# Cybersicherheit – Lücken erkennen und handeln

# Inhalt

# Vorstellung

- 2018 gegründet
- Aktuell 5 Mitarbeiter
- Stellung Datenschutzbeauftragter
- Stellung ISB
- Stellung QM-Manager
- Umstellung auf digitale QM-Systeme
- ISMS Einführung
- Auditbetreuung
- Projektmanagement

---

- Seit 2001 im ISO regulierten Umfeld
- Lead Auditor ISO13485 und ISO27001
- QMB ISO9001
- Zertifizierter Datenschutzbeauftragter
- Risikomanager
- Tisax ® Assessment Professional
- IT Grundschutz Praktiker

# Ziele Inhalt

## Ziele dieser Schulung

- Eigene Risiken ermitteln
- Ein Gefühl für risikobasiertes Denken im Cyber-Umfeld
- Welche Risiken sind kritischer als andere (Priorisierung)
- Basis für weitere Schritte und Beratungen schaffen

## Was diese Schulung nicht möchte bzw. nicht kann:

- Eine professionelle Beratung ersetzen
- Sie zum Risikomanager ausbilden
- Ihre Cyber-Risiken lösen
- Sie mit Normen und Gesetze verwirren

# Einleitung

In einer zunehmend digitalisierten Welt sind Unternehmen mehr denn je den Gefahren von Cyberangriffen ausgesetzt.

Es ist von entscheidender Bedeutung, dass Unternehmen sich bewusst sind, welche Risiken bestehen und wie sie diese erkennen können, um ihre wertvollen Daten und Informationen zu schützen.

In diesem Vortrag werde ich zunächst die wichtigsten Cyber-Risiken erläutern und dann aufzeigen, wie Sie diese Risiken erkennen können.

Jedes Unternehmen hat spezielle und eigene Risiken, diese gilt es zu erkennen!

# Einleitung

Cyber Risiken und Risiken allgemein können in einer logischen Kettenreaktion behandelt werden.

Hierzu erhalten Sie in den folgenden Folien Handlungshinweise und Möglichkeiten diese in Ihrem Unternehmen entsprechend umzusetzen.

Hierbei liegt mein Fokus auf dem Erkennen und sich Bewusst werden, wo welche Risken im Unternehmen bestehen. Dies ist die Basis für angemessene Maßnahmen und ggf. weitere Unterstützung durch externe Partner wie:

- IT Unternehmen
- White Hacker
- IT-Sicherheitsberater

Nur wer seine Risiken kennt, kann sich angemessen schützen.

# Einleitung

## Gut zu wissen:

- Alles, was schiefgehen kann, wird auch schiefgehen (Murphys Gesetz).
- Gibt es unterschiedliche Varianten des Schiefgehen, ist es immer die Extremste.
- Wenn etwas zu gut erscheint, um wahr zu sein, ist es das wahrscheinlich auch.
- Die Natur ergreift immer die Partei des versteckten Fehlers.
- Wenn es mehrere Möglichkeiten gibt, eine Aufgabe zu erledigen, und eine davon in einer Katastrophe endet oder sonstige unerwünschte Konsequenzen nach sich zieht, kann man davon ausgehen, dass es jemand genau so machen wird.


(Copyright © RiskNET GmbH, www.risknet.de)

# Einleitung

QS Kornmann quality solutions

## Kurzer Ausflug in die Gesetze und Normen, denn Risikomanagement ist bei vielen Anforderungen verpflichtend.

### Handelsgesetzbuch Beispiel: §289 Inhalt des Lageberichts

(1) .....Ferner ist im Lagebericht die voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken zu beurteilen und zu erläutern; zugrunde liegende Annahmen sind anzugeben.
(2) Im Lagebericht ist auch einzugehen auf: 1.a)die Risikomanagementziele und -methoden der Gesellschaft einschließlich ihrer Methoden zur Absicherung aller wichtigen Arten von Transaktionen, die im Rahmen der Bilanzierung von Sicherungsgeschäften erfasst werden...

### GMBH Gesetz Beispiel: §43 Haftung der Geschäftsführer

1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden. (Nachweis?)

### Aktiengesetz Beispiel: §91 Organisation Buchführung

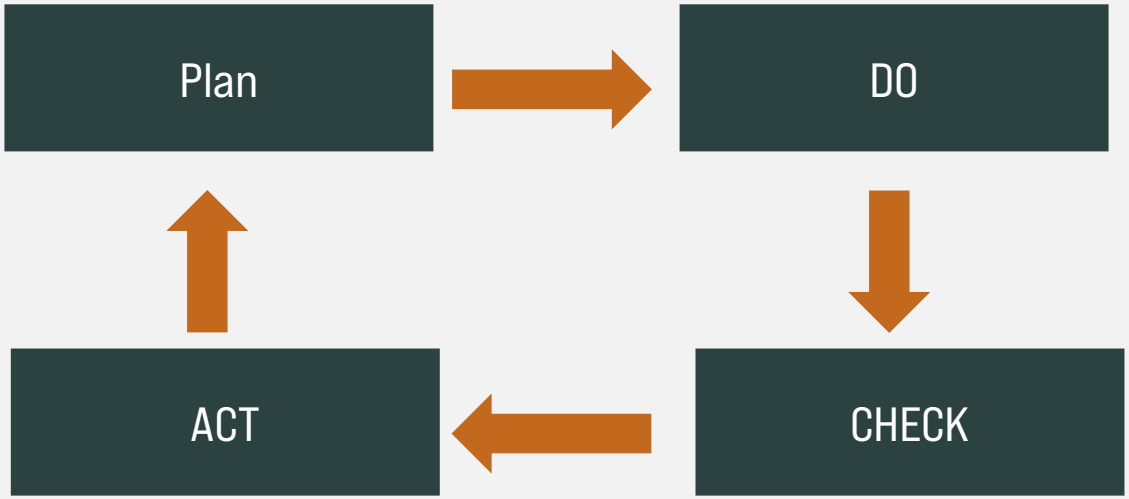
(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

### Nomen

DIN-EN-ISO 9001:2015
DIN-ISO 27001:2017
6.1 Maßnahmen zu Umgang mit Risiken und Chancen
VDS10010
10.10 Risikobasierter Ansatz
DSGVO (Gesetz)
Art. 25, Art. 32,... (21x „Risiko“)
DIN-EN-ISO 13485:2021
4.1.2 Risikobasierter Ansatz
DIN-ISO-31000:2018
Risikomanagement Leitlinien
BSI-Standard 200-3
Risikomanagement

# Einleitung

Egal wie Sie Risiken erkennen und welchen Vorgaben Sie folgen, im Grundsatz folgen alle einer Struktur:

# Was sind Risiken ?

QS Kornmann quality solutions

Ein Risiko ist eine potenzielle Bedrohung oder Unsicherheit, die sich auf ein Unternehmen, eine Organisation oder eine Person auswirken kann.

Es besteht die Möglichkeit, dass ein Ereignis eintritt, das negative Auswirkungen auf die Erreichung von Zielen, den Geschäftsbetrieb oder den individuellen Erfolg haben kann.

Im Zusammenhang mit dem Thema des Vortrags beziehen sich Cyber-Risiken speziell auf die Bedrohungen und Unsicherheiten im Zusammenhang mit der digitalen Welt.

Sie beinhalten die Gefahr von Cyberangriffen, Datenlecks, Identitätsdiebstahl, Systemunterbrechungen und anderen Vorfällen, die den Betrieb, die Integrität oder die Vertraulichkeit von Informationen und Technologien beeinträchtigen können.

# Wie erkenne ich Risiken?

QS Kornmann quality solutions

Zur Ermittlung der Risiken gibt es unterschiedliche Methoden

Suchmethoden

## Kreativitätsmethoden

- ✓ Brainstorm
- ✓ Mind Mapping
- ✓ Kopfstandtechnik
- ✓ Delphi-Methode
- ✓ Business Wargaming

## Analytische Methoden

- ✓ Bow-Tie-Analyse
- ✓ Fehlerbaumanalyse
- ✓ Fehlermöglichkeits- und Einflussanalyse (FMEA)
- ✓ HAZOP
- ✓ Fishbone
- ✓ ...

## Kollektionsmethoden

- ✓ Befragung
- ✓ SWOT Analyse
- ✓ Checkliste
- ✓ ...

# Wie erkenne ich Risiken ?

QS Kornmann quality solutions

## Kopfstandmethode

Die Kopfstandmethode ist eine bewährte Brainstorming Methode, die mit Hilfe von negativen Fragen neue Ideen generiert. Sie nutzt die Eigenschaft der Menschen, die von Natur aus gerne kritisieren. Wenn Sie mit Ihrem Team ebenfalls schnell und effizient neue Ideen generieren möchten, dann sollten Sie die Kopfstandtechnik einfach mal ausprobieren.

Sie überlegen sich, was Sie tun müssen um weniger IT-Sicherheit zu haben und negieren dann die Ergebnisse. Zum Beispiel:

- Virenscanner abschalten
- Nur noch offene WLAN-Hotspots verwenden
- Firewall abschalten
- Server in den Empfang stellen
- Türen offen lassen
- ....

# Wie erkenne ich Risiken?

QS Kornmann quality solutions

## Checkliste

Es gibt eine Vielzahl von Checklisten zu diesem Thema.

Am Ende der Präsentation haben wir Ihnen entsprechende Links hinterlegt.

Mit diesen Checklisten erhalten Sie Ideen und Anregungen welche Risiken ggf. für Sie in Frage kommen.

Elementare Gefährdungen

**Inhaltsverzeichnis**



## Auszug aus Elementargefährdungen BSi



zuletzt geändert am 07.12.2020 / Seite **2** von **50**

Elementare Gefährdungen

# Wie erkenne ich Risiken?

QS Kornmann quality solutions

## Fehlerbaumanalyse

Mit einer Fehlerbaumanalyse können die Komponenten eines Systems auf ihre Beteiligung an einem möglichen Ausfall des Gesamtsystems untersucht werden.

Sie eignet sich, um ausgehend von einem unerwünschten definierten Top-Ereignis rückwärts gerichtet dessen Ursachen zu ermitteln (= Top-down-Ansatz).

Sie starten mit einem unerwünschten Top Ereignis und ergründen dann mögliche Ursachen

| Cyber-Angriff | Insolvenz | Kein Material | Keine Kunden |
|---|---|---|---|

# Wie erkenne ich Risiken?

QS Kornmann quality solutions

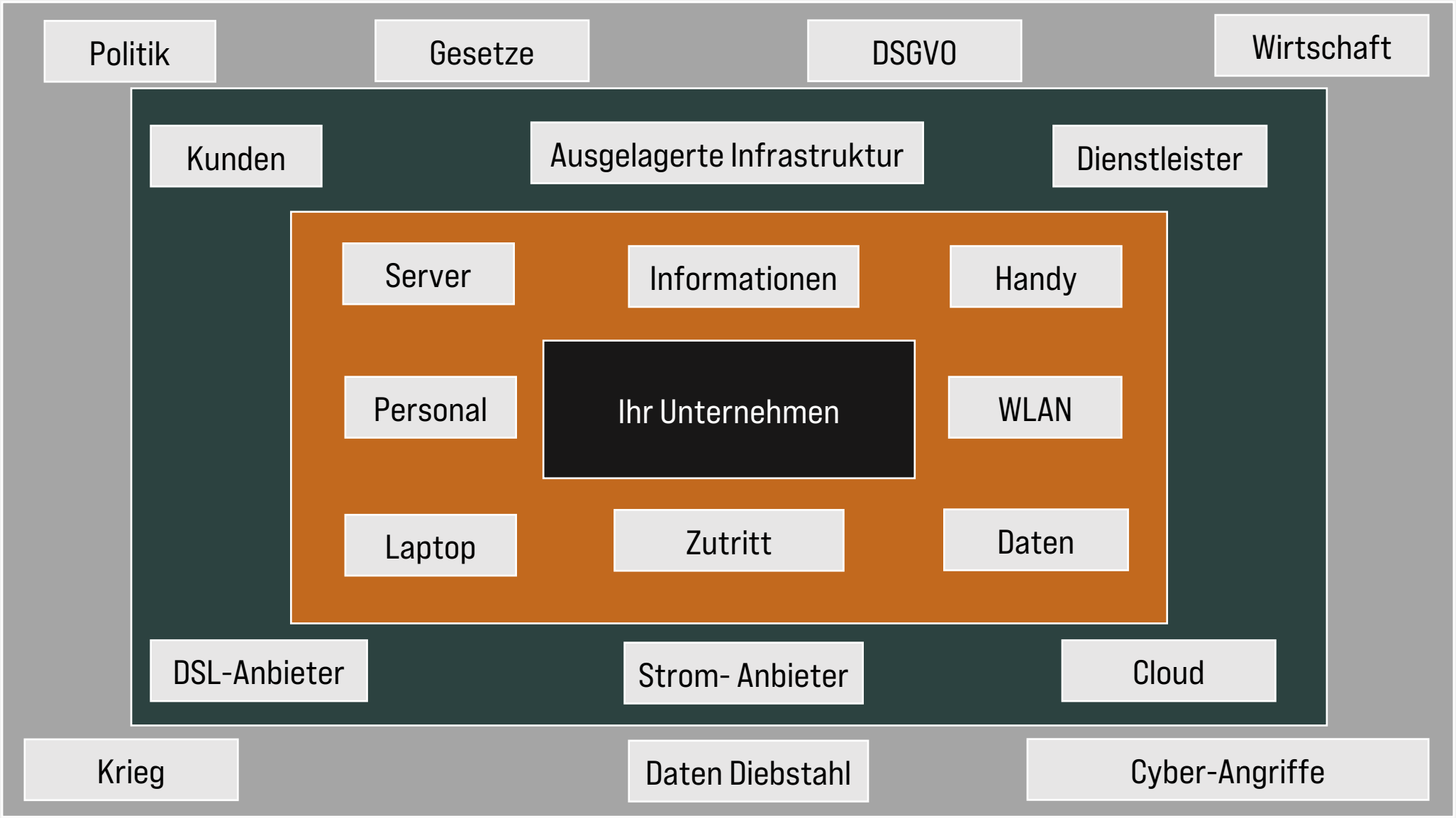
## FMEA

Die Kernidee der FMEA basiert auf dem frühzeitigen Erkennen und Verhindern von potenziellen Fehlern sowie deren Auswirkungen auf die Produktfunktionen. Die FMEA analysiert daher präventiv Fehler und deren Ursache. Sie bewertet Risiken bezüglich Auftreten, Bedeutung und ihrer Entdeckung. Berücksichtigen Sie dabei auch immer die Dauer (Stromausfall, Ausfall Internet, etc.)

| Mögliches Risiko | Mögliche Auswirkung | Wahrscheinlichkeit des Eintritts | Schadenshöhe | Maßnahme |
|---|---|---|---|---|
| ✓ Stromausfall<br>✓ Angriff<br>✓ Diebstahl<br>✓ Krankheit<br>✓ Krieg<br>✓ ....<br>✓ Ermittlung durch Fehlerbaum etc. | ✓ Kein Arbeiten<br>✓ Keine Kunden<br>✓ Daten weg<br>✓ Preise steigen<br>✓ ...<br>✓ Ermittlung durch Fehlerbaum etc. | ✓ unmöglich<br>✓ unwahrscheinlich<br>✓ wahrscheinlich<br>✓ häufig<br>✓ wird passieren | ✓ keine<br>✓ gering<br>✓ vertretbar<br>✓ hoch<br>✓ sehr hoch | ✓ Backup<br>✓ Firewall<br>✓ Regeln<br>✓ Versicherung<br>✓ Berater<br>✓ DSB<br>✓ ..... |

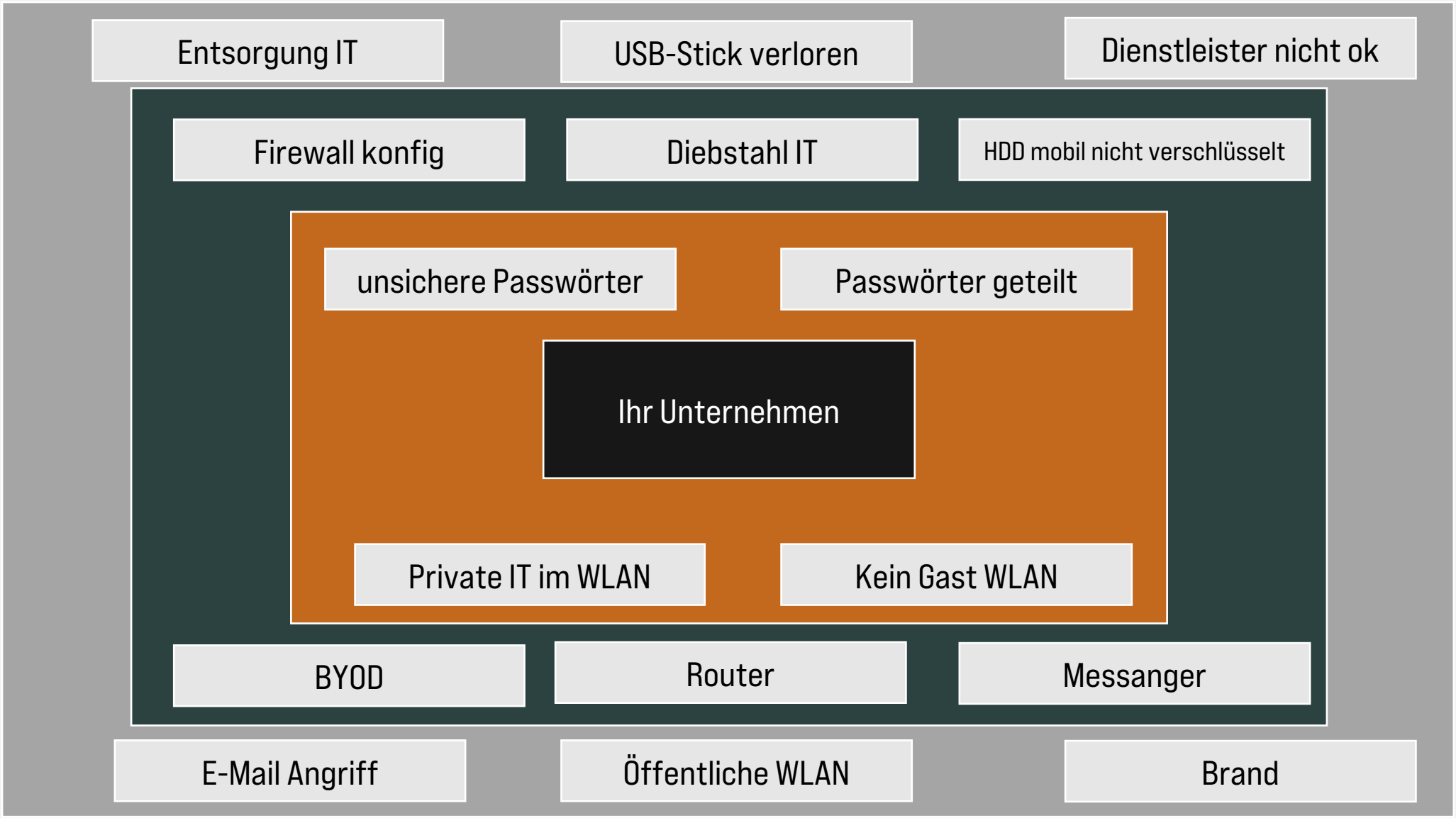
# Wie erkenne ich Risiken?

## Mögliche Einflüsse von außen nach innen



# Wie erkenne ich Risiken?

## Mögliche IT Risiken von außen nach innen



# Wie erkenne ich Risiken?

QS Kornmann quality solutions

## Beispiel einer Risikoermittlung am Beispiel Demo-Unternehmen (Fehlerbaummethode)

### Was muss passieren, dass wir kein Geld verdienen können?

- Mitarbeiter fallen aus
- Stromausfall
- Daten werden geklaut
- Daten werden verschlüsselt
- Ausfall Internet

**Demo-Unternehmen**

- ✓ 1 Geschäftsführer
- ✓ 20 Mitarbeiter
- ✓ Vertrieb Außendienst
- ✓ Herstellung
- ✓ Metall
- ✓ Maschinenpark
- ✓ Eigener Server
- ✓ Office365
- ✓ Eigenes Gebäude
- ✓ Home-Office

Unvollständige Demo-Daten | Keine Gewähr auf Richtig- oder Vollständigkeit

# Umgang mit Risiken

QS Kornmann quality solutions

## Beispiel einer Risikobearbeitung am Beispiel Demo-Unternehmen. (FMEA)

| | Auswirkungen |
|---|---|
| Mitarbeiter fallen aus | Kein Vertrieb<br>Keine Produktion |
| Stromausfall | Keine IT |
| Daten werden geklaut | Kundendaten gehen verloren |
| Daten werden verschlüsselt | Kein Zugriff mehr auf Daten |
| Ausfall Internet | Kein Zugriff auf Cloud Daten |

### Demo-Unternehmen

- ✓ 1 Geschäftsführer
- ✓ 20 Mitarbeiter
- ✓ Vertrieb Außendienst
- ✓ Herstellung
- ✓ Metall
- ✓ Maschinenpark
- ✓ Eigener Server
- ✓ Office365
- ✓ Eigenes Gebäude
- ✓ Home-Office

Unvollständige Demo-Daten | Keine Gewähr auf Richtig- oder Vollständigkeit

# Umgang mit Risiken

QS Kornmann quality solutions

## Beispiel einer Risikobearbeitung am Beispiel Demo-Unternehmen. (FMEA)

Eintrittswahrscheinlichkeit und Schadenshöhe

| | | |
|---|---|---|
| Mitarbeiter fallen aus | wahrscheinlich | vertretbar |
| Stromausfall | wahrscheinlich | hoch |
| Daten werden geklaut | unwahrscheinlich | sehr hoch |
| Daten werden verschlüsselt | wahrscheinlich | sehr hoch |
| Ausfall Internet | häufig | hoch |

### Demo-Unternehmen

- ✓ 1 Geschäftsführer
- ✓ 20 Mitarbeiter
- ✓ Vertrieb Außendienst
- ✓ Herstellung
- ✓ Metall
- ✓ Maschinenpark
- ✓ Eigener Server
- ✓ Office365
- ✓ Eigenes Gebäude
- ✓ Home-Office

Unvollständige Demo-Daten | Keine Gewähr auf Richtig- oder Vollständigkeit

# Umgang mit Risiken

QS Kornmann quality solutions

## Beispiel einer Risikobearbeitung am Beispiel Demo-Unternehmen. (FMEA)

### Klassifizierung

| | keine | gering | vertretbar | hoch | sehr hoch |
|---|---|---|---|---|---|
| Wird passieren | | | | | |
| häufig | | | | Ausfall Internet | |
| wahrscheinlich | | | Mitarbeiter fallen aus | Stromausfall | Daten werden verschlüsselt |
| un-wahrscheinlich | | | | | Daten werden geklaut |
| unmöglich | | | | | |

| | |
|---|---|
| | Prio WICHTIG |
| | Prio MITTEL |
| | Prio NIEDRIG |

### Demo-Unternehmen

- ✓ 1 Geschäftsführer
- ✓ 20 Mitarbeiter
- ✓ Vertrieb Außendienst
- ✓ Herstellung
- ✓ Metall
- ✓ Maschinenpark
- ✓ Eigener Server
- ✓ Office365
- ✓ Eigenes Gebäude
- ✓ Home-Office

Unvollständige Demo-Daten | Keine Gewähr auf Richtig- oder Vollständigkeit

# Umgang mit Risiken

- Wir haben über eine ausgewählte Methode die Risiken ermittelt.
- Wir haben die Auswirkung ermittelt.
- Wir haben die Wahrscheinlichkeit bewertet.
- Wir haben die Auswirkung bewertet.
- Wir haben die Risiken klassifiziert .

Mit diesen Punkten sind Sie sich Ihrer Risiken bewusst und haben diese priorisiert. Nun können Sie in eine gezielte Bearbeitung gehen und sich ggf. Unterstützung holen.

## Demo-Unternehmen

- ✓ 1 Geschäftsführer
- ✓ 20 Mitarbeiter
- ✓ Vertrieb Außenienst
- ✓ Herstellung
- ✓ Metall
- ✓ Maschinenpark
- ✓ Eigener Server
- ✓ Office365
- ✓ Eigenes Gebäude
- ✓ Home-Office

# Umgang mit Risiken

QS Kornmann quality solutions

## Beispiel einer Risikobearbeitung am Beispiel Ausfall Internet

| Ursachen | Maßnahme | Kosten | Wird das Risiko senken | erledigt |
|---|---|---|---|---|
| Router defekt | Router als Ersatzteil beschaffen | 1000,00 | JA | |
| Router kein Strom | USV | 300,00 | JA | |
| Bagger an der Straße | LTE Router beschaffen und einbinden | 1500,00 | JA | |
| Störung Betreiber | LTE Router beschaffen und einbinden | 1500,00 | JA | |

## Eintrittswahrscheinlichkeit und Schadenhöhe nach Maßnahmen

unwahrscheinlich

hoch

Die Auswirkung ist gleich, aber die Wahrscheinlichkeit ist gesunken und somit von Prio WICHTIG auf Prio NIEDRIG gerutscht.

### Demo-Unternehmen

- ✓ 1 Geschäftsführer
- ✓ 20 Mitarbeiter
- ✓ Vertrieb Außendienst
- ✓ Herstellung
- ✓ Metall
- ✓ Maschinenpark
- ✓ Eigener Server
- ✓ Office365
- ✓ Eigenes Gebäude
- ✓ Home-Office

Unvollständige Demo-Daten | Keine Gewähr auf Richtig- oder Vollständigkeit

# Umgang mit Risiken

## Beispiel einer FMEA

Version: 1.0 Datum: 01.07.2022

| | ID | Risiko Identifizierung | | | Risiko Analyse | | | | Risikobewertung | | | | | Risikobehandlung | | | | | | | | Risiko Analyse nach Behandlung | | | | Risikobewertung nach Behandlung | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Bedrohung | Schwachstelle | Risiko Owner | schreibung der potentiellen Auswirku | ntrittswahrscheinlichkeit | | Schadenshöhe | | RKZ | Risikoakzeptanz | Begründung | Datum\| Name | Umsetzung bis | Art. | Maßnahme zur Reduzierung Risiko | Normbezug der Maßnahme | Umsetzung abgeschlossen am \| durch | Nachweisdokumente | Beschreibung der potentiellen Auswirkung | Eintrittswahrscheinlichkeit | | Schadenshöhe | | RKZ | Risikoakzeptanz | Begründung | Datum\| Name |
| Mitarbeiter | P-1 | Isolation der Mitarbeiter | Infektionsketten | Geschäftsleitung | zum reduzieren von Infektionsketten kann es notwendig sein dass die Mitarbeiter nicht in das Unternehmen können und isoliert dezentral arbeiten müssen | Häufig | 12 | Ernst | 3 | 36 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | IT-Struktur auf dezentrales arbeiten umstellen. Notebooks uns endsprechende Hardware beschaffen | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Mitarbeiter | P-2 | Infektion der Mitarbeiter im Unternehmen | Mangelhaftes Hygienekonzept | Geschäftsleitung | Sind Mitarbeiter im Unternehmen kann es zu einer Infektionsketten unter den Mitarbeitern kommen | Häufig | 12 | kritisch | 8 | 96 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Hygiene Konzept erstellen. Mitarbeiter getrennt setzen. Schutzwände aufstellen Zeitversetztes arbeiten | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Mitarbeiter | P-3 | Infektion der Mitarbeiter im Unternehmen | Zutritt ins Unternehmen | Geschäftsleitung | Es findet keine Kontrollen statt ob Personen welche in das Unternehmen kommen gesund sind bzw. einen gültigen Impfstatus haben | Häufig | 12 | kritisch | 8 | 96 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Überprüfung Impfstatus und entsprechende Dokumentation als Nachweis gegenüber der Behörden | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Mitarbeiter | P-4 | Hoher Krankenstand der Mitarbeiter | Infektionen | Geschäftsleitung | Durch eine Pandemie ist der Krankenstand hoch und das Unternehmen ist nicht in der Lager seine Geschäfte aufrecht zu erhalten | Häufig | 12 | kritisch | 8 | 96 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Mitarbeiter isolieren und für Vertretung sorgen | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Mitarbeiter | P-5 | Mangelhafte Kommunikation der Mitarbeiter | Vernetzung im Unternehmen | Geschäftsleitung | Durch dezentrales Arbeiten geht wissen verloren | Wahrscheinlich | 11 | Ernst | 3 | 33 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Geeignete Medien bereit stellen damit sich die Mitarbeiter entsprechend austauschen können. | | 01.06.2021 MKO | | | | | | | | | | |
| Unternehmen | P-6 | Eingeschränkt Geschäftsfähig | Datenzugriff beim dezentralen Arbeiten | Geschäftsleitung | Mitarbeiter können beim dezentralen Arbeiten nicht auf notwendige Informationen vom Unternehmen zugreifen | Wahrscheinlich | 11 | Ernst | 3 | 33 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Zugriff auf internen IT-Infrastuktur herstellen damit Mitarbeiter entsprechend auf Daten Zugreifen können | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Unternehmen | P-7 | Diebstahl, Verlust von mobilen Endgeräten | Geräte sind mobil | Geschäftsleitung | Durch die Nutzung von mobilen Endgeräten ist das Verlustrisiko höher als die Nutzung von stationärer IT im Unternehmen | Gelegentlich | 4 | Ernst | 8 | 88 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Richtlinie erstellen | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Unternehmen | P-8 | Mangelhafter Absatz | Mangelhafte Verfügbarkeit von Verkaufsprodukten | Geschäftsleitung | Durch die Pandemie erhalten wir keine Waren mehr | Gelegentlich | 4 | Ernst | 3 | 12 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Ständiges Beobachten vom Markt und kritischen Komponenten bevorraten wenn möglich | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Unternehmen | P-9 | Verfügbarkeit Produkte | Insolvenz Dritter | Geschäftsleitung | Aufgrund der Pandemie können Geschäftspartner in die die Insolvenz geraten und wir somit Engpässe ich den die Verfügbarkeit von Waren erleiden | Wahrscheinlich | 11 | kritisch | 8 | 88 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | laufende Gespräche mit Lieferanten führen und ggf. nach Alternativen Ausschau halten | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Unternehmen | P-10 | Preise steigen | Verfügbarkeit von Waren | Geschäftsleitung | Durch eine Verknappung von Waren steigt der Preis | Wahrscheinlich | 11 | Ernst | 3 | 33 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Preisspiegel beobachten und kaufen wenn günstig. Sonst ebenfalls Preise entsprechend anpassen | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Unternehmen | P-11 | Umsatz und Gewinn | Weniger Kaufkraft weniger Bedarf am Markt | Geschäftsleitung | Sinkender Umsatz und Gewinn durch geringer Kaufkraft und Warenverfügbarkeit | Häufig | 12 | kritisch | 8 | 96 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Aktion und Angebote locken. Kundenbindung nicht verlieren | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Informationssicherheit | P-12 | Datenschutzverletzung | Datensicherheit und Datenschutz beim dezentralen Arbeiten | Geschäftsleitung | Der Datenschutz kann bei dezentralen Arbeiten nicht aufrecht gehalten werden | Wahrscheinlich | 11 | kritisch | 8 | 88 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Richtlinien Homeoffice erstellen. Mitarbeiter sensibilisieren | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Informationssicherheit | P-13 | Datenschutzverletzung | Mangelhafte Dokumentation | Geschäftsleitung | Die Umsetzung der Datenschutzrichtlinien Anforderungen in der Pandemie sind nicht beschreiben und führen Datenschutzverletzungen mit entsprechenden Strafen | Wahrscheinlich | 11 | kritisch | 8 | 88 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Einbeziehung DSB in die Betrachtung. Erstellungen von Verarbeitungstätigkeiten, Löschkonzept usw. | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Informationssicherheit | P-14 | Mangelhafter Support der IT | Dienstleister hoher Krankenstand | Geschäftsleitung | Aufgrund von hohen Krankenständen bei unseren IT-Dienstleister kann es zu einer eingeschränkten Verfügbarkeit kommen im Servicefall | Wahrscheinlich | 11 | Ernst | 3 | 33 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Internen Mitarbeiter qualifizieren kleiner Problem direkt zu lösen. SLA mit Dienstleister abschließen | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Informationssicherheit | P-15 | Hackerangriff | Datensicherheit und Datenschutz beim dezentralen Arbeiten | Geschäftsleitung | Die Datensicherheit kann bei dezentralen Arbeiten nicht aufrecht gehalten werden | Wahrscheinlich | 11 | kritisch | 8 | 88 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | VPN Zugriff oder Cloud Zugriff mit MFA einrichten | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Informationssicherheit | P-16 | Eingeschränkt geschäftsfähig | Keine notwendige IT-Struktur für dezentrales Arbeiten | Geschäftsleitung | Aufgrund der Verfügbarkeit von IT-Endgeräten haben die Mitarbeiter keine Möglichkeit zum dezentralen Arbeiten | Wahrscheinlich | 11 | kritisch | 8 | 88 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Beschaffung entsprechender IT-Endgeräte und | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |
| Informationssicherheit | P-17 | IT-Sicherheit | Die IT-Sicherheit ist gefährdet durch dezentrale Endgeräte | Geschäftsleitung | Dadurch das viele Endgeräte dezentral agieren verschiebt sich das IT-Sicherheit auf die Endgeräte bzw. auf die End User | Häufig | 12 | Ernst | 3 | 36 | nicht akzeptiert | Risiko nicht angemessen | 01.04.2020 MKO | 01.06.2020 | Reduzieren | Firewall und Virenschutz dezentral aktuell halten. | | 01.06.2021 MKO | | | Gelegentlich | 4 | Vernachlässigbar | 1 | 4 | | | |

# Umgang mit Risiken - Zusammenfassung

QS Kornmann quality solutions

## Definieren Sie Ihre Risiken

- Nutzen Sie hierzu unterschiedliche Methoden
- Schreiben Sie diese Risiken in eine Tabelle

## Bewerten Sie jedes Risiko

- Eintrittswahrscheinlichkeit und Auswirkung ( FMEA)
- Nutzen Sie die Darstellung auf der vorhergehenden Seite

## Definieren Sie, wie Sie mit dem Risiko umgehen

- Tragen (akzeptieren)
- Teilen (Versicherung, Outsourcing)
- Reduzieren (entsprechende Maßnahmen einleiten)
- Vermeiden (Ursache abschalten)

# Umgang mit Risiken - Zusammenfassung

QS Kornmann quality solutions

## Dokumentieren Sie, was Sie getan haben

- Welche Schritte haben Sie unternommen?
- Warum haben Sie akzeptiert?
- An welche Partei ggf. transferiert?

## Bewerten Sie das Risiko erneut nach NACH der Umsetzung

- Hat die Maßnahme das Risiko reduziert?
- Ist das Risiko nach der Maßnahme akzeptabel?

## Überwachen Sie das Risikomanagement fortlaufend !!

- Prüfen Sie regemäßig ob Ihre Maßnahmen noch wirksam sind.
- Prüfen Sie ob ggf. neue Risiken aufgenommen werden müssen.
- Dokumentieren Sie diese Überwachung.

# Und jetzt ?

# Fazit

- Definieren Sie Ihre Risiken - wie erläutert.
- Bestimmen Sie damit auch Ihren Risikoappetit. Was wollen oder können Sie riskieren? Es obliegt Ihnen die Auswirkungen und Höhe zu bewerten.
- Kennen Sie Ihre Risiken, können Sie entsprechend handeln.
- Holen Sie sich Unterstützung bei der Umsetzung, falls notwendig.
- In der Regel werden Sie Maßnahmen zum Reduzieren treffen.
- Diese Maßnahmen bestehen zum Teil aus:
  - Technische Umsetzung
  - Anweisungen, Vorgaben
  - Notfall Handbücher (Notfallhandbuch Pandemie)
- Schulen Sie Maßnahmen und verteilen Sie das Wissen an betroffene Mitarbeiter
- Simulieren Sie Notfälle und lernen Sie aus den Erfahrungen

# Nützliche LINKS

QS Kornmann quality solutions

## 01

### VDA Whitepaper

https://www.vda.de/dam/jcr:152a90b4-fd97-4f5c-88aa-4c45f506ceef/Whitepaper%20Risikomanagement%20in%20der%20Informationssicherheit.pdf?mode=view

## 02

### Migosens

https://migosens.de/risikomanagement-in-der-informationssicherheit/

## 03

### BSI-Standard 200-3

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html

## 04

### BSI Elementar-gefährdungen

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.html?nn=128562

## 05

### Unsere Risikomatrix

https://qs-kornmann.de/uploads/2023/05/Risiko-Website.xlsx

# Vielen Dank für Ihre Aufmerksamkeit

Ihr Profi in Sachen
Datenschutz, Informationssicherheit
und Qualitätsmanagement

Sudetenstrasse 33  35625 Hüttenberg.
info@qs-kornmann.de | https://www.qs-kornmann.de
06403 / 92 95 287
@Kornmann  Michael Kornmann