswahl eines oder mehrerer IKT-Dienstleister

Sobald Sie sich für den/die Dienstleister entschieden haben, stellen Sie sicher, dass alle Leistungen und Parameter der Kooperation in einem Vertrag dokumentiert werden. Ziehen Sie ggf. Ihren Rechtsberater hinzu, um Sie dabei zu unterstützen. Vergessen Sie nicht, die Verpflichtungen des/der Dienstleister(s) im Bereich Informationssicherheit zu dokumentieren.

3) Unternehmensinterne Regeln und Prozesse

Dies ist wahrscheinlich das am schwersten umzusetzende Projekt. Sobald unternehmensinterne Regeln oder Prozesse neu festgelegt werden (z. B. ein Klassifizierungssystem, um vertrauliche Dokumente zu kennzeichnen und diese sicher verschlossen aufzubewahren), **müssen sie zu einem normalen Bestandteil des täglichen Geschäftsbetriebs werden. Sie müssen für alle Mitarbeiter und Manager zur Routine werden!**

Dazu gehen Sie in der Regel in vier Stufen vor:

a) Finalisieren Sie die neue Regel bzw. den Prozess und DOKUMENTIEREN Sie diese in schriftlicher Form.

b) Weisen Sie Ihre Mitarbeiter auf die neue Regel/Richtlinie hin und führen Sie SCHULUNGEN durch, um die Umsetzung zu gewährleisten.

c) Führen Sie die Regel/Richtlinie in Ihren täglichen Geschäftsbetrieb ein.

d) KONTROLLIEREN SIE REGELMÄSSIG, ob die Regel/Richtlinie im täglichen Geschäftsbetrieb von jedem respektiert wird (inkl. der Unternehmensinhaber). Stellen Sie sicher, dass sie zu einem Unternehmensstandard wird.

   Führen Sie unregelmäßige Überprüfungen und interne Revisionen durch, um sicherzustellen, dass sich jeder an die Regel/Richtlinie hält.

   Ergreifen Sie ggf. disziplinarische Maßnahmen, falls die Regel/Richtlinie missachtet wird. Vielleicht müssen Sie auch die Schulungen dazu wiederholen.

Die Stufen (b) und (d) sind am wichtigsten, wenn Sie eine neue Regel/Richtlinie einführen.

(b) Umsetzung von Maßnahmen im technischen Bereich

In diesem Bereich sollten Sie Ihren IKT-Berater bzw. -Dienstleister bei der Umsetzung zu Rate ziehen.

Neben der technologischen Umsetzung und der Installation könnten hier auch interne Schulungen der Nutzer notwendig werden (z. B. beim Thema Verschlüsselung und Entschlüsselung von Daten auf Computern etc.).

(c) Kontrolle der Maßnahmen und Lösungen

Wie bereits erwähnt, müssen Sie sicherstellen, dass die neu eingeführten Regelungen und Richtlinien im Geschäftsalltag auch von allen respektiert werden.

Es gibt vier Möglichkeiten, dies zu kontrollieren:

1) Geben Sie einem bestimmten Mitarbeiter die Verantwortung, die Regeln oder Richtlinien im Geschäftsalltag zu verankern. Direkt nach der Einführung soll der Mitarbeiter vor allem darauf achten, ob die neue Regel/Richtlinie überwiegend befolgt wird.

Es kann durchaus passieren, dass bei der Umsetzung weitere Verbesserungsmöglichkeiten sichtbar werden. Nehmen Sie die notwendigen Änderungen vor und setzten Sie die generelle Umsetzung der neuen Regel/Richtlinie dann fort.

2) Setzen Sie Disziplinarmaßnahmen durch (die Wiederholung einer Schulung ist ein weniger strenges Beispiel), insbesondere für die Mitarbeiter, die die neue Regel/Richtlinie bewusst umgehen oder „vergessen“.

Wenn Sie einen Verstoß feststellen, sorgen Sie sofort dafür, dass die Regel/Richtlinie wieder befolgt wird. Stellen Sie sicher, dass verstanden wird, wie ernst es Ihnen damit ist.

3) Führen Sie regelmäßige UND unangekündigte Prüfungen für jede Regel/Richtlinie durch. Anfangs sollte das relativ häufig passieren, später in längeren Intervallen.

4) Manche Unternehmen nutzen bestimmte Softwareüberwachungs-Programme, die Alarm schlagen, wenn eine Gefährdung für das IKT System

besteht. Solche Softwarelösungen können in vielen Fällen eine Abweichung von festgelegten Richtlinien verhindern. Besprechen Sie diese Option mit Ihrem IKT-Berater und überlegen Sie unter Berücksichtigung der Kosten eine eventuelle Anschaffung.

Wir empfehlen Ihnen, dass Sie alle Ihre Sicherheitsmaßnahmen einmal im Jahr von einem externen Berater kontrollieren lassen. Dieser wird Sie auf eventuelle Sicherheitslücken und Schwachstellen aufmerksam machen. Mit Hilfe dieser Informationen können Sie notwendige Anpassungen vornehmen und Ihr Unternehmen noch besser schützen.

Vergessen Sie nicht, dass Sicherheit ein sehr dynamisches Thema ist, das sich schnell ändern kann. Regelmäßige Kontrollen, Überwachungen, Prüfungen und Verbesserungen Ihres Systems sind darum unbedingt erforderlich.

Last but not least: Denken Sie an die regelmäßige Schulung Ihrer Mitarbeiter, so dass sich das Thema Sicherheit fest in der DNA Ihres Unternehmens festsetzt.

13.3. Vorbereitung von Plänen und Umsetzung von Lösungen

Manche Maßnahmen verlangen nach umfassenden Plänen. Dabei handelt es sich um dokumentierte Vorgehensweisen und wichtige Informationen, die genutzt werden, wenn der Geschäftsbetrieb durch eine bestimmte Bedrohung Gefahr läuft, unterbrochen zu werden oder bereits unterbrochen wurde. Diese Pläne unterstützen Ihr Unternehmen dabei, die richtigen Maßnahmen in solchen negativen Situationen zu ergreifen und den Geschäftsbetrieb erfolgreich wiederherzustellen.

Die Erstellung dieser Pläne ist unbedingt notwendig bei Risiken mit niedriger Eintrittswahrscheinlichkeit und hoher Auswirkung oder bei Risiken mit hoher Eintrittswahrscheinlichkeit und hoher Auswirkung, die auf keine andere Art und Weise weiter reduziert werden können.

Eine nicht vollständige Liste dieser Gefahren beinhaltet:

- Naturkatastrophen (Überschwemmungen, Winterstürme, extreme Temperaturen, Erdbeben, Erdrutsche, Waldbrände etc.)

- Technische Gefahren (Stromausfälle, Geräteausfälle, Cyber-Sicherheit, Freisetzung von gefährlichen Stoffen etc.)
- Terrorismus und Gewalt (Bombenanschläge, Entführungen, chemische oder biologische Bedrohungen, Gewalt am Arbeitsplatz, Aufstände, etc.)
- Geschäftsrisiken (Ausfall eines wichtigen Geschäftspartners etc.)

Sie sollten sich darüber im Klaren sein, dass gewisse Pläne (z. B. der Back-Up- und der Wiederaufbauplan) die zusätzliche Bereitstellung und Umsetzung von technischen Lösungen bzw. Systemen notwendig machen (z. B. neue Festplatte für Back-Ups oder ein weiterer Server an einem alternativen Standort etc.). Vergessen Sie nicht, finanzielle Mittel dafür einzuplanen. Ein Plan ist nur dann ein guter Plan, wenn die notwendigen technischen Lösungen bei Bedarf auch vorhanden sind und funktionieren.

13.3.1. Wie viele Pläne sind notwendig?

SO VIELE WIE SIE BENÖTIGEN! Es gibt keine Einschränkung für die Anzahl Ihrer Notfallpläne. Eine nicht vollständige Liste möglicher Anwendungsbereiche beinhaltet:

- Plan zum Umgang mit Vorfällen und Krisen
- Notfall- und Evakuierungsplan[16]
- Versicherungsplan
- Vertretungsplan
- Plan für Herausforderungen mit Zulieferern, Geschäftspartnern etc.
- IT Back-Up Plan
- Kommunikations- und Benachrichtigungsplan
- Ressourcen und Wiederaufbauplan
- Plan zum Umgang mit Informationssicherheits-Vorfällen

[16] Notfall- und Evakuierungspläne sind in den meisten Ländern verpflichtend.

Sie sollten weitere Pläne vorbereiten, wenn Sie für Ihr Unternehmen notwendig sind. In den folgenden Passagen konzentrieren wir uns auf die Pläne in dieser Liste und wie Sie die Pläne erarbeiten können. Wir helfen Ihnen damit, Ihr Unternehmen widerstandsfähiger zu machen.

13.4. Ihr „Plan zur Sicherstellung des Geschäftsbetriebes“ – ein Plan, der alle Pläne beinhaltet

In unserem Ansatz fassen wir alle diese Pläne in einem integrierten Plan für Ihr gesamtes Unternehmen zusammen. Dabei handelt es sich um den sog. „Plan zur Sicherstellung des Geschäftsbetriebes“ – ein einzelnes Dokument, das alle erwähnten Pläne in unterschiedlichen Bereichen bzw. Kapiteln (z. T. mit Anhängen) beinhaltet.

Bitte nutzen Sie die Vorlage **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** im Anhang (Word-Dokument zum Download). In diese Vorlage wurden bereits alle Pläne und weitere notwendige Informationen integriert.

Sobald Sie alle Pläne erarbeitet haben, werden diese Ihnen überlebenswichtige Dienste leisten, sollte Ihr Unternehmen von Notfällen, negativen Zwischenfällen, Sicherheitsproblemen oder anderen katastrophalen Ereignissen betroffen werden.

13.4.1. Vier wichtige Vorüberlegungen

Es gibt vier wichtige Punkte, zu denen Sie sich bei der Erstellung des Dokuments Gedanken machen sollten:

(a) Es sollte **regelmäßig aktualisiert** werden (z. B. alle 3, 6 aber maximal alle 12 Monate). Die Erstellung der ersten Version ist relativ aufwendig, die Aktualisierung der Informationen benötigt dagegen vergleichsweise wenig Zeit und Aufwand.

(b) Stellen Sie sicher, dass Ihre **Mitarbeiter den Plan kennen und entsprechend geschult werden**. Die Schulungen verlangen nur ein wenig Zeit und Aufwand, die Vorteile sind dagegen enorm.

(c) **Bewahren Sie eine Kopie der aktuellen Version des Dokuments außerhalb Ihrer Räumlichkeiten auf**, auf die Sie trotzdem bei Bedarf **sofort zugreifen** können.

(d) **Klassifizieren Sie den Plan als vertrauliches Dokument**. Die Informationen darin sind vertraulich und sehr wichtig für Ihr Unternehmen, also wollen Sie nicht, dass ein Wettbewerber sie zu Gesicht bekommt.

Bitte beachten Sie alle vier Punkte. Sie sind alle wichtig!

13.4.2. Struktur des Plans zur Sicherstellung des Geschäftsbetriebes

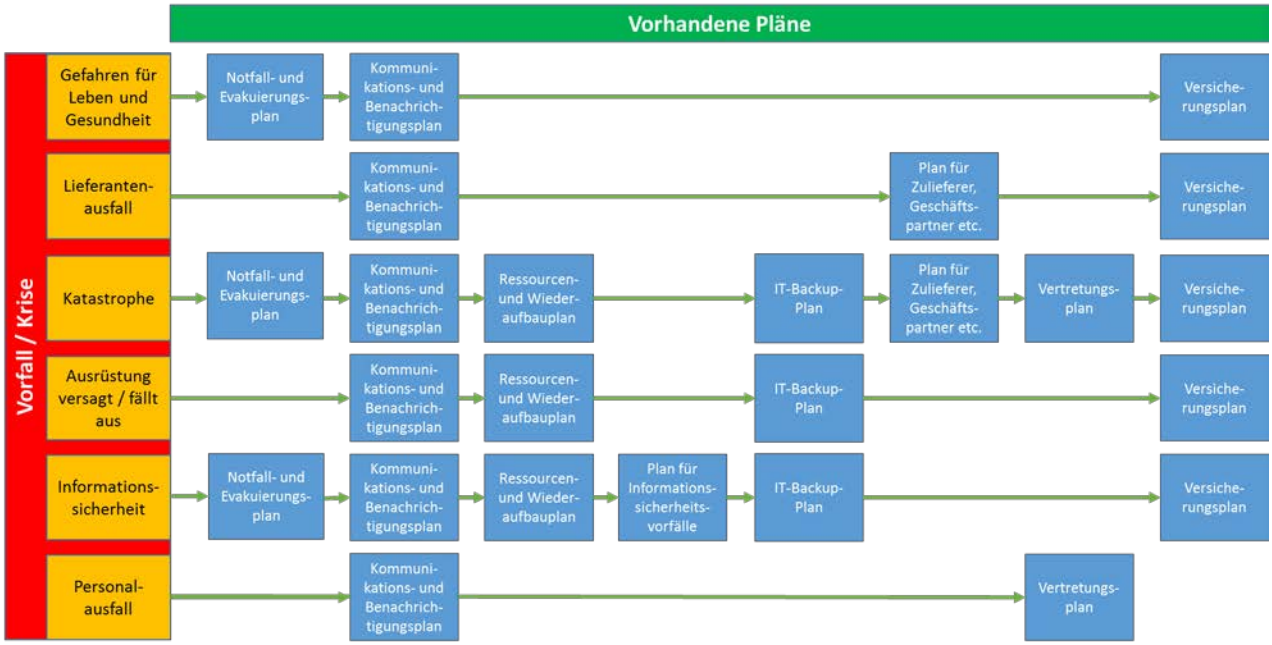
Ihr Plan zur Sicherstellung des Geschäftsbetriebes ist ein einziges, integriertes Dokument, das die diversen Teil-Pläne zusammenführt. Das zweite (B) und das dritte Kapitel (C) sind einführende Abschnitte mit allgemeinen Informationen.

Kapitel (B) ist eine allgemeine Einführung, die sich auf das gesamte Dokument bezieht.

Die wichtigsten Bestandteile von Kapitel B sind:

- Die Adresse der Räumlichkeiten Ihres Unternehmens
- Der externe Aufbewahrungsort, an dem sich eine Kopie dieses Plans befindet
- Die jeweils verantwortlichen Personen für die Teil-Pläne; in einem KMU kann es sich dabei durchaus um dieselbe Person für alle Pläne handeln
- Informationen über die letzte Aktualisierung des Plans und wann die nächste Aktualisierung stattfinden soll

In Kapitel (C) finden Sie unter anderem eine Übersicht aller Pläne (siehe Schaubild unten), die Sie für eventuell auftretende Zwischenfälle vorbereitet haben. Je nach Art des Zwischenfalls werden Sie mehrere Teilpläne gleichzeitig beziehungsweise nacheinander aktivieren und umsetzen müssen.



Das Schaubild dient Ihnen zur Orientierung. Sie werden nicht immer exakt so vorgehen müssen, z. B. weil in manchen Fällen nicht alle Pläne benötigt werden (beispielsweise werden Sie im Falle einer Naturkatastrophe ggf. keinen Vertretungs-plan benötigen, wenn alle Mitarbeiter glücklicherweise trotzdem verfügbar sind).

Jeder der folgenden Abschnitte in diesem Handbuch behandelt einen der Teil-Pläne, die oben bereits erwähnt wurden.

Es gibt in den einzelnen Kapiteln der Vorlage diverse Tabellen. Bitte tragen Sie hier jeweils die spezifischen Informationen für Ihr Unternehmen ein. Sie finden mehrere gelbe Markierungen in der Vorlage. Das sind potenzielle Startpunkte für die Erarbeitung und Eintragung Ihrer Informationen. Darüber hinaus enthält die Vorlage Beispiele, um Ihnen zu einem besseren Verständnis der benötigten Inhalte zu verhelfen. Nicht alle Inhalte treffen auf jedes Unternehmen zu, jedoch wurde darauf geachtet, dass die zur Verfügung gestellten Informationen in den meisten Fällen Gültigkeit haben. Bitte ändern Sie das Dokument aber nach Belieben, bis es zu Ihrem Unternehmen passt. Fügen Sie Ihre eigenen Spalten hinzu oder lassen Sie diverse Bereiche unausgefüllt, wenn diese für Sie nicht relevant sind.

In den folgenden Abschnitten finden Sie Informationen über jeden einzelnen Plan. Zusätzlich enthält die Vorlage weitere Anweisungen, die Sie gerne parallel studieren können.

13.4.3. Plan zum Umgang mit Vorfällen und Krisen

In dem untenstehenden Schaubild können Sie erkennen, wie typischerweise auf Vorfälle oder Krisen reagiert werden muss. Eine detaillierte Anleitung dazu finden Sie in der Vorlage des Plans, hier folgen einige notwendige Erklärungen und Anweisungen.

Es hängt von der Art, dem Umfang und den Konsequenzen eines Vorfalles ab, ob Sie die einzelnen Schritte schneller oder langsamer umsetzen müssen.

Zum Beispiel kann ein Vorfall im ersten Schritt entweder bereits passiert sein oder er passiert gerade. Bevor Sie einen Vorfall erkennen, können Minuten, Stunden, Tage oder sogar Monate vergehen. Ein Feuer wird oftmals innerhalb von Sekunden oder Minuten bemerkt werden (wenn es während der normalen Bürozeiten ausbricht); das Hacken Ihres ERP-Systems könnte auch sofort erkannt werden, es ist aber auch möglich, dass dieser Vorfall erst mehrere Stunden, Tage (falls über mehrere Tage

nicht mit dem ERP-System gearbeitet wurde) oder sogar erst Monate später entdeckt wird (z. B., wenn Kundendaten illegal kopiert und Ihren Wettbewerbern zugespielt wurden).

In Schritt 2 (vgl. Schaubild) hat ein Mitarbeiter bemerkt, dass es einen Vorfall gibt. Dabei könnte es sich um eine Fehlfunktion handeln (z. B. technische Probleme mit dem ERP-Server), die Dienstleistungserbringung eines Zulieferers könnte beeinträchtigt sein (z. B. kein Internetzugriff aufgrund von Problemen Ihres Internetproviders) oder eine Ihrer eigenen Dienstleistungen für Ihre Kunden könnte behindert sein (von Hacking bis hin zu einem nicht richtig verbundenen Kabel kann es dafür einfache oder schwerwiegende Ursachen geben).

Bei der ersten Diagnose spielen mehrere Faktoren eine Rolle, zum Beispiel:

- Handelt es sich um einen echten Vorfall (oder liegt eventuell ein Fehlalarm vor)?
- Worum geht es in dem Vorfall wirklich?
- Handelt es sich um Serverprobleme oder sind Hacker in Ihr System eingedrungen? Oder wurde eventuell (unabsichtlich) nur ein Kabel nicht richtig verbunden?
- …

Diagnose bedeutet die Art, den Umfang und die Auswirkung des Vorfalles zu verstehen. Das ist ein sehr wichtiger Schritt.

Basierend auf Ihrer Diagnose können Sie sich für eine Strategie entscheiden und die nächsten Schritte einleiten.

WICHTIGE ANWEISUNG: Egal wie Sie vorgehen, beachten Sie das Folgende: **Wenn von dem Vorfall eine Gefahr für Leben oder Gesundheit ausgeht oder ausgehen könnte, müssen Sie UMGEHEND Ihren Notfall- und Evakuierungsplan aktivieren und umsetzen.**

Die Reaktion auf einen Vorfall oder die Bewältigung einer Krise ist komplex (vgl. Schritt 4). Sie werden von Fall zu Fall reagieren und entscheiden müssen. In manchen Fällen werden Sie die Behörden informieren (Feuer, Diebstahl, Betrug etc.), während in anderen Fällen nur die Reparatur eines bestimmten Gerätes notwendig ist.

Bei Vorfällen, die weitreichende Konsequenzen für Ihr Geschäft, Ihre Marke, Ihr Renommee oder sogar für Leib und Leben haben können, gibt es keine Musterlösung. Ihr Krisenmanagement wird sehr spezifisch auf die jeweilige Herausforderung zugeschnitten sein. Folgende Punkte sollten Sie dennoch beachten:

- Nutzen Sie Ihren gesunden Menschenverstand und Ihre Erfahrungen.
- Verschaffen Sie sich einen guten Überblick von allen Auswirkungen und Konsequenzen.
- Sie werden im Zusammenhang mit der Krise verschiedene Bereiche managen müssen (Mitarbeiter, Interessenvertreter/Stakeholder, Rechtsberater, Finanzen etc.).
- Eine gute Vorbereitung auf Krisen ist entscheidend.
- Kommunikationsmanagement: Wer muss wann über was informiert werden?

Für Vorfälle im Zusammenhang mit Informationssicherheits-Verstößen sprechen Sie bitte umgehend mit Ihrem IKT-Berater oder -Dienstleister (wenn dieser Teil des Problems ist, sollten Sie sich Unterstützung von einem Dritten holen).

Schritt 5 zeigt Ihnen, dass es auch noch einiges zu tun gibt, wenn die Krise überwunden ist und Sie Ihren normalen Geschäftsbetrieb wiederaufnehmen konnten:

- Identifizieren Sie die Ursache des Problems und beheben Sie diese wenn möglich, sodass das Problem möglichst nicht wieder auftreten kann.
- Identifizieren Sie, welche Teil-Pläne Ihres Plans zur Sicherstellung des Geschäftsbetriebes verbessert werden müssen. Folgendes könnte z. B. angepasst werden:
    - Ausführlichere Dokumentation in den einzelnen Teil-Plänen
    - Optimierung Ihrer Mitarbeiterschulungen

- Umsetzung von bisher nicht vorhandenen Lösungen, die sich als hilfreich erwiesen hätten (z. B. Back-Up-Server an einem alternativen Standort)
- …

Stellen Sie sicher, dass Sie möglichst alle Sicherheitslücken schließen und den damit verbundenen Risiken keine Chance geben, Sie erneut zu schädigen.

13.5. Notfall- und Evakuierungsplan

Dieser Plan bezieht sich auf das Thema Gesundheit und die Sicherheit in lebensbedrohlichen Situationen, wie Feuer, Erdbeben etc.

Wir empfehlen Ihnen, dass Sie **Kapitel D** aus der Vorlage heranziehen, wenn Sie Ihren hausinternen Notfalls- und Evakuierungsplan vorbereiten. Die Vorlage finden Sie in Anhang **18.3 Plan zur Sicherstellung des Geschäftsbetriebes**.

13.6. Versicherungsplan

Der Abschluss einer Versicherung ist eine der beliebtesten Strategien zur Risikoübertragung. Sie zahlen einen vergleichsweise überschaubaren Betrag an ein Versicherungsunternehmen und Sie erhalten einen Großteil (oder den Gesamtgegenwert) Ihres Schadens erstattet. Dies ist v. a. relevant bei großen und existenzbedrohenden Gefahren (z. B. Gebäudeschaden, Vermögensverlust, längerer Betriebsstillstand etc.), deren Folgen Ihr Unternehmen aus eigener Kraft finanziell nicht verkraften kann.

Dabei gilt es auf folgendes zu achten:

- Ihre Versicherungspolice ist gültig und der Versicherungsschutz ist nicht abgelaufen.
- Der Versicherungsschutz Ihrer einzelnen Verträge ist ausreichend, um potenzielle Verluste abzudecken oder zu vermindern. Die Entscheidung über die angemessene Abdeckung Ihrer Risiken wurde von Ihrem Management bzw. dem Inhaber zusammen mit Ihrem Versicherungsberater getroffen. Beachten Sie: Eine zu hohe Risikoabdeckung führt zu überhöhten Kosten, während eine

Unterdeckung die Gefahr birgt, dass die Zahlung der Versicherung im Schadensfall zu niedrig ausfällt.

- Die Auszahlung einer (hohen) Versicherungssumme macht eine Katastrophe nicht ungeschehen. Sie erhalten (immerhin) eine Menge Geld, Ihre Kunden sind aber trotzdem verloren, wenn Sie keinen passenden Wiederaufbauplan für Ihre Dienstleistungen haben. Wir empfehlen Ihnen, den Versicherungsplan daher unbedingt in Kombination mit Ihrem Gesamtplan zur Sicherstellung des Geschäftsbetriebes und mit dem Wiederaufbauplan zu erstellen.

Bei der Erstellung Ihres Versicherungsplans können Sie auf **Kapitel E** der Vorlage zurückgreifen. Die Vorlage finden Sie in Anhang **18.3 Plan zur Sicherstellung des Geschäftsbetriebes**. Diese unterstützt Sie in folgenden Punkten:

(a) Bewertung Ihres aktuellen Versicherungsschutzes und Identifizierung von möglichen oder notwendigen Verbesserungen.

(b) Sie besitzen eine aktuelle Auflistung aller Versicherungen, die zusammen mit Ihren anderen Plänen aufbewahrt wird, sodass Sie im Falle eines negativen Zwischenfalles alle wichtigen Informationen zur Hand haben.

Wir empfehlen, dass Sie diese Liste immer dann aktualisieren, wenn ein Versicherungsvertrag erneuert oder verändert wird und Sie die gesamte Liste zusätzlich einmal im Jahr vollständig überprüfen (z. B. in einem Gespräch mit Ihrem Versicherungsberater).

13.7. Vertretungsplan

Sie sollten einen Vertretungsplan für jeden Mitarbeiter Ihres Unternehmens haben (inklusive sich selbst), um sicherzustellen, dass kein einzelner Mitarbeiter bei Ausfall für den Stillstand des gesamten Betriebes verantwortlich sein kann. Besonders relevant ist der Vertretungsplan für Mitarbeiter in Schlüsselpositionen. In Ihrem Vertretungsplan geht es nicht darum, wer wessen Platz im Unternehmen einnimmt, wenn ein Mitarbeiter das Unternehmen verlässt. Vielmehr wird hiermit geplant, wer die Aufgaben übernehmen kann, wenn ein Mitarbeiter gerade nicht verfügbar ist. In einem typischen KMU gibt es normalerweise keine freien personellen Ressourcen und Ihre Mitarbeiter werden wahrscheinlich mehrere Rollen und Verantwortlichkeiten zusätzlich übernehmen müssen. Gerade deshalb sollten Sie aber Ihren derzeitigen

Status analysieren, um die Lücken und Risiken in Ihrer aktuellen Personalstruktur zumindest zu kennen.

Dokumentieren Sie alle relevanten Informationen in **Kapitel F** der Vorlage, die Sie im Anhang **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** finden können**.**

13.8. Plan für Herausforderungen mit Zulieferern, Geschäftspartnern etc.

Der Ausfall eines wichtigen Zulieferers oder Geschäftspartners, der dem Unternehmen notwendige Produkte oder Dienstleistungen zur Verfügung stellt, kann einen signifikanten Einfluss auf Ihren Geschäftsbetrieb und die Verfügbarkeit Ihrer Dienstleistungen haben.

Wir empfehlen Ihnen daher die Suche nach alternativen Unternehmen, die Ihnen im Ernstfall die gleichen Produkte oder Dienstleistungen (bei gleichbleibender Qualität) liefern können.

Dokumentieren Sie alle relevanten Informationen in **Kapitel G** der Vorlage, die Sie im Anhang **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** finden können**.**

13.9. IT-Back-Up-Plan

Ein Back-Up Ihrer IT-Daten zu erstellen bedeutet, dass Sie eine elektronische Kopie aller Daten Ihrer IKT-Systeme auf einem externen Gerät erstellen. Es ist extrem wichtig, Kopien Ihrer IT-Daten zu haben. Tatsächlich ist die Kopie mindestens genauso wichtig wie das Original. Dafür gibt es mehrere Gründe, zum Beispiel:

- Falls Ihr IKT-System aus irgendwelchen Gründen zerstört wird (Störung, kaputte Festplatte, Zerstörung durch Feuer/Wasser etc.), verlieren Sie auch Ihre gesamten Daten. Auch wenn Sie relativ einfach Ersatz für das verlorene System beschaffen können, so ist die Wiederherstellung der Daten oftmals schwierig bis unmöglich.
- Einzelne Daten oder Dateien in Ihrem IKT-System könnten aufgrund technischer Fehler beschädigt sein. Das führt dazu, dass Sie diese Daten oder Dateien nicht öffnen bzw. nicht darauf zugreifen können – ein weiterer Fall, der die Notwendigkeit eines Back-Ups aufzeigt.

- Es passiert täglich, dass Nutzer unabsichtlich Dateien, Archive oder andere Informationen in Systemen oder auf Festplatten löschen. Das stellt absolut kein Problem dar, sofern Sie ein Back-Up der Dateien haben.

Beginnen Sie damit, jemandem die Verantwortlichkeit für die Back-Ups Ihrer Unternehmensdaten zu übertragen. Diese Person ist dann für alle Aspekte des Back-Ups verantwortlich.

Wichtig: Wir empfehlen Ihnen hier die Zusammenarbeit mit einem externen IKT-Berater oder -Dienstleister, es sei denn, Sie haben einen Mitarbeiter, der alle notwendigen Qualifikationen mitbringt.

Erarbeiten Sie eine Back-Up-Strategie für Ihr Unternehmen. Die notwendigen Informationen fügen Sie in **Kapitel H** der Vorlage ein, die Sie im Anhang **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** finden.

Stellen Sie sicher, dass dieser Plan regelmäßig überprüft und aktualisiert wird.

13.10. Kommunikations- und Benachrichtigungsplan

Eine der wichtigsten Aufgaben während eines Notfalls (und auch nach einem zerstörerischen oder katastrophalen Ereignis) ist die effektive Kommunikation mit den Interessenvertretern bzw. Stakeholdern im Umfeld Ihres Unternehmens. Dies beinhaltet die Kommunikation mit:

- Mitarbeitern und Management
- Anteilseignern
- Kunden
- Behörden und Notfalldiensten
- Zulieferern, Geschäftspartnern etc.
- Nachbarn und der relevanten Öffentlichkeit

- Medien
- …

Falls der Zwischenfall Ihr Unternehmen direkt betrifft, vergessen Sie nicht, ggf. Ihren Rechtsberater heranzuziehen.

Dokumentieren Sie alle notwendigen Informationen in **Kapitel I** der Vorlage, die Sie im Anhang **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** finden.

13.10.1. Verantwortlichkeit für die Kommunikation

Geben Sie jemandem die Verantwortlichkeit für die interne und externe Kommunikation des Unternehmens und bestimmen Sie auch einen Stellvertreter. Diese Personen sind die einzigen Ansprechpartner. Alle Mitarbeiter müssen das wissen, damit jegliche Kommunikation über diese Personen läuft.

13.10.2. Notfallbenachrichtigung

Im Kommunikationsplan gibt es eine Mitarbeiterliste, die genutzt werden sollte, um alle Mitarbeiter zu benachrichtigen (z. B. wenn der Wiederaufbauplan umgesetzt werden soll).

13.10.3. Kontaktnummern im Krisenfall

Es ist wichtig, alle Kommunikationskanäle Ihres Unternehmens offen und zugänglich zu halten (Telefonleitungen, Fax, E-Mail). Im Falle einer Katastrophe an Ihrem Standort kann es passieren, dass Sie Telefonanrufe auf eine andere funktionierende Nummer umleiten müssen, auf die Sie dann zugreifen können (z. B. auf Ihr Mobiltelefon). Stellen Sie sicher, dass Sie alle notwendigen Vorkehrungen getroffen haben und die notwendigen Informationen dazu in Ihrem Kommunikationsplan dokumentiert sind.

13.11. Ressourcen und Wiederaufbauplan

Dieser Plan deckt alle operativen Ausfälle ab. Störungen können interne oder externe Gründe haben. Dazu zählen Ausfall von Anlagen, Stromausfälle, nicht verfügbare Mitarbeiter, Ausfälle von wichtigen Zulieferern, Katastrophen, Bombendrohungen etc. Diese Vorfälle könnten den Geschäftsbetrieb erheblich stören oder sogar ganz unterbrechen.

13.11.1. Vorfallkategorien und Reaktionsstrategien

Störende Zwischenfälle können in zwei Hauptkategorien unterteilt werden:

(a) **Nichtverfügbarkeit, Ausfall oder Fehlfunktion** von jeder Art von Ressourcen, wie z. B.:

- Fehlfunktion oder Ausfall der IT-Infrastruktur (Server, Computer, Drucker etc.)
- Ausfall von IT-Anwendungen
- Ausfall oder Fehlfunktion der Büroausstattung (Fax, Kopiergerät, Telefonanlage etc.)
- Fehlfunktion oder Verlust der Infrastruktur (z. B. Lager, Serverraum etc.)
- Verlust oder Nichtverfügbarkeit von Dateien und Archiven (elektronisch, auf Papier etc.)
- Fehlfunktion oder Verlust von Produktionsanlagen
- Versorgungs- und Kommunikationsausfall (Strom, Wasser, Datentransfer, Sprachleitungen etc.)
- Nichtverfügbare Mitarbeiter (aus unterschiedlichen Gründen wie Grippepandemien, Feuer, Verletzungen etc.)
- Ausfall eines wichtigen Geschäftspartners oder Zulieferers
- Räumlichkeiten temporär nicht verfügbar (z. B. Evakuierung und kein Zutritt aufgrund einer Bombendrohung)

(b) **Notfälle: Komplettversagen oder Totalverlust** von Betriebsgebäude, Infrastruktur, Geräten, Anlagen, Dateien und Informationen aufgrund eines katastrophalen Ereignisses (Feuer, Überschwemmung, Erdbeben etc.). Das ist

das mit Abstand komplexeste Szenario, wenn alle oder viele der oben dargestellten Probleme gleichzeitig auftreten.

Sie gehen damit um, indem Sie zwei unterschiedliche Ansätze bzw. alternative Vorgehensweisen erarbeiten:

(a) Ansatz für Nichtverfügbarkeit, Ausfall oder Fehlfunktion von Ressourcen

Diese Vorfälle könnten tagtäglich in Ihrem Geschäftsalltag passieren: das Faxgerät ist defekt, Ihr IT-Server-Systems fällt aus, eine Software funktioniert nicht oder es gibt in Ihrer Region einem kompletten Stromausfall.

Beispiele für Vorgehensweisen, die Sie umsetzen können, sind:

- Schließen Sie Support- und Wartungsverträge mit Ihren wichtigsten Zulieferern bzw. Dienstleistern ab:
    - Vor-Ort-Service- bzw. Reparaturvertrag im Falle eines Serverausfalls.
    - Vertrag für die Reparatur oder den Ersatz Ihres Kopiergerätes.
    - Supportvertrag für Ihre Software-Anwendungen.
- Bereiten Sie alternative Lösungen vor:
    - Gewährleisten Sie eine unterbrechungsfreie Stromversorgung (USV) und stellen Sie einen Stromgenerator für den Fall eines Stromausfalles bereit.
    - Spiegeln Sie Ihr Server-Laufwerk für den Fall, dass die Festplatte ausfällt.
    - Stellen Sie zwei IT-Server bereit, falls der Hauptserver ausfällt.
- Bereiten Sie alternative Prozesse vor:
    - Erarbeiten Sie eine Back-Up Strategie, um Datenverlust zu verhindern.
    - Temporäres Home-Office.
- Arbeiten Sie mit alternativen Dienstleistern:
    - Nutzen Sie parallel zwei verschiedene Kommunikationsanbieter für Internet und Telefon.

- Beziehen Sie das gleiche Produkt oder die gleiche Dienstleistung von zwei unterschiedlichen Zulieferern.

- …

(b) Ansatz für den Notfall: Komplettversagen oder Totalverlust

Hier wird in der Regel wie folgt vorgegangen:

- Bereiten Sie **alternative Lösungen außerhalb Ihrer Räumlichkeiten vor** (für den Fall, dass das Gebäude und alle vorhandenen Vermögensbestände zerstört werden).
- Priorisieren Sie Ihre Bereiche, Aktivitäten o. ä. danach, was zuerst wiederaufgebaut werden muss. Sie können nicht alles gleichzeitig wiederherstellen und es ist nicht möglich, ein „zweites Unternehmen“ als Reserve in der Hinterhand vorzuhalten. Sie müssen sich also zuerst auf die Aktivitäten konzentrieren, die für Ihr Unternehmen am wichtigsten sind.
- Bereiten Sie einen strukturierten Handlungsplan vor, um die Krise zu bewältigen, so dass der Betrieb rechtzeitig wieder anlaufen kann.

Für beide Pläne, müssen Sie Antworten auf die folgenden Fragen parat haben:

1. Wie lange darf der Geschäftsbetrieb maximal stillstehen, damit kein nachhaltiger Schaden für das Unternehmen entsteht?
2. Was ist nach einem Vorfall Ihre geplante Zeit für den Wiederaufbau?
3. Wie priorisieren Sie Ihre Aktivitäten, um tatsächlich mit den wichtigsten zu beginnen?
4. Wer ist wofür zuständig, wenn eine Katastrophe eintritt?
5. Wo sind Ihre alternativen Arbeitsplätze, falls Ihre Büroräume komplett zerstört werden? Wie kümmern Sie sich um die IT-Systeme für den alternativen Standort? Schaffen Sie sich neue Geräte erst dann an, wenn eine Katastrophe eintritt, oder halten Sie diese vor? Werden Sie ggf. auf Cloud-Lösungen zugreifen?

Um diese Fragen korrekt beantworten zu können, lesen Sie sich bitte die folgenden Passagen aufmerksam durch.

13.11.2. Aktivität 1: Rollen und Verantwortlichkeiten

Nutzen Sie die Tabelle aus **Kapitel J** des Anhangs **18.3 Plan zur Sicherstellung des Geschäftsbetriebes**, um die unterschiedlichen Rollen und Verantwortlichkeiten in Ihrem Team zu dokumentieren.

Wählen Sie einen verantwortlichen Mitarbeiter und einen Stellvertreter für jeden Bereich aus. Nutzen Sie die Beispiele in der Tabelle und fügen Sie ggf. weitere Verantwortlichkeiten hinzu.

In einem KMU kann bzw. wird dieselbe Person oftmals für mehrere Rollen verantwortlich sein, stellen Sie jedoch sicher, dass es in jedem Bereich einen Stellvertreter gibt.

J1. Rollen und Verantwortlichkeiten

Die folgende Tabelle fasst die wesentlichen Rollen und Verantwortlichkeiten zur Vorbereitung und Umsetzung des Plans zusammen.

Rolle	Titel	Verantwortlichkeiten	Name verantwortliche Person	Name Stell-vertreter
Mitglieder des Wiederaufbauplan-Teams	Entscheidungs-träger	Verantwortlich für: Einleiten des Plans		
	Leiter Krisen-Management und der Wiederaufbau	Verantwortlich für: Benachrichtigung des Teams und relevanter Zulieferer		
	Team-Mitglieder	Verantwortlich für: Benachrichtigung von Mitarbeitern und Anteilseigner		
		Verantwortlich für: Kommunikation mit Kunden und Medien		
		Verantwortlich für: Unterstützung des Wiederaufbaus		
		Verantwortlich für: Unterstützung des Wiederaufbaus		
		Verantwortlich für: Wiederherstellung der IT-Systeme		
Mitglieder des Teams für Anlagen-Ausfälle	Unterstützer	Ausfall der Büroausstattung (Fax, Kopierer etc.)		
		Ausfall von IT-Systemen		
		Ausfall von Strom oder Wasser		

13.11.3. Aktivität 2: Analyse der Auswirkungen und Berechnung der angestrebten Wiederaufbauzeit

Im Falle eines negativen Zwischenfalls, der Ihren Geschäftsbetrieb stört oder komplett lahmlegt (und dadurch auch alle Dienstleistungen für Ihre Kunden unmöglich macht), ist es unbedingt notwendig, die **maximal tolerierbare**

Störungsdauer (bzw. Unterbrechungsdauer)[17] zu bestimmen. Das ist die Zeitspanne, in der sich Ihr Unternehmen eine Unterbrechung von Dienstleitungen für Ihre Kunden leisten kann, ohne einen wesentlichen, d. h. existenzbedrohenden Schaden zu nehmen.

Wie bereits beschrieben, können die Auswirkungen finanziell (Umsatzverluste, hohe zusätzliche Kosten etc.), rechtlich oder regulatorisch (Vertragsstrafen, staatliche Bußgelder etc.) bzw. Renommee schädigend sein (negative Auswirkungen auf den guten Ruf, Vertrauensverlust) und/oder zum Verlust Ihrer Kunden führen.

Um die Auswirkungen zu bewerten, können Sie die folgende Skala heranziehen:

- Unerheblich
- Gering
- Wesentlich
- Gravierend

Dieselbe Skala haben Sie bereits in Kapitel **11.5 Risikopriorisierung** verwendet.

Ein Beispiel: Wenn ein Feuer Ihr Gebäude zerstört und das Unternehmen am vierten Tag noch immer stillsteht, kann das, je nach Art des Geschäftes und der Verträge mit Ihren Kunden, katastrophale Verluste verursachen.

Ihre maximale tolerierbare Störungsdauer beträgt daher drei Tage.

Im nächsten Schritt geht es um die Festlegung der **Wiederanlauf-Dauer** bzw. der **maximalen Dauer bis zum Wiederaufbau**[18]. Das ist die Zeitspanne, die Ihnen zur Verfügung steht, bevor die maximal tolerierbare Störungsdauer (siehe oben) erreicht wird, also bevor der Ausfall katastrophale Züge annimmt. Ihr Betrieb muss sich vorher erholt haben.

Die Wiederanlauf-Dauer ist kürzer als die maximal tolerierbare Störungsdauer. Im oben genannten Beispiel wäre die Wiederanlauf-Dauer zwei Tage (maximal drei).

[17] Englisch: MTPD = Maximum Tolerable Period of Disruption: Siehe Kapitel 16: Ausgewählte Begriffe und Abkürzungen.
[18] Englisch: RTO = Recovery Time Objective: Siehe Kapitel 16: Ausgewählte Begriffe und Abkürzungen.

In den folgenden Passagen erfahren Sie, wie Sie beide Werte berechnen. Fragen Sie sich für Ihre Unternehmung anhand des oben genannten Beispiels (Bürogebäude durch Feuer zerstört) parallel dazu, was die maximale Zeit wäre, die Ihr Unternehmen geschlossen sein kann, ohne einen erheblichen Schaden davonzutragen.

Es gibt zwei Möglichkeiten, die **maximale Dauer bis zum Wiederaufbau** Ihres Unternehmens zu bestimmen bzw. zu berechnen:

(a) Sie könnten das als Manager oder Inhaber Ihres Unternehmens einfach entscheiden bzw. festlegen. In vielen KMU ist das möglich, da die verantwortlichen Personen ihr Geschäftsumfeld in der Regel sehr gut kennen und somit ein gutes Gefühl für ihre spezifische maximale Wiederanlauf-Dauer haben.

(b) Sie können auch etwas analytischer vorgehen und die folgenden Schritte abarbeiten:

1. Nutzen Sie die Tabelle in **Kapitel J2** des Anhangs **18.3 Plan zur Sicherstellung des Geschäftsbetriebes,** um die Auswirkungen für Ihr Unternehmen zu identifizieren.
2. Füllen Sie die Spalten unter „**Dauer der Unterbrechung des Geschäftsbetriebes**“ für jede Auswirkung aus und bedenken Sie dabei, welche Einflüsse die Dauer der Störung auf Ihr Unternehmen hat („Was passiert, wenn das Unternehmen für einen, zwei oder mehrere Tage geschlossen bleibt?“). Nutzen Sie die Ampelfarben zur besseren Darstellung der Ergebnisse (siehe unten).

Die Zeitintervalle sollten komplett an Ihr Unternehmen angepasst werden. Geben Sie die Zeiten so vor, wie es für Ihr Geschäft am besten ist (z. B. auch möglich: 1-4 Stunden, 5-8 Stunden, 8 Stunden bis 1 Tag etc.).

Die Angaben in der Spalte mit den Auswirkungen sind ebenfalls nur als Anregung gedacht. Tragen Sie hier die Auswirkungen ein, die für Ihr Unternehmen relevant sind.

3. Füllen Sie die Spalte „**Maximal tolerierbare Störungsdauer**“ aus, indem Sie die Informationen aus Schritt 2 auswerten. Sie tragen hier die Dauer ein, die Ihnen bleibt, bevor die Auswirkung gravierend wird. So wird das Ausmaß der

Auswirkungen in unserem Beispiel im Schaubild unten bei „Vertragsstrafen“ (fünfte Zeile) gravierend, wenn das Unternehmen nicht bis zum Ende des dritten Tages wieder arbeiten kann. Die Maximal tolerierbare Störungsdauer beträgt daher „weniger als drei Tage“ oder „1-2 Tage“.

Auswirkung	**Dauer der Unterbrechung des Geschäftsbetriebes** Zeigt an, ob die Auswirkung eines Stillstands unerheblich, gering, wesentlich oder gravierend (katastrophal) ist. Sie sollten die untenstehenden Zeitintervalle auf die Bedürfnisse Ihres Unternehmens anpassen.									**Maximal tolerierbare Störungs-dauer**	**Maximale Dauer bis zum Wieder-aufbau**
	0-12 h	**1 Tag**	**2 Tage**	**3 Tage**	**1 Woche**	**2 Wochen**	**1 Monat**	**Später**			
Umsatzeinbußen	Uner-heblich	Uner-heblich	Gering	Wesentlich	Gravierend				→	Weniger als 1 Woche	2-3 Tage
Einfluss auf Cash-Flow	Uner-heblich	Gering	Gering	Gering	Wesentlich	Wesentlich	Gravierend		→	Weniger als 1 Monat	1-2 Wochen
Erhöhung der Ausgaben	Uner-heblich	Uner-heblich	Gering	Wesentlich	Wesentlich	Gravierend			→	Weniger als 2 Wochen	3-5 Tage
Behördliche und rechtliche Einflüsse	Uner-heblich	Uner-heblich	Gering	Wesentlich	Gravierend				→	Weniger als 1 Woche	2-3 Tage
Vertragsstrafen	Uner-heblich	Uner-heblich	Gering	Gravierend					→	Weniger als 3 Tage	1-2 Tage
Unzufriedenheit der Kunden	Uner-heblich	Uner-heblich	Gering	Wesentlich	Wesentlich	Gravierend			→	Weniger als 2 Wochen	1 Woche
Verlust von Kunden	Uner-heblich	Uner-heblich	Gering	Gravierend					→	Weniger als 2 Tage	1-2 Tage
Negative Auswirkungen auf die Marke und das Renommee	Uner-heblich	Uner-heblich	Gering	Wesentlich	Wesentlich	Gravierend			→	Weniger als 2 Wochen	1 Woche
Gesamt-Unternehmen (jeweils das Minimum wählen)									↓	Weniger als 2 Tage	1-2 Tage

4. Basierend auf den Informationen aus Schritt 3 können Sie jetzt die „**Maximale Dauer bis zum Wiederaufbau**“ bestimmen, indem Sie den nächstkleineren Wert verglichen mit der Maximal tolerierbaren Störungsdauer nehmen. Für eine maximal tolerierbare Störungsdauer von „weniger als 3 Tage“ (wie in Zeile 5 unseres Beispiels) beträgt die maximale Dauer bis zum Wiederaufbau also „1-2 Tage“.
5. Wiederholen Sie die Schritte 2, 3 und 4 für jede Auswirkung in Ihrer Tabelle.
6. In der untersten Zeile (Gesamt-Unternehmen) tragen Sie in den beiden rechten Spalten jeweils den niedrigsten Wert ein, den Sie in den einzelnen Auswirkungs-Zeilen darüber finden können.

Der Wert ganz rechts unten ist die „**Maximale Dauer der Wiederherstellung**“ für das gesamte Unternehmen – oder Ihr sog. **Wiederaufbauziel**. Das ist der Zeitrahmen, in dem die wichtigsten Geschäftsprozesse wieder laufen müssen. Im Beispiel sind es „1-2 Tage“, was bedeutet, dass sich das Unternehmen **am ersten oder zweiten Tag NACH der Störung** von dieser erholt haben muss.

Alle Ihre Aktivitäten sollten auf diesen Zeitrahmen ausgerichtet sein. Es muss dabei nicht der gesamte Geschäftsbetrieb vollständig wiederhergestellt werden, aber die kritischen Prozesse, die Sie analysiert haben, müssen wieder laufen.

13.11.4. Aktivität 3: Priorisierung der Wiederaufbau-Aktivitäten

Es ist sehr wichtig, die Hauptprozesse bzw. Aktivitäten in Ihrem Unternehmen abzubilden (alle Prozesse und ähnliche Aufgaben, die Ihnen bei der Erbringung von Dienstleistungen für Ihre Kunden helfen) und diese nach der angestrebten Wiederaufbaudauer zu priorisieren. Sie werden diese Informationen benötigen, um bei Bedarf einen effektiven Wiederaufbau zu gewährleisten.

Nutzen Sie die Tabelle in **Kapitel J3** des Anhangs **18.3 Plan zur Sicherstellung des Geschäftsbetriebs**, um die Vorgänge in Ihrem Unternehmen abzubilden und zu priorisieren.

Hauptprozesse / Aktivitäten	Wichtige Termine für diese Aktivität	Interner Kontext bzw. interne Abhängigkeiten (Systeme, Anwendungen etc.)	Externer Kontext bzw. externe Abhängigkeiten (Zulieferer etc.)	Maximal tolerierbare Störungsdauer	Angestrebte Wiederauf-baudauer

13.11.5. Aktivität 4: Definieren und dokumentieren Sie Ihre Wiederaufbaustrategie

Während die Wiederaufbaustrategien für Fehlfunktionen und Ausfälle von Geräten normalerweise recht einfach sind (z. B. Anruf beim Ihrem Dienstleister für Support, Ersatz, Reparatur etc.), ist der Wiederaufbau nach einer Katastrophe bzw. einer schwerwiegenden Krise alles andere als leicht. Hierfür müssen Sie Ihre

Lösungsansätze bereits vor einer potenziellen Krise vorbereitet haben bzw. im Bedarfsfall parat halten, um eine rechtzeitige Erholung gewährleisten zu können.

Um die richtigen Vorbereitungen für katastrophale Vorfälle (Verlust von Räumlichkeiten, wichtige Geräte und Anlagen, Dateien, Archive etc.) zu treffen, müssen Sie die folgenden Punkte beachten:

- Sie benötigen einen alternativen Arbeitsplatz, von dem aus Ihre Mitarbeiter an den Tagen arbeiten können, an denen Ihre Räumlichkeiten nicht zugänglich sind. Dabei könnte es sich um einen zweiten Unternehmensstandort handeln, Ihre Mitarbeiter könnten von zu Hause aus arbeiten oder Sie mieten vorübergehend neue Räumlichkeiten etc.
- Der Aufbau von alternativen Lösungen für Anlagen und Systeme kann Tage oder Wochen bis zur Fertigstellung in Anspruch nehmen. Es kann sein, dass Ihr Unternehmen nicht so lange warten kann und die **maximale tolerierbare Dauer bis zum Wiederaufbau** überschritten wird (z. B. kann der Kauf und die Neuinstallation eines großen Servers mit Ihrem ERP-System zwischen 2 bis 4 Wochen dauern. Diese Zeitspanne könnte für Sie nicht annehmbar sein, da Ihr Unternehmen in der Zwischenzeit in Konkurs gehen müsste, wenn es nicht weiterarbeiten kann).
- Prüfen Sie die Möglichkeiten zum Ad-hoc Kauf von Geräten in lokalen Fachgeschäften. Geräte, z. B. Drucker, müssen verfügbar und leicht zu installieren sein.

Fassen Sie in Ihrem Plan alle existenten Strategien für den Wiederaufbau zusammen, damit diese bei Bedarf zur Verfügung stehen. Nur so können Sie vermeiden, dass Sie Ihre Entscheidungen nach dem Motto „Augen zu und durch“ treffen müssen.

Füllen Sie die relevanten Bereiche in **Kapitel J4a** im Anhang **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** aus.

13.11.6. Aktivität 5: Bereiten Sie einen Wiederaufbau für einzelne Ressourcen vor

In **Kapitel J4b** des Anhangs **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** finden Sie diverse Tabellen, die Ihnen bei der Dokumentation aller wichtigen Informationen für die detaillierte Vorbereitung Ihres Wiederaufbauplans helfen werden.

Mitarbeiter (Anzahl während des normalen Geschäftsbetriebs in / an verschiedenen Arbeitsbereichen bzw. Einsatzorten)				
Stellenbeschreibung oder Namen	**Anzahl normaler Geschäfts-betrieb**	**Möglicher alternativer Arbeitsplatz**	**Erwartete Wiederauf-baudauer**	**Wie erfolgt der Zugriff auf Anwendungen, Dateien, E-Mails etc.**
Manager	1	Von zuhause aus mit privatem Laptop	Kann an Tag 1 beginnen	Daten und Anwendungen über Cloud (Internetzugang)
Berater	2	Von zuhause aus für 2 Wochen. Kauf von 2 Laptops an Tag 1 notwendig	Können an Tag 2 beginnen	
Sekretariat	1	Nutzt des Büro XYZ, das das Unternehmen angemietet hat		
Buchhaltung	1			

(a) Mitarbeiter (dokumentieren Sie, wo jeder Mitarbeiter wie lange arbeiten wird und welche Voraussetzungen es am alternativen Standort gibt)

(b) IT-Anwendungen oder Software

(c) IKT-Systeme und relevante Geräte

(d) Büroausstattung

(e) Produktionsanlagen

(f) Kommunikationsleitungen (Daten- und Sprache)

(g) Dateien und Archive des Unternehmens

Sie können bzw. sollten weitere für das Unternehmen relevante Informationen hinzufügen. Die bereits voreingetragenen Informationen dienen als Beispiel und sollen Ihnen den Umgang mit der Tabelle erleichtern. Nutzen Sie die vorgeschlagenen Spalten, um den Umgang mit beiden Szenarien ((a.) Nichtverfügbarkeit, Ausfall oder Fehlfunktion oder (b.) Notfälle (Komplettversagen bzw. Totalverlust)) möglichst ausführlich zu dokumentieren.

13.11.7. Aktivität 6: Erstellen Sie eine Checkliste für den Wiederaufbau

Sie sollten eine Checkliste erstellen, die abgearbeitet werden kann, wenn es zu einem katastrophalen Ereignis bzw. einem Notfall kommt.

In **Kapitel J5** des Anhangs **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** finden Sie eine Beispielliste, die Sie nach Belieben verändern und ergänzen sollten.

13.12. Plan zum Umgang mit Informationssicherheits-Vorfällen

Der Umgang mit Informationssicherheits-Vorfällen unterscheidet sich nicht allzu sehr vom Umgang mit „normalen“ Vorfällen und Krisen (siehe oben). Sie finden Informationen dazu in **Kapitel K** des Anhangs **18.3 Plan zur Sicherstellung des Geschäftsbetriebes** und sollten diese in Verbindung mit dem Plan zum Umgang mit Vorfällen und Krisen nutzen.

Die angemessene Reaktion hängt hauptsächlich von der Art des Vorfalls ab. Einige wichtige Bereiche (siehe unten) könnten Ihnen hier etwas mehr Aufmerksamkeit und Mühe abverlangen.

13.12.1. Anzeichen, die manchmal übersehen werden

In einigen Fällen gibt es Hinweise darauf, dass ein Sicherheitsvorfall passieren kann. Dabei handelt es sich unter anderem um die folgenden:

- Warnungen des Betriebssystems, wie z. B.: „Fehler beim Lesen der Datei auf Festplatte x“. Dieser Fehler könnte mehrmals auftauchen, bevor die Festplatte ausfällt.
- Eine oder mehrere unbekannte Personen im W-LAN des Unternehmens.
- Eine Anwendung zeigt mehrere fehlgeschlagene Login-Versuche von einer unbekannten Quelle.
- Negatives Verhalten von unzufriedenen Mitarbeitern könnte zu zukünftigen Sicherheitsverstößen führen.
- …

Mitarbeiter sollten stets ihre Augen offenhalten und das Management bei solchen Warnsignalen kontaktieren. Das ermöglicht ggf. eine prophylaktische Reaktion und somit die Minderung der möglichen Risiken.

13.12.2. Einen Informationssicherheits-Vorfall erkennen

Es mangelt in KMU oftmals an Wissen in Bezug auf technische Probleme, da es unternehmensintern keine IKT-Experten gibt. Das führt dazu, dass die schwierigsten Aspekte im Bereich der Informationssicherheits-Vorfälle die folgenden sind:

- **Feststellen, dass/ob (überhaupt) ein Vorfall vorliegt** und in solch einem Fall
- **dessen Ausmaß und die Auswirkungen erkennen und verstehen**.

Im Anhang finden Sie eine Liste mit einigen Warnsignalen oder Indikatoren. Diese helfen Ihnen zu identifizieren, ob aktuell ein sicherheitsrelevanter Vorfall stattfindet oder ob ein Vorfall stattgefunden hat.

Sie können diesen Prozess dadurch unterstützen, dass Sie verschiedene potenzielle Vorfalls-Szenarien und dafür typische Indikatoren durchgehen bzw. Ihren IKT-Berater bitten, diese Szenarien mit Ihren Mitarbeitern bzw. Kollegen durchzusprechen. Es ist ein großer Vorteil, wenn das Personal in einem KMU z. B. die Antworten auf die folgenden Fragen kennt:

- Wie erkennt man einen Denial-of-Service Angriff auf unsere Webseite?
- Was sind Indikatoren dafür, dass unsere Datenbank kompromittiert wurde?
- Wie identifiziert man eine Phishing E-Mail?
- Wie können wir herausfinden, ob es unbefugte Zugriffe auf unser ERP-System gab?
- …

13.12.3. Identifizierung und Sicherung von Beweisen

Wenn ein Sicherheitsvorfall direkt mit einer möglichen Straftat zusammenhängt (z. B. unbefugtes Eindringen, Diebstahl von vertraulichen Geschäftsdaten, Einschleusen von böswilliger Software in das System des Unternehmens etc.), dann ist es nicht

nur wichtig, diese Aktivitäten zu bemerken, sondern auch alle Informationen und Beweise über den Vorfall aufzubewahren und zu sichern. Bewahren Sie diese Beweise gut auf, um mögliche rechtliche Schritte einleiten zu können.

Zur professionellen Sicherstellung dieser Daten sollten Sie mit Ihrem IKT-Berater zusammenarbeiten (z. B. Back-Up des infizierten Systems, Systemlogs kopieren etc.).

13.12.4. Benachrichtigung von Interessenvertretern bzw. Stakeholdern

Manche Angriffe richten sich nicht allein gegen Ihr Unternehmen, sondern sie nutzen Ihre IKT-Systeme, um einige oder alle damit verbundene Systeme anzugreifen.

Ein Beispiel:

- Ein Virus, der Ihren E-Mail-Server infiziert, könnte alle Ihre gespeicherten Kontakte nutzen, um Spam oder infizierte E-Mails an diese zu versenden, sodass der Virus weiterverbreitet wird.
- Ein Hacker, der sich Zugang zu Ihren Kundendaten verschafft hat, könnte auch alle Kontendaten bzw. Kreditkarteninformationen etc. Ihrer Kunden finden, wenn diese Daten in Ihrem System gespeichert sind.

In solchen Fällen ist es unbedingt notwendig, sich u. a. an alle gültigen rechtlichen Vorgaben zu halten. Benachrichtigen Sie ggf. Ihre Kunden und informieren Sie darüber, was geschehen ist, wie Sie reagiert haben und welches Risiko noch besteht.

Bevor Sie diese Schritte ergreifen, sollte sich das Management Ihres Unternehmens unbedingt zuerst an einen Rechtsberater und einen IKT-Experten wenden, um festzustellen, ob die Benachrichtigung z. B. Ihrer Kunden notwendig ist. Sie müssen zusammenarbeiten, um festzulegen, was genau kommuniziert werden soll, wie formuliert wird, wer die Nachricht erhält, inwiefern Sie (Mit-)Verantwortung für den Vorfall tragen etc.

In manchen Fällen sollten auch die staatlichen Behörden informiert werden und alle notwendigen Informationen erhalten. Das kann so weit gehen, dass Sie den Behörden Zugriff auf Ihr System gewähren.

13.13. Aufbewahrung Ihres Plans zur Sicherstellung Ihres Geschäftsbetriebes

Vergessen Sie nicht, eine Kopie Ihres Plans mit allen Teil-Plänen an einem alternativen Standort aufzubewahren. Dabei sollte es sich um einen Ort handeln, der nicht zum Betriebsgelände gehört. Das könnte zum Beispiel das Haus des Inhabers sein, eine passwortgeschützte Website oder jeder andere Standort, an dem das bzw. die Dokument(e) sicher und zugänglich aufbewahrt werden kann/können.

Vergessen Sie nicht, jedem für den Plan Verantwortlichen den alternativen Standort und die gültigen Zugangsinformationen mitzuteilen. Überprüfen Sie mindestens alle sechs Monate, ob sich der Plan in der aktuellsten Fassung an diesem Standort befindet. Stellen Sie sicher, dass er dort sicher aufbewahrt wird.

13.14. Schulungen in Bezug auf den Gesamtplan bzw. die einzelnen Teil-Pläne

Es macht keinen Sinn, einen Plan zu haben, den niemand kennt, anwendet oder überhaupt finden kann. Nun da Sie alle Teil-Pläne vorbereitet haben und alle damit verbundenen Vorsorge-Maßnahmen umgesetzt wurden, sollten Sie Ihre Mitarbeiter wie folgt schulen:

- Legen Sie einen Schulungstermin fest.
- Verteilen Sie die vorbereiteten Plan-Dokumente.
- Erklären Sie die Rollen und Verantwortlichkeiten.
- Erklären Sie, welche Aufgaben erfüllt werden müssen.
- Erklären Sie die Kommunikationsplanung.
- Beschreiben Sie die Entscheidungsfindung während eines Vorfalls bzw. einer Krise und die notwendigen Aktivitäten und Schritte.
- Erklären Sie die Bedeutung aller Pläne. Besprechen Sie Ziele, Inhalte etc. aller Pläne.

Eine gute Möglichkeit zur Festigung des Wissens und zur der Steigerung des unternehmensinternen Risiko-Bewusstseins ist, wenn Ihre Mitarbeiter die Schulungen für neue Kollegen danach selbst durchführen.

Wiederholen Sie die Schulung jedes Mal, wenn der Plan grundlegend aktualisiert oder ein neuer Mitarbeiter eingestellt wird. Einmal im Jahr sollte die Schulung mindestens stattfinden.

13.15. Testen und Üben

Sie können sich nicht sicher sein, dass ein Plan die gewünschten Ergebnisse bringt, wenn Sie ihn nicht testen. Sie sollten regelmäßige Tests und Übungen durchführen, um die folgenden Punkte sicherzustellen:

(a) Alle Bestimmungen und Informationen in Ihrem Plan sind richtig und aktuell.

(b) Insbesondere die Mitglieder Ihres Wiederaufbau-Teams, aber auch alle weiteren Mitarbeiter erweitern ihr Wissen und kennen ihre Rollen bzw. Verantwortlichkeiten im Falle eines Vorfalls bzw. einer Krise/Katastrophe. In Übungen kann das Team bzw. Ihre Mitarbeiter die eigene Reaktionsfähigkeit steigern und feststellen, wo sie sich noch weiteres Know-how bzw. Fähigkeiten aneignen müssen.

(c) Die Mitglieder Ihres Wiederaufbau-Teams zeigen, dass sie fest entschlossen sind, im Krisenfall zusammenzuarbeiten und gemeinsam eine Herausforderung bestehen können.

Es gibt verschiedene Übungen, die Sie nutzen können, um Ihre Notfallpläne, -prozesse und -kapazitäten zu evaluieren:

- Durchdenken bzw. Diskutieren von Szenarien

  Dabei handelt es sich um Besprechungen mit Mitarbeitern bzw. den zuständigen Teams, in denen jeder über seine Rolle und seine Aufgaben in Notfallsituationen spricht. Dies ist eine kostengünstige und wenig zeitintensive Übung, die sich leicht wiederholen lässt und gut geeignet ist, um neue Mitarbeiter miteinbeziehen.

  Die diskutierten Szenarien können von vergleichsweise einfachen Vorfällen (z. B. Verlust eines Büroschlüssels) bis hin zu komplexen Krisensituationen (z. B. Brand in den Geschäftsräumlichkeiten) gehen.

- Praktische Übung spezifischer Situationen

Diese Übungen befassen sich mit einzelnen Szenarien. Sie konzentrieren sich hauptsächlich auf den Ausfall von bestimmten Geräten oder auf spezifische Aspekte des täglichen Geschäftsbetriebes (z. B. Ausfall eines IT-Systems oder der Telefonleitung). Bei diesen Übungen testen Sie alternative Lösungen, um zu überprüfen, ob diese komplett funktionsfähig sind und ob Ihr Team in der Lage ist, wie geplant zu reagieren. Diese Vorgehensweise wird normalerweise für IT- und Kommunikationssysteme bzw. weitere operative Produktionssysteme und Geräte angewendet.

Auch Ihr Kommunikations- und Benachrichtigungsplan kann in Verbindung mit diesen Übungen getestet werden.

- Großübungen

  Eine Großübung ist einem echten Zwischenfall sehr ähnlich. Es ist die komplexeste Übung, da Sie z. B. die vorgesehenen Arbeitsplätze an alternativen Standorten sowie Ihre Ersatz-Geräte und -Maschinen etc. testen. Eine solche Übung muss gut vorbereitet werden und sie dauert für gewöhnlich auch länger. Sie testen alle Teile Ihres Plans zur Sicherstellung Ihres Geschäftsbetriebes (auch die Wiederherstellung des IT-Systems).

Machen Sie sich während der Übungen Notizen, um mögliche Verbesserungsansätze zu dokumentieren. Alles ist wichtig: Vorhandene Lösungen optimieren, das Engagement Ihrer Mitarbeiter, der gesamte Planungs- und Umsetzungsprozess etc. Setzen Sie gute Verbesserungsideen zügig um.

13.15.1. Entwicklung eines Trainingsprogrammes

Für die Entwicklung eines Trainingsprogramms sind im Normalfall die folgenden Schritte nötig:

- Entscheiden Sie sich für eine Übungsart (z. B. Diskutieren von Szenarien, Großübung).
- Überlegen Sie, wer teilnehmen soll.
- Legen Sie den Umfang fest (Standort, Geschäftsbetrieb, Systeme, Tätigkeiten etc.), auf den die Übung bezogen ist.

- Legen Sie Szenarien fest (Ausfall, Feuer, Erdbeben etc.).
- Legen Sie Startzeit und Dauer der Übung fest.
- Bereiten Sie Bewertungs- und Verbesserungsformulare bzw. -Fragebögen für die Übung vor, die von allen Teilnehmenden ausgefüllt werden.
- Stellen Sie sicher, dass die Übung selbst nicht ein Risiko für Ihr Unternehmen darstellt. Führen Sie die Übung z. B. nicht an Tagen durch, an denen der ganze Betrieb unter Stress steht. Machen Sie die Übung außerhalb von Stoßzeiten.
- Benachrichtigen Sie alle Mitarbeiter, die teilnehmen sollen.

Setzen Sie ein Meeting zur Nachbesprechung an, sobald die Übung abgeschlossen wurde, um die Ergebnisse zu besprechen. Stellen Sie fest, was gut war und wo nachgebessert werden muss. Sammeln Sie die Fragebögen/Formulare mit den Verbesserungsvorschlägen ein und entscheiden Sie, welche Maßnahmen Sie ergreifen wollen, um die Widerstandsfähigkeit Ihres Unternehmens weiter zu verbessern.

Aktualisieren Sie Ihre Pläne und teilen Sie Ihren Mitarbeitern alle Änderungen mit.

13.16. Qualitätskontrolle aller ausgewählten Handlungsoptionen

Sobald eine ausgewählte Handlungsoption (siehe Risikoregister) unternehmensintern umgesetzt wurde, empfehlen wir, dass Sie sich ein paar Minuten nehmen, um zu evaluieren, ob die ausgewählte Maßnahme auch die gewünschten Ergebnisse erzielt hat.

Überprüfen Sie die Qualität der Umsetzung so, wie Sie dies mit jedem anderen Projekt in Ihrem Unternehmen tun würden.

Stellen Sie sicher, dass die umgesetzten Maßnahmen zum Umgang mit einem bestimmten Risiko nicht zu neuen Risiken geführt haben, die ggf. mehr Probleme verursachen können als das bearbeitete Risiko.

Zu guter Letzt überprüfen Sie, ob **die aktuelle Risiko-Bewertung des behandelten Risikos** auch tatsächlich so ist, wie das vor der Umsetzung der Maßnahmen angestrebt und in Ihrem Risikoregister dokumentiert wurde. Bewerten Sie die

aktuelle Eintrittswahrscheinlichkeit und Auswirkung erneut und vergleichen Sie das Ergebnis mit den geplanten Werten:

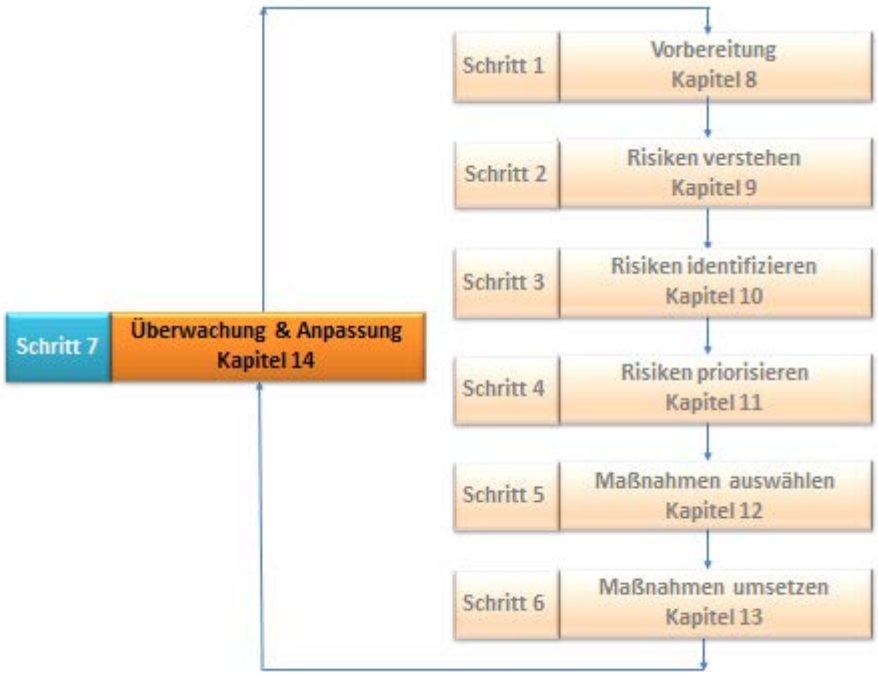
(a) Wenn die Werte gleich oder besser sind, dann haben Sie großartige Arbeit geleistet.

(b) Sollte die Risiko-Bewertung höher sein, versuchen Sie die Gründe dafür herauszufinden und überlegen Sie, ob diese Risiko-Bewertung so trotzdem akzeptabel ist.

- Wenn der Wert akzeptabel ist, **korrigieren Sie die Spalte „Risiko-Bewertung nach dem Risikomanagement“ und nutzen Sie die Spalte „Notizen“, um diese Entscheidung und relevante Informationen dazu zu dokumentieren**.
- Sollte der Wert nicht akzeptabel sein, müssen Sie Ihre Bemühungen fortsetzen und zusätzliche Maßnahmen bzw. Verbesserungen ausfindig machen. Folgen Sie dazu erneut den in diesem Handbuch bis hierher beschriebenen Schritten.

Sie sollten alle Ihre Maßnahmen stetig verbessern. Nutzen Sie dazu am besten weiter die CASSANDRA-Methode, um die Widerstandfähigkeit Ihres Unternehmens kontinuierlich zu steigern.

14. Schritt 7 – Überwachung und Anpassung



Glückwunsch! Wenn Sie Schritt 6 durchgearbeitet haben, dann haben Sie erfolgreich einmal einen gesamten Risikomanagement-Prozess absolviert.

Sie haben die Risiken Ihres Unternehmens identifiziert, bewertet, priorisiert und passende Maßnahmen ausgewählt und implementiert. Dadurch konnten die Risiken für Ihr Unternehmen auf ein akzeptables Level gesenkt werden.

Ihr Unternehmen ist jetzt widerstandsfähiger als zuvor. Nun müssen Sie sicherstellen, dass das auch so bleibt. Ihr Ziel sollte sein, die Anpassungsfähigkeit und damit die Zukunftsfähigkeit Ihres Unternehmens weiter stetig zu verbessern.

Dafür ist es notwendig, dass Sie an den folgenden Punkten arbeiten:

(a) Legen Sie ein internes **Archiv** für Ihr Resilienz-Management an. Stellen Sie sicher, dass die gesamte Projektdokumentation archiviert wird und dass Ihr Risikoregister auf dem neuesten Stand bleibt.

Stellen Sie sicher, dass sich alle Ihre Notfall- und Wiederaufbaupläne stets an den festgelegten Orten befinden und im Falle einer Krise oder Katastrophe zugänglich sind.

(b) Stellen Sie sicher, dass Ihre **Mitarbeiter ausreichend geschult** wurden und über das **nötige Wissen verfügen**, um auf Herausforderungen und Krisen wie geplant zu reagieren.

Setzen Sie mindestens eine jährliche Schulung an (sie muss nicht lange dauern). Dadurch fördern Sie das Risiko-Bewusstsein Ihrer Mitarbeiter und stellen sicher, dass jeder weiß, was im Notfall zu tun ist.

Stellen Sie sicher, dass alle Rollen und Verantwortlichkeiten klar sind und von Ihren Mitarbeitern auch angenommen werden (z. B. sollte die zuständige Person für Back-Ups ihren Aufgabenbereich kennen und tagtäglich routiniert umsetzen).

(c) Als Steigerung von Punkt (b) können Sie daran arbeiten, dass ein **erhöhtes Risikobewusstsein gleichsam zur DNA Ihres Unternehmens wird**.

Schlagen Sie vor, dass jeder Mitarbeiter (inklusive Sie selbst) jeden neuen Prozess, jede Handlung und jede getroffene Entscheidung auch aus der Risiko-management-Perspektive betrachtet. Auch wenn in diesem Handbuch die negativen Risiken in den Mittelpunkt gestellt werden mussten, vergessen Sie dabei niemals auch immer die Chancen zu identifizieren. Es wäre ein großer Fortschritt für Ihr Unternehmen, wenn die Risikoabwägung als Standard im Unternehmensalltag bei jeder Entscheidungsfindung automatisch mitberück-sichtigt wird.

(d) Arbeiten Sie den gesamten **CASSANDRA-Risikomanagement-Prozess mindestens einmal im Jahr durch** (Schritte 2 bis 6), aktualisieren Sie Ihr Risikoregister, verbessern Sie die Risiko-Bewertungen, indem Sie neue Maßnahmen ergreifen oder bestehende Maßnahmen optimieren, planen Sie für neue Eventualitäten und verbessern Sie Ihren Resilienz-Status insgesamt.

Vergessen Sie nicht, dass der Aufwand bei einem zweiten Durchgang weitaus geringer sein wird. Sie werden sich mit vielem leichter tun und auch Ihre Ergebnisse (weitere Verbesserung der Resilienz Ihres Unternehmens) werden effektiver und fortgeschrittener sein.

(e) Planen Sie eine **regelmäßige** (z. B. einmal im Quartal) **Revision aller umgesetzten Lösungen, Maßnahmen und Kontrollen**, um zu überprüfen, ob sie noch genauso effektiv und effizient arbeiten wie erhofft, oder ob Sie eventuell nachjustieren müssen.

Achten Sie auf Veränderungen in Ihrem externen und internen Geschäftsumfeld. Identifizieren Sie neue Risiken sowie Veränderungen bei bestehenden Risiken, die dazu führen könnten, dass Sie Ihre Maßnahmen und Prioritäten noch einmal überdenken müssen.

Aktualisieren Sie, wenn notwendig, Ihre Risikoregister und behandeln Sie jedes neue oder veränderte Risiko, wie Sie es gelernt haben.

Stellen Sie regelmäßig sicher (z. B. einmal im Quartal), dass die geplanten (Not-) Lösungen zur Sicherstellung Ihres Geschäftsbetriebes vorhanden und funktionsfähig sind (z. B., dass ein zweiter Server im Bedarfsfall funktioniert und dass Back-Up-Geräte und alternative Arbeitsplätze verfügbar sind).

Kontrollieren und überwachen Sie regelmäßig, ob die Sicherheitsregeln und Richtlinien, die Sie festgelegt haben (siehe Kapitel **12.2.2. Umgang mit IT-Risiken**) wirklich im Geschäftsalltag verankert sind.

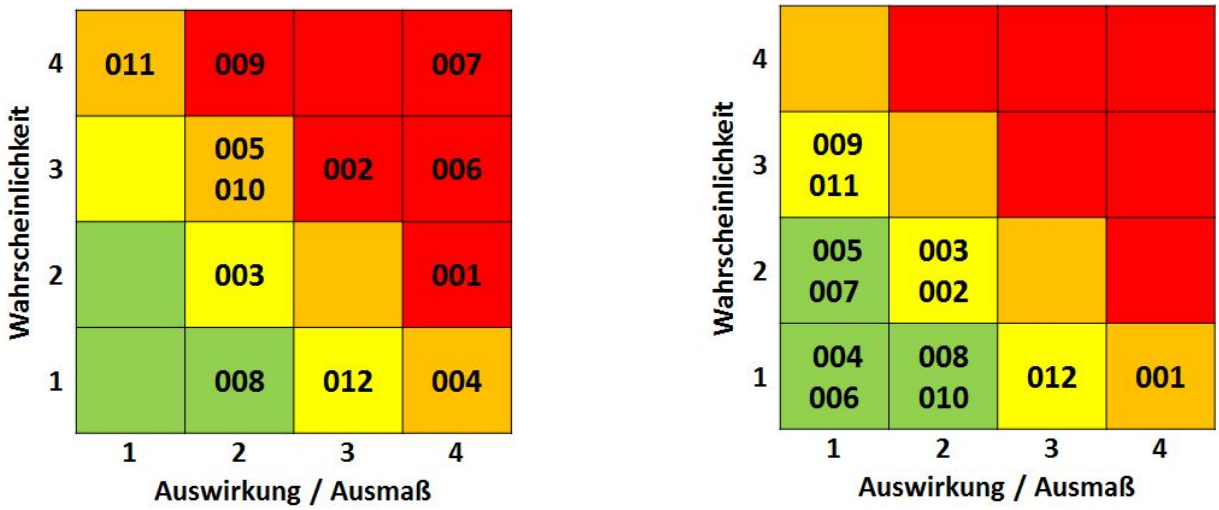
(f) Organisieren Sie **mindestens einmal im Jahr Übungen für Ihre Notfallpläne**, um die Aktualität der Inhalte zu überprüfen und Ihre Teams in die Lage zu versetzen, alle Systeme, Maßnahmen und Dienstleistungen bei Bedarf wiederherstellen zu können.

Überprüfen Sie, ob alle Mitarbeiter ihre Rollen und Verantwortlichkeiten kennen und wissen, wie sie zu handeln haben, wenn der Ernstfall eintritt.

(g) **Führen Sie Tagebuch über alle negativen Ereignisse und Vorfälle**. Notieren Sie alle Veränderungen, Trends, Erfolge und Fehlschläge (auch solche Vorfälle, bei denen Sie Glück hatten und gerade noch einmal alles gut gegangen ist). Analysieren Sie Ihre Einträge und versuchen Sie, aus jedem Vorfall etwas zu lernen, um die Widerstandsfähigkeit Ihres Unternehmens weiter zu verbessern.

14.1. Das Restrisiko oder „der Tag danach“

Sobald Sie Ihre ausgewählten Maßnahmen zur Risiko-Minderung umgesetzt haben, erhält jedes der bearbeiteten Risiken eine neue Risiko-Bewertung (mit einem neuen Wert für die Eintrittswahrscheinlichkeit und/oder für die Auswirkung). Die neue, akzeptable Risiko-Bewertung ist das verbleibende Risiko oder auch das Restrisiko.



Risiko Matrix VOR der Umsetzung der Maßnahmen

Management der Risiken →

Risiko Matrix NACH der Umsetzung der Maßnahmen

Ihre Risiko-Bewertungen für alle Risiken sollten Sie regelmäßig überprüfen, egal ob die Risiken schon über längere Zeit in Ihrem Risikoregister erfasst sind oder erst vor kurzem identifiziert und hinzugefügt wurden.

14.2. Resilienz und Risikomanagement: Der tägliche Geschäftsbetrieb

Risikomanagement in den täglichen Geschäftsbetrieb von möglichst vielen Unternehmen einzubetten, war und ist der Anspruch unseres EU-Projekts.

Dies ist auch die einzige Möglichkeit um sicherzustellen, dass bei jeder Entscheidung, Handlung, Unternehmensfunktion etc. bestehende Risiken, Bedrohungen und Maßnahmen berücksichtigt werden und Sie so Ihr Unternehmen auch bei stürmischer See auf Kurs halten können.

Je mehr Sie Risikomanagement in Ihrem Unternehmen ganz praktisch leben, desto widerstandsfähiger und erfolgreicher wird Ihr Unternehmen sein.

15. Vom Anfänger zum Profi

15.1. CASSANDRA: ein großer Schritt in Richtung Widerstandsfähigkeit

CASSANDRA bietet eine kostenfreie Methode zur Unterstützung von KMU im Bereich der Unternehmens-Resilienz.

Die CASSANDRA-Methode wurde so entwickelt, dass sie sich voll und ganz im Einklang mit den einschlägigen internationalen Standards in diesem Themenfeld befindet. Wer CASSANDRA nutzt, kann die Anpassungsfähigkeit und Resilienz eines Unternehmens nachhaltig verbessern. Dafür wurden die Grundprinzipien der Themenbereiche Risikomanagement, Informationssicherheit und Sicherstellung des Geschäftsbetriebes für ein normales KMU entsprechend nutzerfreundlich aufbereitet. Ein KMU, das der CASSANDRA-Methode folgt, wird große Fortschritte in Bezug auf die Minimierung seiner Risiken machen, es kann Bedrohungen und Schwächen in Chancen umwandeln und insgesamt seine Anpassungsfähigkeit entscheidend erhöhen.

15.2. Das nächste Level der Unternehmens-Resilienz erreichen

15.2.1. Internationale Normen und Standards

Folgende internationale ISO[19]-Normen und Standards bilden die Basis für die Inhalte der CASSANDRA-Methode:

ISO 31000:2009 Risikomanagement - Grundsätze und Richtlinien

Diese Norm beinhaltet Grundsätze, Rahmenbedingungen und Anleitungen für ein Risikomanagement. Es kann von jeder Organisation, unabhängig von seiner Größe oder Branche, verwendet werden. Mit ISO 31000 können Unternehmen die Wahrscheinlichkeit erhöhen, ihre Ziele zu erreichen, die Identifizierung von Chancen und Bedrohungen zu verbessern und Ressourcen für den Umgang mit Risiken effektiv einzusetzen.

[19] ISO = International Organization for Standardization, www.iso.org.

ISO 27001:2013 Informationstechnik, Sicherheitsverfahren und Informations-sicherheitsmanagementsysteme

Diese Norm ist Teil der Normenfamilie ISO 27000, die Organisationen bei der IT-Sicherheit unterstützt. ISO 27001 ist der bekannteste Standard. Er legt die Voraussetzungen für die Einrichtung, Umsetzung, Wartung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems fest. Die Norm enthält auch Anforderungen an die bedarfsgerechte Bewertung und Behandlung von Informationssicherheitsrisiken. Die Anforderungen der ISO 27001:2013 sind allgemeingültig und gelten für alle Organisationen, unabhängig von Größe, Art und Tätigkeit.

ISO 22301:2012 Sicherheit und Schutz des Gemeinwesens - Betriebliche Kontinuitätsmanagementsysteme

Diese Norm spezifiziert Anforderungen an die Einrichtung und Durchführung eines Managementsystems, um vor unerwarteten Störfällen geschützt zu sein, deren Eintrittswahrscheinlichkeit zu verringern, vorbereitet zu sein, angemessen reagieren und sich davon erholen zu können. Die Anforderungen nach ISO 22301:2012 sind allgemeingültig und sollen für alle Organisationen oder Teile davon gelten, unabhängig von Art, Größe und Tätigkeit.

ISO 9001:2015 Qualitätsmanagementsysteme

Diese Norm ist der bekannteste Teil der ISO 9000-Familie. Sie befasst sich mit verschiedenen Aspekten des Qualitätsmanagements. Die ISO 9001 bietet Anleitungen und Werkzeuge für Unternehmen und Organisationen, die sicherstellen möchten, dass ihre Produkte und Dienstleistungen den Anforderungen ihrer Kunden entsprechen und die Qualität konsequent verbessert wird. ISO 9001 beinhaltet die Implementierung und Nutzung eines Risikomanagements. Die Anforderungen nach ISO 9001:2015 sind allgemeingültig und gelten für alle Organisationen, unabhängig von Art, Größe oder Tätigkeit.

ISO/DIS 22316:2017-03 Sicherheit und Resilienz - Leitfaden für Resilienz von Organisationen

Dieser Standard wir zurzeit entwickelt. Er bietet einen Rahmen, Organisationen zu unterstützen, ihre Zukunft sicherer zu gestalten, indem sie eine Kultur der Widerstandsfähigkeit schaffen, ihre Fähigkeiten zur Einschätzung und Reaktion auf Bedrohungen und Chancen verbessern und der Organisation ermöglichen, ihre Verpflichtungen angesichts komplexer Veränderungen einzuhalten.

15.2.2. Lückenanalyse (Gap Analyse)

Es gibt diverse Webseiten und Bücher, die Sie (teilweise kostenfrei) dabei unterstützen, den aktuellen Status Ihres Unternehmens in Bezug auf diverse ISO-Standards zu ermittelt. Folgende Links können wir empfehlen[20]:

Für ISO 27001

http://advisera.com/27001academy/free-tools/free-iso-27001-gap-analysis-tool/

http://www.bsigroup.com/LocalFiles/BSI-ISOIEC27001-Assessment-Checklist-UK-EN.pdf

Für ISO 22301

http://www.bsigroup.com/LocalFiles/es-MX/ISO%2022301/BSI-ISO-22301-Self-Assesment-checklist.pdf

Für ISO 9001

http://advisera.com/9001academy/iso-9001-gap-analysis-tool/

https://www.bsigroup.com/Documents/iso-9001/resources/BSI-ISO-9001-self-assessment-checklist.pdf

http://www.iso9001help.co.uk/Gap%20Analysis%20Checklist.pdf

[20] Stand 31. August 2017.

15.2.3. Einhaltung der Normen und Zertifizierung

Die vollständige Einhaltung der oben genannten ISO Normen verlangt von Ihnen diverse Schritte und Entscheidungen: Anpassung und Dokumentation von Regelungen, Richtlinien, Abläufen und Prozessen; Implementierung eines Monitoring-Systems; Erstellung diverser Berichte; Durchführung regelmäßiger interner und externer Audits, um sicherzustellen, dass ein funktionierendes Managementsystem implementiert wurde, also ein System, das garantiert, dass die Umsetzung aller ISO-Anforderungen auch tatsächlich stattfindet.

Obwohl theoretisch jedes Unternehmen diese Schritte in Eigenregie umsetzen kann, wird normalerweise ein externer Fachberater hinzugezogen, der das Unternehmen bei der zügigen Umsetzung der notwendigen Schritte unterstützt. Das CASSANDRA-Konsortium empfiehlt Ihnen die Zusammenarbeit mit einem externen Experten.

Eine Zertifizierung wird von autorisierten Behörden bzw. Unternehmen nach einem erfolgreichen Audit erteilt. Zertifizierungen sind für ISO 9001, ISO 22301 und für ISO 27001 möglich. Unternehmen wählen die Zertifizierung, wenn sie davon überzeugt sind, dass sich durch die Umsetzung eines Standards z. B. die internen Abläufe nachhaltig verbessern lassen, und/oder um gegenüber ihren Kunden zu dokumentieren, dass sie gemäß international anerkannter Normen und Standards agieren.

16. Ausgewählte Begriffe und Abkürzungen

Aktivität: Ein von einer Organisation oder in ihrem Namen durchgeführter Prozess (oder eine Reihe von Prozessen), der ein oder mehrere Produkte oder Dienstleistungen erzeugt oder unterstützt (ISO 22301:2012).

Anpassungs- und Widerstandsfähigkeit einer Organisation: Die Fähigkeit, wichtige Trends und daraus resultierende Ereignisse zu antizipieren, sich ständig an Veränderungen anzupassen und sich von störenden und schädigenden Verfällen zu erholen (The BCI, 2013).

Bedrohung: ein Zu- oder Umstand, bei dem aus einer bestimmten Gefahr ein Schaden oder Verlust entstehen kann; eine Quelle möglichen Schadens.

Cyber-Risiko: Jegliche Art von Risiken, die auf einen Ausfall oder eine Beeinträchtigung des IT-Systems eines Unternehmens zurückzuführen sind mit Folgen wie z. B. finanziellem Verlust, Störung/Unterbrechung des Betriebsablaufes, negative Auswirkungen auf die Unternehmensreputation.

Enterprise resource planning (ERP-Systeme): Üblicherweise aus verschiedenen Anwendungen bestehende Betriebswirtschaft-Software, welche das Sammeln, Speichern, Verwalten und Auswerten von Daten der verschiedenen Geschäftsaktivitäten einer Unternehmung ermöglicht. ERP-Systeme umfassen in der Regel die Bereiche Buchhaltung, Vertrieb, Anlagen-Management, Personalwesen etc.

Gefahrenpotenzial: Eine Situation, eine Tätigkeit oder ein Zustand, die/der negative Konsequenzen haben kann (kann von einer Aktivität, einer Ressource, einer Person oder einer Anlage ausgehen).

IKT: Informations- und Kommunikationstechnologie (umfasst Computer-Hardware, Software, technische Kommunikation jeglicher Art).

Informationen und Datenbestände: Jegliche Art von Informationen: in Form von elektronisch gespeicherter Daten (auf Disketten, CDs etc.); aus IT-Systemen, die Daten speichern und verarbeiten; aus Kommunikationssystemen, die Daten auf Ihr oder von Ihrem System übertragen; aus IT-Anwendungen (ERP, E-Mail etc.); physisch vorhandene Dokumente und Archive sowie auch immaterielle Rechte (z. B. geistiges Eigentum).

Informationssicherheit: Der umfassende Schutz aller Informationen eines Unternehmens (sowohl materiell als auch immateriell, auf Papier oder elektronisch etc.). Dies gilt für den Schutz und die Wahrung der Vertraulichkeit, der Integrität, der Authentizität, der Verfügbarkeit und der Zuverlässigkeit der Informationen.

Integrität von Informationen: Sicherstellen, dass Informationen unverändert und vollständig zur Verfügung stehen, insbesondere der Schutz der Informationen vor unerlaubten oder unbemerkten Änderungen oder Löschungen.

KMU: Kleine und mittlere Unternehmen. Dazu gehören Kleinstunternehmen, sowie kleine und mittlere Unternehmen (KMU) mit weniger als 250 Mitarbeitern, einem Jahresumsatz von nicht mehr als 50 Millionen Euro und/oder einer jährlichen Bilanzsumme von nicht mehr als 43 Millionen Euro.

Krise: Eine Situation, bei der dringender Handlungsbedarf besteht. Charakteristisch ist ein hoher Grad an Unsicherheit, durch die die Kernaktivitäten einer Organisation gestört und/oder ihre Glaubwürdigkeit in Frage gestellt werden (ISO 22300:2012).

Maximale tolerierbare Ausfallzeit (Maximum Tolerable Period of Disruption: MTPD): Die höchstens erlaubte Zeit einer Prozessunterbrechung (z. B. eine Dienstleistung kann nicht angeboten werden), vom Eintritt des Störfalls bis zur vollständigen Rückkehr zum Normalbetrieb.

Plan für die Sicherstellung des Geschäftsbetriebes: Schriftlich definierte Vorgehensweisen, die Organisationen bei Störungen anwenden, um den Geschäftsbetrieb auf einem zuvor definierten Niveau aufrechtzuerhalten oder wiederherzustellen (ISO 22301:2012).

Recovery Time Objective (RTO; Wiederanlauf-Dauer): Der festgelegte Zeitraum nach einem Störfall, innerhalb dessen die Produktion oder die Aktivitäten wiederaufgenommen werden bzw. die Ressourcen wieder zu Verfügung stehen müssen (vgl. ISO 22301:2012).

Restrisiko: Der Teil des Risikos, der nach der Durchführung von Maßnahmen und Kontrollen übrigbleibt.

Risiko: Aktuell eine Eventualität, die in Zukunft zur Realität werden kann. Wenn das geschieht, dann kann dies positive oder negative Auswirkungen bzw. Konsequenzen für Ihr Unternehmen haben.

Risikomanagement: Koordinierte Aktivitäten, um eine Organisation in Hinblick auf Risiken zu leiten und zu steuern.

Sicherstellung des Geschäftsbetriebes (betriebliches Kontinuitäts-management): Die Fähigkeit einer Organisation nach einem den Geschäftsbetrieb störenden Vorfall auf einem zuvor definierten und akzeptablen Niveau, die Produkte und Dienstleistungen des Unternehmens wieder zur Verfügung zu stellen (ISO 22300:2012).

Thema: Ein Problem, das geschehen und Realität geworden ist und bereits Auswirkungen auf die Ziele und Aktivitäten des Unternehmens hat.

USV: Eine technische Installation, die im Notfall für eine unterbrechungsfreie Stromversorgung (USV) sorgt, z. B. wenn die Hauptstromversorgung ausfällt. Eine USV wird typischerweise zum Schutz von Hardware wie Computern, Rechenzentren, Telekommunikationsausstattung oder anderen elektronischen Geräten an Stellen, wo eine unerwartete Unterbrechung der Stromzufuhr Verletzungen, Todesfälle, ernste Geschäftsunterbrechungen oder Datenverlust verursachen kann, eingesetzt.

Verfügbarkeit von Informationen: Schutz von Informationen und Sicherstellung, dass sie auf Abruf verfügbar sind.

Vertraulichkeit von Informationen: Ein Zustand, in dem sichergestellt ist, dass nicht autorisierte Personen, Einrichtungen oder Prozesse keinen Zugang zu Informationen haben.

Vorfall: Ereignis, das einen Verlust, eine Unterbrechung, einen Notfall oder eine Krise auslösen kann. (ISO 22300:2012).

Widerstandsfähigkeit/Resilienz: Die Fähigkeit einer Organisation, mit Veränderungen umgehen zu können.

17. Ausgewählte Bibliografie

BCI Good Practice Guidelines 2013, The Business Continuity Institute

ISO 9001:2015 Quality management systems – Requirements

ISO 22301:2012 Societal security – Business continuity management systems – Requirements

ISO 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements

ISO 31000 Risk Management – Principles and guidelines

ISO/DIS 22316 Security and resilience — Guidelines for organizational resilience

Risk Management Standard – The Institute of Risk Management (IRM)

The Nuclear Energy Option, Bernard L. Cohen, Plenum Press, 1990

18. Anhänge

18.1. Vorlagen Risikoregister

Siehe separate Dokumente zum Download (Excel-Vorlagen).

18.2. Beispiele für mögliche Strategien und Maßnahmen zur Risiko-Minderung

Unternehmens- und strategische Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Marktrisiken (und Risiken im Ihrem Geschäftsbereich)	Überprüfung des Geschäftsplans
Politisches Umfeld	Überprüfung des Geschäftsplans
Wettbewerb	Marktinformationen; Berichte; Überprüfung von Dienstleistungen, Preisen etc.
Status (öffentliche) Sicherheit	Überprüfung der physischen Sicherheitsmaßnahmen und/oder des Versicherungsschutzes
Nationale Wirtschaftslage	Überprüfung des kurz-, mittel- und langfristigen Geschäftsplans
Änderung des Kundenverhaltens	Überprüfung der Strategien für Marketing und Vertrieb; Umfragen zur Kundenzufriedenheit
Änderungen in der Nachfrage nach Dienstleistungen	Überprüfung der Strategien für Marketing und Vertrieb; Überprüfung und Anpassung des Vertriebs- und Geschäftsplans
Arbeitsrecht (Gesetzes-Änderungen sowie bestehende Vorschriften)	Überprüfung der Mitarbeiterverträge
Fusionen und Übernahmen	Überprüfung der Strategien für Marketing und Vertrieb; Überprüfung und Anpassung des Vertriebs- und Geschäftsplans
Neue umwälzende Technologien	Überprüfung der Strategien für Marketing und Vertrieb; Überprüfung und Anpassung des Vertriebs- und Geschäftsplans
Änderungen in Richtung Protektionismus	Überprüfung der Strategien für Marketing und Vertrieb; Überprüfung und Anpassung des Vertriebs- und Geschäftsplans
Steigende Arbeits- oder Materialkosten	Gewinn- und Verlustrechnung analysieren; Cash-Flow Pläne anpassen; Verträge mit externen Dienstleistern
Investitionsrisiken	Erstellen eines detaillierten Geschäftsplans; Überprüfen des Geschäftsplan mit der Hausbank, dem Steuerberater bzw. weiteren Beratern
Markenkommunikation und	Unternehmens- und Markenkommunikationsplan

Unternehmens- und strategische Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Marketing	
Risiko für das Renommee	Unternehmens- und Markenkommunikationsplan
Betrug und Korruption	Schriftlich dokumentierte Prozesse; regelmäßige Audits (intern und/oder extern)
Veralterung von geistigem Eigentum	Überprüfung der Ablaufdaten; Überprüfung der Strategien für Marketing und Vertrieb; Überprüfung und Anpassung des Vertriebs-und Geschäftsplans
Schlechte Qualitätskontrollen	Schriftlich dokumentierte Prozesse; Formulare bzw. Formblätter; Qualitäts-Audits; Umfragen zur Kundenzufriedenheit
Unzureichende Investitionen in Forschung und Entwicklung	Forschung und Entwicklung in die Jahres-Budgetplanung aufnehmen

Operative Risiken und Risiken für die Sicherstellung des Geschäftsbetriebes	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Geringe Qualität der erbrachten Dienstleistungen	Schriftlich dokumentierte Prozesse; Schulungen für das Personal; Qualitätssicherungsprozess; Überwachung der Dienstleistungserbringung; Feedback-Gespräche mit Kunden
Unzureichendes Projektmanagement	Schulungen; Schriftlich dokumentierte Prozesse; Projekt-Controlling
Risiken im Bereich Logistik und Transport	Vorbereitung von Notfallplänen, falls ein Teil der Transportkette ausfällt (Ausfall eines Zulieferers, zerstörtes Lager etc.); Analyse und/oder Verbesserung des Versicherungsschutzes; Outsourcing an Dritte
Änderung im Nachfrageverhalten und Fähigkeit, damit umzugehen	Regelmäßige Überprüfung aller Dienstleistungen für Kunden; Überprüfung des Geschäftsplans
Vertragsrisiken	Überprüfung bestehender Verträge: - Vertragsstrafen, falls ein Zulieferer nicht liefert; - klären, ob der Zulieferer einen Plan zur Sicherstellung des Geschäftsbetriebes hat; - klären, ob der Zulieferer die Sicherheit aller Daten oder Informationen gewährleisten kann, die er von Ihrem Unternehmen erhalten hat; - keine Vertragsstrafen für eigene Dienstleistung akzeptieren
Versicherungsmanagement und aktuelle Deckungssummen	Überprüfung, ob Versicherungsschutz für Katastrophen, Vermögensverluste, Umsatzeinbußen und Verbindlichkeiten besteht.
Outsourcing-Management	Siehe oben „Vertragsrisiken“ plus genaue schriftliche Fixierung des jeweiligen Service-Levels
Menschliches Versagen im operativen Geschäft	Schriftlich dokumentierte Prozesse; Risikomanagement auf bestehende Prozesse anwenden
Arbeitskonflikte und Streik	Eindeutiger Arbeitsvertrag
Fälschung	Überprüfung bestehender Berechtigungen von allen Mitarbeitern; offene Kommunikation mit Banken

Operative Risiken und Risiken für die Sicherstellung des Geschäftsbetriebes	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Betrug	Regelmäßige Überprüfung der Buchhaltung und Rechnungslegung; Regelmäßige Abstimmung aller Konten (Kunden, Banken, Lieferanten); jährliche interne und/oder externe Audits
Epidemien – Grippepandemie	Vorbereitung eines Pandemieplans
Vertretungen	Vorbereitung eines Vertretungsplan
Wasserschäden oder sanitäre Probleme	Vorbereitung eines Plans zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz
Stromausfälle	USV und/oder Generatoren
Probleme mit der Heizung, Klimaanlage etc.	Regelmäßige Wartungen; Servicevertrag mit Dienstleister
Maschinenausfälle	Service- und Supportvertrag mit Dienstleister
Verlust oder Zerstörung des Grundstücks	Versicherungsschutz; Plan zur Sicherstellung des Geschäftsbetriebes
Giftmüll: chemische Flüssigkeiten und Kontaminierung (z. B. aufgrund von nahegelegener Produktion, Transport oder Lagerung)	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz
Internes Feuer: gravierend, wesentlich, gering	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz
Externes Feuer: gravierend, wesentlich, gering	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz

Operative Risiken und Risiken für die Sicherstellung des Geschäftsbetriebes	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Staub- bzw. Sandsturm	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz; Wartung von Heizung, Klimaanlage etc.
Erdbeben: wesentliche oder geringe Schäden	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz
Überschwemmung oder Dürre	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz
Erdrutsche	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz; Wetterberichte verfolgen; Kommunikation mit staatlichen Behörden
Hitzewelle	Installation oder Wartung von Klimaanlage; Überprüfung alternativer Stromversorgung; Plan zur Sicherstellung des Geschäftsbetriebes
Tornado, Taifun, Windstürme	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz; Wetterberichte verfolgen; Kommunikation mit staatlichen Behörden
Schnee- oder Eissturm	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz; Wetterberichte verfolgen; Kommunikation mit staatlichen Behörden
Vulkanausbruch	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz
Starke Winde, Wirbelstürme	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz; Wetterberichte verfolgen; Kommunikation mit staatlichen Behörden
Gezeiten und Tsunamis	Plan zur Sicherstellung des Geschäftsbetriebes; Notfall- und Evakuierungsplan; Versicherungsschutz; Wetterberichte verfolgen; Kommunikation mit staatlichen Behörden

Operative Risiken und Risiken für die Sicherstellung des Geschäftsbetriebes	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Physische Sicherheit und Zugang zum Gebäude	Liste aller Mitarbeiter mit Schlüsseln zum Gebäude; Kameras und Alarmanlagen; Risikobewertung des Gebäudes
Arbeitsschutz: Geräte und Maßnahmen	Jährliche Überprüfung der Haltbarkeitsdaten aller Feuerlöscher; Testen der Ausrüstung (z. B. Erste-Hilfe-Set); Mitarbeiterschulungen zur Nutzung der Ausrüstung; Sicherstellen, dass Personal Schutzkleidung und/oder -instrumente nutzt
Diebstahl, Raub	Erhöhung Sicherheitsvorkehrungen; Versicherungsschutz; Alarmanlage und Videoüberwachung
Bombendrohungen	Erhöhung Sicherheitsvorkehrungen; Versicherungsschutz; Alarmanlage und Videoüberwachung; Notfall- und Evakuierungsplan
Entführungen	Erhöhung Sicherheitsvorkehrungen; Versicherungsschutz; Alarmanlage und Videoüberwachung; Notfall- und Evakuierungsplan
Terror-Anschläge	Erhöhung Sicherheitsvorkehrungen; Versicherungsschutz; Alarmanlage und Videoüberwachung; Notfall- und Evakuierungsplan
Verkehrsunfälle	Schulung zum Thema sicheres Fahren; Versicherung und Pannenhilfe; Vertretungsplan
Zug-, Flugzeug-, Schiffsunfälle	Versicherungsschutz; Vertretungsplan

Finanzielle Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Kapital	Monatsabschlüsse mit Finanzmanager oder Steuerberater überprüfen; Überprüfung Cash-Flow und Geschäftsplanung
Verbindlichkeiten	Vorbereitung und regelmäßige Kontrolle der Cash-Flow Planung; regelmäßige Kontenabstimmung
Forderungen	Überprüfung aller Forderungen täglich oder wöchentlich; tägliche Überwachung der Zahlungseingänge
Betriebsausgaben und Management-Risiken	Planung von jährlichen und monatlichen Budgets und regelmäßige Kontrollen (Soll-Ist-Vergleich); Abweichungen besprechen und Korrekturmaßnahmen vornehmen
Investitionsausgaben	Planung von jährlichen und monatlichen Budgets und regelmäßige Kontrollen (Soll-Ist-Vergleich); Abweichungen besprechen und Korrekturmaßnahmen vornehmen
Budgetierung	Planung von jährlichen und monatlichen Budgets und regelmäßige Kontrollen (Soll-Ist-Vergleich); Abweichungen besprechen und Korrekturmaßnahmen vornehmen
Buchhaltung und Finanzverwaltung	Anforderung und Überprüfung von monatlichen Berichten (BWA monatlich und kumuliert)
Steuer	Monatliche Überprüfung der BWA
Zahlungen: Steuern und Sozialversicherung	Monatliche Überprüfung der BWA; Abstimmung mit Gehaltsabrechnungen
Cash-Flow und Liquidität	Vorbereitung und regelmäßige Kontrolle der Cash-Flow Planung
Zugang zu Krediten: Kreditwürdigkeit	Kommunikation mit Bank
Zinsrisiko	Regelmäßige Besprechungen mit Bank: Darlehensstatus überprüfen
Währungsrisiko	Regelmäßige Besprechungen mit Bank: (währungs-) politische Neuigkeiten beachten

Finanzielle Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Kostenstruktur	Kostenstruktur regelmäßig mit Steuerberater überprüfen
Preissystem	Regelmäßig Kosten und Gewinnmargen überprüfen; Nutzung von Marktforschung zum Vergleich der Marktpreise; Feedbackgespräch zu Preissystem mit Kunden
Gewinnmargen	Regelmäßig Kosten und Gewinnmargen überprüfen; Nutzung von Marktforschung zum Vergleich der Marktpreise; Feedbackgespräch zu Preissystem mit Kunden

IT- und Informationssicherheits-Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Unbeabsichtigtes Löschen von Daten	Back-Up
Falsche Dateneinträge	Back-Up; Software optimieren, um falsche Dateneinträge zu identifizieren; Datenabgleich
Arbeitsplätze ohne Passwortschutz	Umsetzung von Passwortschutz und Zugriffskontrollen
Unzureichende oder nicht bestehende Software-Lizenzen	Überprüfung aller Software-Lizenzen; Erfassung der legalen Software und der jeweiligen Anzahl der Lizenzen
Unzureichende Schulung von zeitlich befristeten und neuen Mitarbeiter	Schriftlich dokumentierter Trainingsplan für neue Mitarbeiter
Dringender Zugriff auf Dateien auf dem Computer eines abwesenden Mitarbeiters nötig	Vertretungsplan; Back-Up
Dateien verloren bzw. falsch	Funktionales Archivierungssystem; elektronische

IT- und Informationssicherheits-Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
abgespeichert	Kopien von Dokumenten nutzen (Scans)
Versand von Computer zur Reparatur mit Firmendaten auf der Festplatte	Richtlinie zur Entfernung von Geräten aus dem Bürogebäude erstellen (Geräte dürfen nur mit Genehmigung entfernt werden)
Fehlende Anweisungen für Nutzer und Administratoren	Zulieferer um Gebrauchsanleitung bitten
Ausfall einer Anwendung (aufgrund von Software- bzw. Hardware-Problemen oder wegen menschlichen Versagens etc.)	Supportvertrag mit Dienstleiter; Back-Up einführen
Ausfall des Zentralcomputers	Supportvertrag mit Dienstleister (Hardware und/oder Software) abschließen; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Ausfall der Telefonleitung	Alternative Möglichkeiten vorbereiten (z. B. Umleitung auf Mobiltelefon)
Hardware Fehlfunktion	Supportvertrag mit Hardware-Zulieferer abschließen; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Stromausfall hat Auswirkungen auf Daten	USV und/oder Generatoren
Ausfall von Geräten	Supportvertrag mit Zulieferer abschließen; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Beschädigte Dateien durch neue oder aktualisierte Software	Supportvertrag mit Dienstleister; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Software Fehlfunktion	Supportvertrag mit Dienstleister; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Software Update verhindert Zugriff auf Daten oder andere Programme	Supportvertrag mit Dienstleister; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes

IT- und Informationssicherheits-Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Daten auf Computer nicht verfügbar wegen Ausfall der Festplatte	Supportvertrag mit Dienstleister (Hardware und/oder Software) abschließen; Back-Up für alle Computer einführen: zentrale Speicherung aller Dateien
Unprofessionelle (keiner weiß, was wirklich gesichert wird) oder überhaupt keine Back-Ups	Back-Up planen und dokumentieren (wann, was, wo etc.); Verantwortung zuteilen; prüfen, ob tägliche Back-Ups erfolgreich und vollständig waren; Back-Ups testen, indem regelmäßig Wiederherstellung geübt wird
Back-Up nicht geprüft	Verantwortung zuteilen; prüfen, ob tägliche Back-Ups erfolgreich und vollständig waren; Back-Ups testen, indem regelmäßig Wiederherstellung geübt wird
Back-Up Datenträger nie geprüft	Verantwortung zuteilen; prüfen, ob tägliche Back-Ups erfolgreich und vollständig waren; Back-Ups testen, indem regelmäßig Wiederherstellung geübt wird
Back-Up wird Büro aufbewahrt	Back-Up täglich an einem auswärtigen Standort bringen
Fehlerhafte Hardware	Supportvertrag mit Zulieferer abschließen; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Fehlerhafte Programmierung	Supportvertrag mit Zulieferer abschließen; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Verlust von Systemen und Geräten	Supportvertrag mit Zulieferer (Software und/oder Hardware) abschließen; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes
Durchführung von unautorisierten und falschen Transaktionen	Genehmigungsprozess überprüfen (mit Banken, Zugang zu Online-System etc.); Buchhaltung und Bankbelege abgleichen; mehrstufigen Genehmigungsprozess für Online-Überweisungen einführen (z. B. Passwort und USB)
Zugriff auf Informationen für das Putzpersonal außerhalb der Bürozeiten	Politik des „sauberen Schreibtischs“ einführen (nach Dienstschluss keine Dokumente am Arbeitsplatz)
Ehemalige Mitarbeiter haben Zutritt zum Gebäude und Zugriff auf Daten	Checkliste für Mitarbeiter, die das Unternehmen verlassen, erstellen: Schlüssel, Computer, E-Mail-Zugang entziehen; Vorgaben für den Zutritt in das Gebäude machen und kontrollieren (um Probleme mit Schlüsseln und Alarmcodes zu lösen)

IT- und Informationssicherheits-Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Physischer Zutritt zu vertraulichen Bereichen durch unbefugte Personen	Sicherheitsmaßnahmen implementieren (Einbrecheralarm, Videoüberwachung etc.); Vorgaben für den Zutritt in das Gebäude machen und kontrollieren (um Probleme mit Schlüsseln und Alarmcodes zu lösen)
Physische Weitergabe von vertraulichen Informationen	Videoüberwachung; Vertrauliche Informationen verschließen; Schulungen für Mitarbeiter
Physischer Zutritt durch Unbefugte	Sicherheitsmaßnahmen implementieren (Einbrecheralarm, Videoüberwachung etc.); Vorgaben für den Zutritt in das Gebäude machen und kontrollieren (um Probleme mit Schlüsseln und Alarmcodes zu lösen)
Schlechte Sicherheitsbedingungen im Umfeld des Gebäudes	Sicherheitsmaßnahmen implementieren (Einbrecheralarm, Videoüberwachung etc.); Arbeitsschutzmaßnahmen umsetzen
Inkorrekter oder unangemessener Zugriff auf Dokumente	Vorgaben für Zugriffe durch Nutzer; Prozess für Zugriffsgenehmigung auf Dateispeicherungssysteme einführen

IT- und Informationssicherheits-Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Gefälschte Dokumente zur Genehmigung übermittelt	Zugriff auf wichtige Dokumente nur wenigen Personen gestatten (Schließfächer); Zutrittskontrolle für den (IT-System-)Bereich, wo Dokumente aufbewahrt bzw. gespeichert werden; verschlossene Kuverts und Paketdienste zur Übermittlung von Dokumenten an Dritte nutzen
Betrügerische Programmierung, die Datenintegrität beeinflusst	Zugriffskontrolle für Programmierer von externen Dienstleistern; Vertraulichkeitsvereinbarung mit externen Dienstleistern; Dokumentation aller Software-Änderungen (inkl. Begründung, was verändert wurde etc.)
Zugriff auf gefährliche Internetseiten	Antivirus-Software installieren; Webzugriff einschränken, riskante Seiten blockieren; Schulung von Mitarbeitern
Hacking	Antivirus-Software und Firewall installieren; Penetrationstest (Pentest) zur Erhöhung der Sicherheit durchführen; Mitarbeiter schulen; Plan zum Umgang mit Vorfällen und Krisen erstellen; Kommunikations- und Benachrichtigungsplan erstellen; Plan zur Sicherstellung des Geschäftsbetriebes erstellen
Computer-Viren	Antivirus-Software installieren; Webzugriff einschränken, riskante Seiten blockieren; Schulung von Mitarbeitern
Offenlegung von Berichten an Unbefugte	Zugriffskontrolle einführen; Schulungen für Mitarbeiter zum Thema Informationssicherheit; Plan zum Umgang mit Vorfällen und Krisen erstellen; Kommunikations- und Benachrichtigungsplan erstellen
Denial Of Service Angriffe (gegen die Unternehmens-Website)	Antivirus-Software und Firewall installieren; Penetrationstest (Pentest) zur Erhöhung der Sicherheit durchführen; Mitarbeiter schulen
E-Mail Sicherheit	Zugriffskontrolle einführen; Antivirus-Software installieren; Schulungen von Mitarbeitern zum Thema E-Mail Sicherheit
Mitarbeiter geben Passwörter untereinander weiter	Passwörter regelmäßig ändern; Schulungen von Mitarbeitern; Richtlinie einführen, die die Weitergabe von Passwörtern untersagt; Strafen verhängen

IT- und Informationssicherheits-Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Vertrauliche Informationen werden in Unterhaltungen erwähnt	Mitarbeiter schulen bzw. sensibilisieren
Interner Informationsdiebstahl	Zugriffe dokumentieren und Zugriffsvorgaben einführen; Vertraulichkeitsvereinbarung unterschreiben lassen; Passwörter regelmäßig ändern; Informationen klassifizieren und verschlüsseln bzw. verschließen
Netzwerk Sniffing	Antivirus-Software und Firewall installieren; Penetrationstest (Pentest) zur Erhöhung der Sicherheit durchführen
Cyber Angriff	Antivirus-Software und Antimalware-Software installieren; Penetrationstest (Pentest) zur Erhöhung der Sicherheit durchführen; Plan zum Umgang mit Vorfällen und Krisen erstellen; Passwörter regelmäßig ändern; Einsatz von „starken“ Passwörter durchsetzen
Erbeutung von System-Benutzernamen und Passwörtern	Penetrationstest (Pentest) zur Erhöhung der Sicherheit durchführen; Plan zum Umgang mit Vorfällen und Krisen erstellen; Passwörter regelmäßig ändern; Einsatz von „starken“ Passwörter durchsetzen
Vertrauliche Informationen werden zwischen Boten und Mitarbeitern ausgetauscht	Mitarbeiter schulen; Vertraulichkeitsvereinbarung unterschreiben lassen; Vorgaben zum Informations- und Dokumentenaustausch mit Dritten machen
Vertrauliche Informationen an Boten weitergegeben	Mitarbeiter schulen; Vertraulichkeitsvereinbarung unterschreiben lassen; Vorgaben zum Informations- und Dokumentenaustausch mit Dritten machen
Daten, die an einem externen Standort gespeichert sind, sind nicht verschlüsselt und wurden kompromittiert	Informationssicherheitsmaßnahmen einführen (Zugriffskontrolle, Verschlüsselung etc.); Plan zum Umgang mit Vorfällen und Krisen erstellen; Kommunikations- und Benachrichtigungsplan erstellen; Mitarbeiter schulen
Firewall unzureichend konfiguriert	Regelmäßige Überprüfung durch externen Dienstleister; Penetrationstest (Pentest) durchführen

IT- und Informationssicherheits-Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Identitätsdiebstahl (Kunde, Zulieferer, Mitarbeiter etc.)	Mitarbeiter schulen; Informationssicherheitsmaßnahmen einführen (Zugriffskontrolle, Verschlüsselung etc.); Passwörter regelmäßig ändern; Videoüberwachung
Informationen werden von ehemaligem Mitarbeiter beschädigt/ beeinträchtigt	Zugriffe dokumentieren und Zugriffsvorgaben einführen; Vertraulichkeitsvereinbarung unterschreiben lassen; Passwörter regelmäßig ändern; Zugriffsrechte am Ende der Zusammenarbeit entziehen
Ausführung von nicht genehmigten Programmen durch Nutzer, die zu Problemen im Hauptsystem führen	Informationssicherheitsmaßnahmen einführen (Zugriffskontrolle, Verschlüsselung etc.); Installation von Programmen nur durch Systemadministratoren durchführen lassen; Back-Up; Plan zur Sicherstellung des Geschäftsbetriebes erstellen; Plan zum Umgang mit Vorfällen und Krisen erstellen
Versuche, das Netzwerk zu sabotieren oder zu beschädigen	Informationssicherheitsmaßnahmen einführen (Zugriffskontrolle, Verschlüsselung etc.); Plan zum Umgang mit Vorfällen und Krisen erstellen; Software zur Netzwerküberwachung installieren; Firewall installieren
Vertrauliche Informationen werden nach außen getragen	Informationssicherheitsmaßnahmen einführen (Zugriffskontrolle, Verschlüsselung etc.); Plan zum Umgang mit Vorfällen und Krisen erstellen; Kommunikations- und Benachrichtigungsplan erstellen; Mitarbeiter schulen
Support aufgrund von Ausfällen eines externen Dienstleisters nicht verfügbar	Plan zur Sicherstellung des Geschäftsbetriebes erstellen und den Zulieferer ebenfalls auffordern, diesen zu erstellen
Abhängigkeit von IT-Wissen von Einzelpersonen	Dokumentation vorbereiten; Vertretungsplan
Externer Dienstleister (support) hat Zugriff auf vertrauliche Daten	Zugriffe dokumentieren und Zugriffsvorgaben einführen; Vertraulichkeitsvereinbarung unterschreiben lassen; Passwörter regelmäßig ändern; Zugriffsrechte am Ende der Zusammenarbeit entziehen

Behördliche und rechtliche Risiken	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Einhaltung von rechtlichen Vorschriften (in unserem Marksegment)	Status regelmäßig überprüfen; Maßnahmen zur Einhaltung der Vorschriften einführen; Versicherungsschutz
Einhaltung von behördlichen Vorschriften (in unserem Marksegment)	Status regelmäßig überprüfen; Maßnahmen zur Einhaltung der Vorschriften einführen
Einhaltung von Arbeitsschutz-Vorschriften (Feuerschläuche, Feuerlöscher, Warnhinweise etc.)	Arbeitsschutz-Normen vollständig umsetzen
Vertragsrisiken (Verträge mit Kunden und Lieferanten)	Überprüfung aller Verträge, um Verpflichtungen und Bestimmungen zu bewerten
Negative Entscheidung in laufender Gerichtsverhandlung	Vor Gerichtsverhandlung auf negativen Ausgang vorbereiten
Staatliche und steuerliche Anforderungen pünktlich erfüllen	Prozess zur Überprüfung von steuerlichen und staatlichen Anforderungen einführen; Bilanzen und Jahresabschlüssen im Hinblick auf die Erfüllung von steuerlichen Verpflichtungen überprüfen; jährliches externes Audit
Änderungen von Regulierungen und Gesetzen	Nachrichten für Ihr Marktsegment verfolgen; Plan zum Umgang mit Vorfällen und Krisen erstellen; Änderung des Geschäftsplans

Risiken im Personalbereich	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Verfügbarkeit von kompetentem Personal am Arbeitsmarkt und im Unternehmen	Vertretungsplan; Outsourcing
Derzeitige Anzahl an Mitarbeitern	Kapazitätsplanung überprüfen und verbessern
Derzeitige Kompetenzen von Mitarbeitern	Derzeitige Kompetenzen bewerten und Weiterbildung anbieten/einfordern
Probleme beim Arbeitsschutz	Arbeitsschutz-Normen vollständig umsetzen
Unfälle am Arbeitsplatz	Arbeitsschutz-Normen vollständig umsetzen
Reiseschutz	Anweisungen zum sicheren Reisen vorbereiten und kommunizieren
Mutterschutz	Vertretungsplan
Verlust von wichtigen Mitarbeitern (Krankheit, Kündigung etc.)	Vertretungsplan; Prozesse und Abläufe dokumentieren
Handlungen von Mitarbeitern sind unangemessen oder unklar	Verhaltenskodex verfassen und einführen
Unehrliche Mitarbeiter	Hintergrund von Mitarbeitern vor Einstellung überprüfen; Mitarbeiter mit Verstoß direkt konfrontieren; Konsequenzen ziehen: z. B. Vertrag beenden; genau überwachen
Fehlende Vertretungsplanung (wer vertritt nicht verfügbare Mitarbeiter)	Vertretungsplan vorbereiten
Unfälle am Arbeitsplatz	Arbeitsschutz-Normen vollständig umsetzen; Ursachenanalyse für den Vorfall
Gewalt am Arbeitsplatz	Klaren Verhaltenskodex erstellen und kommunizieren (z. B. „Null-Toleranz“ bei Belästigung oder anderen Arten von Gewalt am Arbeitsplatz); effektive Kommunikationskanäle einführen; Konflikte nicht eskalieren lassen
Unzureichende Schulungen zu IT-Systemen	Schulung für alle Mitarbeiter vorbereiten und durchführen; für alle neuen Mitarbeiter Schulung wiederholen

Risiken im Personalbereich	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Unzureichendes Sicherheitstraining	Schulung für alle Mitarbeiter vorbereiten und durchführen; für alle neuen Mitarbeiter Schulung wiederholen
Unzureichende Schulungen zu den operativen Geschäftsprozessen des Unternehmens	Schulung für alle Mitarbeiter vorbereiten und durchführen; für alle neuen Mitarbeiter Schulung wiederholen
Grippepandemie	Vorbereitung eines Pandemieplans
Nichteinhaltung von Sicherheitsvorschriften	Schulung für alle Mitarbeiter vorbereiten und durchführen; für alle neuen Mitarbeiter Schulung wiederholen; Sanktionen bei Nichteinhaltung verhängen
Kündigung, Ruhestand	Vertretungsplan; Prozesse und Abläufe dokumentieren
Streiks oder Unruhen	Plan für die physische Sicherheit erstellen; Vertretungsplan; Plan zur Sicherstellung des Geschäftsbetriebes; Versicherungsschutz
Schlechte Moral und Leistung	Mitarbeiter direkt konfrontieren; Geschäftsplan

Management-Risiken und Risiken durch Interessenvertreter	
Risiken	**Mögliche Strategien und Maßnahmen zur Risiko-Minderung**
Organisationsstruktur	Organigramm erstellen
Klare Rollen und Verantwortlichkeiten für alle Mitarbeiter	Rollen und Verantwortlichkeiten von allen Mitarbeitern dokumentieren
Management-Fähigkeiten	Regelmäßige Schulung von Management-Fähigkeiten; Weiterbildungen besuchen
Management-Kompetenzen	Regelmäßige Schulung von Management-Kompetenzen; Weiterbildungen besuchen
Genehmigungsprozess (inklusive Zugriff auf IT-Systeme)	Internen schriftlichen Genehmigungsprozess erarbeiten und umsetzen (auch für Zugriff auf IT-Systeme)
Schlechtes Management oder Micro-Management	Delegieren und Verantwortlichkeiten übertragen
Intrigen unter Kollegen	Verhaltenskodex erstellen, einführen und kontrollieren
Fehlende Werte und Prinzipien im Unternehmen	Definieren und dokumentieren Sie diese zusammen mit Ihrem Personal und mit externen Beratern und verankern Sie sie in Ihrem Geschäftsalltag
Management und Bewertung von Lieferanten, Zulieferern und Dienstleistern	Bewerten Sie Ihre derzeitigen externen Dienstleister etc. im Hinblick auf deren Qualität und potenziellen Beitrag zur Sicherstellung Ihres Geschäftsbetriebes
Interessen der Anteilseigner	Unternehmens- und Geschäftsziele mit Anteilseigner besprechen
Interessen der Mitarbeiter	Einhaltung der rechtlichen und behördlichen Vorschriften im Personalbereich
Kommunikation mit Mitarbeitern	Umfrage zur Mitarbeiterzufriedenheit starten
Management von und Kommunikation mit Kunden (Kommunikation mit wichtigen Kunden, von denen das Unternehmen abhängig ist)	Kommunikationsplan einführen, um Beziehungen zu Kunden zu verbessern; Umfrage zur Kundenzufriedenheit starten
Beziehungen mit der lokalen Nachbarschaft	Kommunikationsplan einführen, um Beziehungen zu verbessern

18.3. Plan für die Sicherstellung des Geschäftsbetriebes

Siehe separates Dokument zum Download (Word-Vorlage).


STRAŽ
NETGEAR
VIRUS