hvs consulting

Handbuch
IT-Notfallmanagement

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.

Für eine umfassende Beratung kontaktieren Sie uns gerne.

Verantwortlich	<name>
Freigabe	<name>
Status	Entwurf | Review | Freigegeben
Version	x.x
Gültig ab	<datum>
Klassifikation	<Klassifikation>

Inhaltsverzeichnis

1 Allgemeines 3

1.1 Zielsetzung 3
1.2 Zielgruppe 3
1.3 Verstöße 3
1.4 Abweichungen 3
1.5 Definitionen 4

2 Rollen und Verantwortlichkeiten 5

2.1 IT-Notfallteam 5
2.2 IT-Notfallmanager (Security Board) 7
2.3 IT-Notfallmanagement-Koordinator 7
2.4 Assistenz 8

3 Ablauforganisation IT-Notfallbewältigung 9

3.1 Identifikation Vorfall mit Notfallpotenzial 10
3.2 Erstanalyse Lage durchführen 10
3.3 Sofortmaßnahmen prüfen und durchführen 11
3.4 IT-Notfallteam einberufen 11
3.5 Lagebewertung vornehmen 12
3.6 Eskalation als Krise prüfen 12
3.7 Expertenteam für Krisenbehandlung organisieren 12
3.8 Relevante Stellen informieren 13
3.9 Lösungen erarbeiten, umsetzen und prüfen 13
3.10 Abschluss kommunizieren 16
3.11 Lessons learned und Abschlussbericht 16

4 Notfalldokumentation 17

4.1 Anforderung an die Notfalldokumentation 17
4.2 Inhalt der Dokumentation und Aufbewahrungsorte 17
4.3 Notfallausstattung 17

5 Notfallübungen 18

5.1 Planung von Übungen im Bereich Notfallmanagement 18
5.2 Durchführung von Tests und Übungen 18

Farblegende Mustervorlage:

Anzupassen an unternehmensspezifische Begrifflichkeiten

Optionale Passagen (z.B. private Nutzung erlaubt/verboten)

1 Allgemeines

1.1 Zielsetzung

Das vorliegende Handbuch dient als Rahmenwerk zur Vorbereitung und Reaktion auf Ereignisse und Situationen in Bezug auf IT-Sicherheit, in denen die präventiven Maßnahmen das Eintreten eines Notfalls nicht abwenden konnten. Es soll ebenfalls Anwendung finden bei akuten Bedrohungen, die unverzügliche Aktivitäten erfordern, da ein Schadenseintritt bei KUNDE mit hoher Wahrscheinlichkeit zu erwarten ist. Auch, wenn dieses Dokument ausschließlich Fälle mit Bezug auf IT-Sicherheit adressiert, so ist die Nomenklatur bewusst so neutral gewählt, dass dieses Dokument als Vorlage für andere Notfall-Szenarien genutzt werden kann.

Das Ziel besteht darin, mit Hilfe einer funktionierenden Aufbau- und Ablauforganisation die nur bedingt vorhersehbaren Vorfälle möglichst zielgerichtet, zügig, nachhaltig und unter weitgehender Vermeidung zusätzlicher Beeinträchtigungen zu bearbeiten und soweit möglich zu beseitigen.

Das IT-Notfallmanagement stellt dabei die Ebene zwischen der routinemäßigen Behandlung von (Sicherheits-)Vorfällen (sog. Störungen) mit nur geringen Auswirkungen bis hin zu Major Incidents mit Security Bezug und Krisenfällen mit erheblichen Auswirkungen (siehe Kap. 1.5 Definitionen) dar.

Die im Kapitel 5 (Notfallübungen) beschriebenen Maßnahmen sind darauf ausgerichtet, bestmögliche Vorkehrungen für das Eintreten eines Notfalls zu treffen. Demgegenüber soll mit dem in Kapitel 3 (Ablauforganisation IT-Notfallbewältigung) aufgeführten Prozessablauf Hilfestellungen bei der tatsächlichen Bewältigung eines Notfalls bzw. der Durchführung einer Übung gegeben werden.

1.2 Zielgruppe

Die Vorgaben in dieser Richtlinie sind für alle Mitarbeiter der KUNDE verbindlich, die an der Vorbereitung und Umsetzung von Maßnahmen im Bereich IT-Notfallmanagement sowie der Bewältigung von IT-Notfällen beteiligt sind. Dies betrifft insbesondere die nachfolgenden Rollen:

- IT-Notfallteam
- IT-Notfallmanager (Security Board)
- IT-Notfallmanagement-Koordinator
- Assistenz

Darüber hinaus muss beachtet werden, dass weiterführende Regeln (gesetzliche, vertragliche oder interne Anforderungen) existieren können, die zusätzlich zu den Regeln in dieser Richtlinie beachtet werden müssen.

Die Einhaltung der Vorgaben in dieser Richtlinie gilt gleichermaßen für Mitarbeiter der KUNDE als auch für externe bzw. temporäre Mitarbeiter (Berater, Freelancer, Mitarbeiter von Fremdfirmen, Mitarbeiter von Dienstleistern, Zeit- bzw. Leiharbeitskräfte, Mitarbeiter aus Arbeitnehmerüberlassung, Werksstudenten, Praktikanten, …), die Aufgaben im oben genannten Tätigkeitsfeld im Namen der KUNDE erbringen bzw. bei der Leistungserbringung der KUNDE mitwirken.

1.3 Verstöße

Verletzungen bzw. die Missachtung von den Vorgaben dieser Richtlinie können sanktioniert werden. Einzelheiten sind in der Information Security Policy (ISP) der KUNDE (Kap. 1.4) beschrieben.

1.4 Abweichungen

Option 1 Ausnahmeprozess nachfolgend:

Abweichungen von den Vorgaben dieser Richtlinie müssen an den Informationssicherheits-beauftragten (ISB) gemeldet werden. Der ISB muss die Abweichung bewerten und – je nach Risiko – ablehnen, oder genehmigen.

Abhängig vom Risiko der Regelabweichung kann eine Genehmigung pauschal, oder unter Auflagen gewährt werden, d.h. die Regelabweichung ist nur zulässig, sofern die definierten risikominimierenden Maßnahmen umgesetzt werden.

Eine Ausnahme kann dabei sowohl dauerhaft als auch temporär genehmigt werden. Die Entscheidung der Ablehnung bzw. Genehmigung (inkl. Dauer der genehmigten Ausnahme) muss vom ISB dokumentiert und nach Ablauf der Frist erneut überprüft werden.

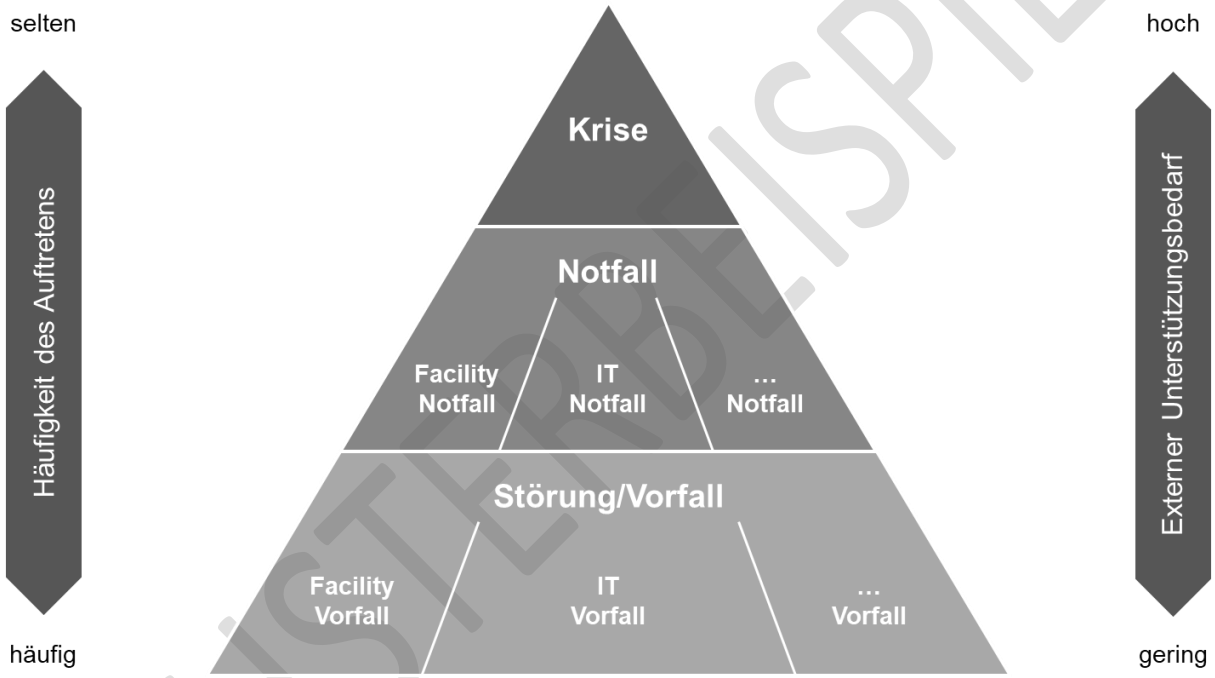
Option 2 Verweis auf Ausnahmeprozess:

Abweichungen von den Vorgaben dieser Richtlinie müssen gemäß des ISMS-Ausnahmebehandlungsprozesses gehandhabt werden.

1.5 Definitionen

Die nachstehenden Definitionen gelten für alle relevanten Bereiche bzw. auslösenden Ursachen. Ereignisse in Bezug auf IT-Sicherheit stellen somit eine (mögliche) Teilmenge dar.

Die Regelungen in Bezug auf IT-Notfallmanagement werden auch für sich daraus entwickelnde Krisensituationen angewendet, solange hierfür keine übergeordneten Regelungen (unternehmensweites Krisenmanagement) etabliert sind.



Krise:

Unerwartetes Ereignis oder unerwartete Situation, die zu einer Unterbrechung von Geschäftsprozessen oder einer Beeinträchtigung der Geschäftstätigkeit bzw. des Ansehens von KUNDE oder Auswirkungen auf die körperliche und/oder geistige Unversehrtheit von Personen hat. Die durch eine Krise entstehenden Schäden sind aus Sicht des Unternehmens bzw. der betroffenen Personen als erheblich und/oder nicht nur von kurzfristiger Dauer einzustufen. Für die Bewältigung der Krise stehen aufgrund der Einmaligkeit der Konstellation nur bedingt im Voraus festgelegte Verfahren und Dokumentationen zur Verfügung. Zur Lagebewertung, Analyse von Ursachen und Lösungsmöglichkeiten sowie für die Planung und Umsetzung von Interimslösungen wird eine interdisziplinär zusammengesetzte Krisenorganisation benötigt, die für die Dauer der Krise (mehrere Stunden bis hin zu Wochen oder Monaten) etabliert wird. Zusätzlich kann die Einbindung externer Kräfte zur Schadensbegrenzung, Ursachenermittlung sowie Krisenbewältigung sinnvoll und erforderlich sein.

Katastrophen stellen einen Sonderfall von Krisen dar, indem sie zeitlich und örtlich kaum begrenzbar sind und großflächige Auswirkungen auf Menschen, Infrastrukturen und/oder Werte haben. Die Bewältigung einer Katastrophe erfordert die Unterstützung externer Kräfte und steht häufig unter Einbindung oder Leitung einer externen Katastrophenschutzorganisation.

Notfall:

Unerwartetes Ereignis oder unerwartete Situation mit erheblichen, jedoch zeitlich bzw. unter Umständen örtlich/regional absehbaren Auswirkungen, die nicht im Rahmen des Tagesgeschäftes bzw. des Störungsmanagements beseitigt werden kann. Die Ursachenermittlung und Behandlung erfordern die kurzfristige Bereitstellung entsprechender Ressourcen, möglicherweise aus unterschiedlichen Bereichen sowie evtl. externer Spezialisten. Im Rahmen der Analyse des Notfalls ist die Erfordernis zur Eskalation als Krise zur prüfen.

Störung:

Ereignis oder Situation, in der Prozesse oder Ressourcen von KUNDE nicht wie vorgesehen funktionieren oder die Auswirkungen auf die Unversehrtheit von Personen hat. Die durch eine Störung entstehenden Schäden sind aus Sicht des Unternehmens bzw. der betroffenen Personen als gering und/oder zeitlich absehbar einzustufen. Für die Störungsbehebung reichen im Regelfall Ressourcen aus dem Tagesgeschäft aus.

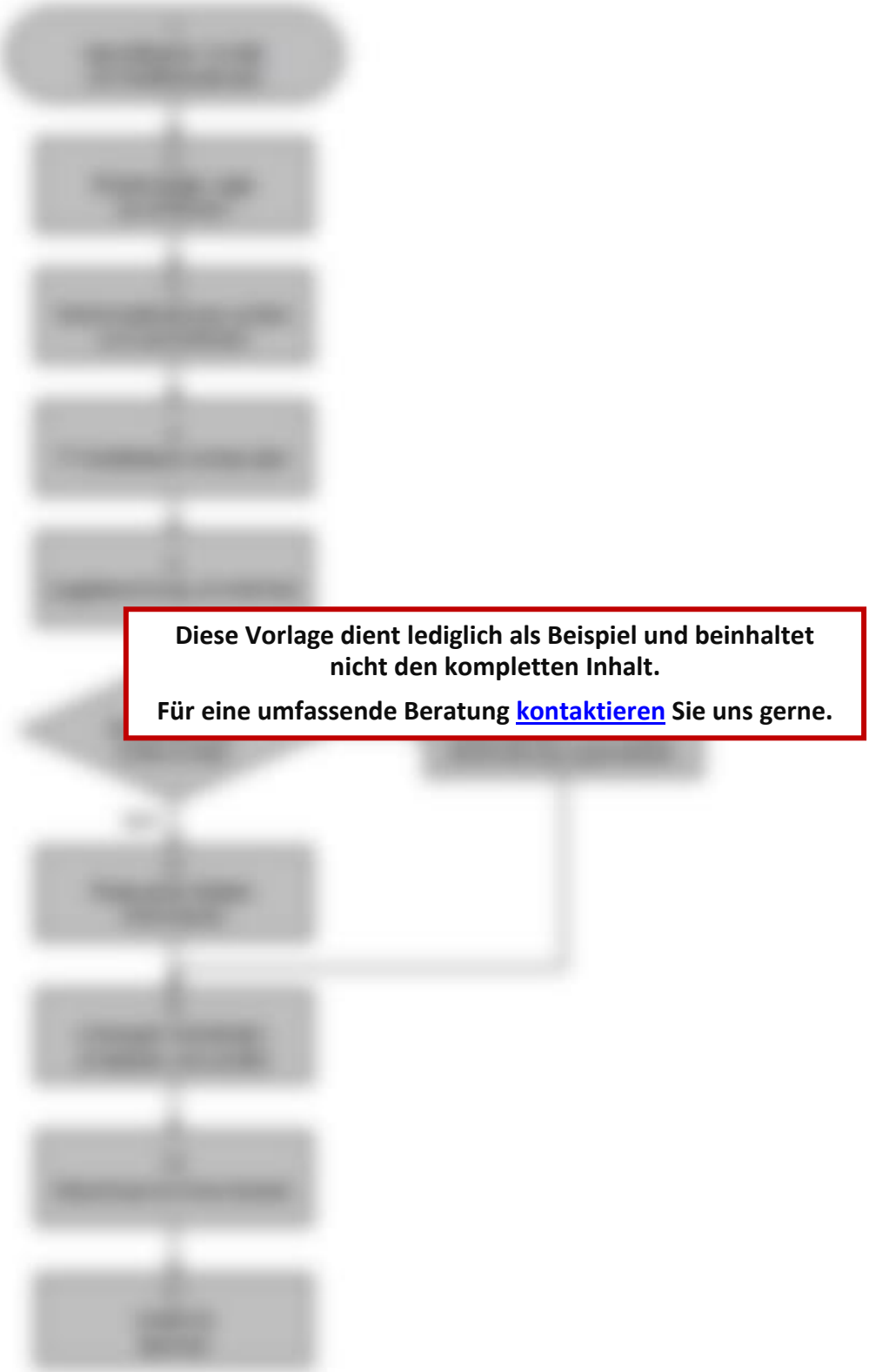
2 Rollen und Verantwortlichkeiten

2.1 IT-Notfallteam

Für die fallweise Etablierung eines IT-Notfallteams stehen neben den namentlich benannten Rolleninhabern ein Pool von Mitarbeitern aus den verschiedenen Bereichen zur Verfügung. Die festen Mitglieder sind bei jedem Notfall bzw. jeder Übung eingebunden, die fallweisen Mitglieder nur bei Bedarf, d.h. in Abhängigkeit des konkreten Notfalls.

Für das IT-Notfallteam ist aktuell keine permanente Verfügbarkeit in Form eines Bereitschaftsdienstes erforderlich. Stattdessen werden die betreffenden Personen in einem Notfall kontaktiert und nehmen außerhalb von Standardarbeitszeiten die vorgesehene Rolle war, sofern es die Umstände erlauben.

3 Ablauforganisation IT-Notfallbewältigung



Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.

Für eine umfassende Beratung kontaktieren Sie uns gerne.

3.2 Erstanalyse Lage durchführen

Die wichtigste Aufgabe des IT-Notfallmanagers besteht darin, eine Erstanalyse der aktuellen Situation zusammen mit dem IT-Support vorzunehmen, aus der sich die Erfordernis für die Eskalation als Notfall und dementsprechend die Einberufung des IT-Notfallteams ergibt.

Bei dieser Bewertung sind insbesondere folgende Punkte zu betrachten:

- Reichweite des Problems (z.B. Anzahl betroffener Systeme, Bereiche/Personen, Daten, Kunden)
- Betroffene Systeme (z.B. Kritikalität aus Verfügbarkeitssicht, Relevanz/Verbreitungsgrad im Unternehmen)
- Betroffene Informationen (z.B. sensible Unternehmensinformationen, personenbezogene Daten)
- Bereits absehbare Auswirkungen (z.B. Beeinträchtigungen von Abläufen, Wahrnehmbarkeit intern/extern, Meldepflichten)
- Mögliche/wahrscheinliche Ursachen (z.B. technischer Defekt, Bedienerfehler, absichtliche Handlungen)
- Dauer für Analyse und Behebung (z.B. Einfluss auf Arbeitszeiten betroffener Bereiche/Personen, Erfordernis von mehreren „Schichten“ für Lösungsteams)
- Erforderliche Ressourcen für Behebung (z.B. internes Personal, externer Unterstützungsbedarf, Einschaltung von Ermittlungsbehörden)

Sollten für die Beurteilung weitere Informationen vom IT-Support oder anderen Bereichen/Personen benötigt werden, hat der IT-Notfallmanager in diesem Zusammenhang das Recht, diese Bereiche/Personen kurzfristig einzubinden und mit entsprechenden Aufgaben zur Unterstützung zu betrauen.

In jedem Fall ist der Krisenmanager von KUNDE bzw. eine seiner Stellvertretungen über den Notfall und die wichtigsten Erkenntnisse in diesem Zusammenhang auf einem geeigneten und sicheren Weg zu informieren.

Während der Arbeitsphasen herrscht – im Gegensatz zur Beratungs-/Entscheidungsphase – für gewöhnlich hektische Betriebsamkeit aus parallelen Gesprächen und Telefonaten sowie der Ausarbeitung von Detailplänen (insbesondere unter Anwendung des nachfolgend beschriebenen FORDEC-Prinzips).

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.

Für eine umfassende Beratung kontaktieren Sie uns gerne.

4 Notfalldokumentation

Der schnelle Zugriff auf die vorbereitete Dokumentation für die Bewältigung eines Notfalls einschließlich aller Detaildokumente – auch bei Ausfall oder erheblicher Beeinträchtigung der Infrastruktur und IT-Systeme – ist im Notfall von entscheidender Bedeutung. Dementsprechend ist bei der Speicherung darauf zu achten, möglichst gängige Formate zu verwenden, die auf Standardrechnern zur Verfügung stehen bzw. kurzfristig einsetzbar sind.

Zu dieser Dokumentation zählen insbesondere

- die übergeordnete Dokumentation des Notfallmanagements in Form dieses Handbuchs einschließlich Anlagen;
- Detaildokumentationen zu ausgewählten Notfallszenarien (soweit vorhanden);
- Detaildokumentationen der jeweiligen Fachbereiche (z.B. Checklisten, vorbereitete Pressetexte, Runbooks für gravierende Vorfälle).

4.1 Anforderung an die Notfalldokumentation

Bei der Erstellung der Dokumentation ist darauf zu achten, dass diese leicht lesbar ist, eindeutige Hinweise (z.B. zur Vermeidung typischer Fehler) deutlich gekennzeichnet sind und dass in einer Notsituation jederzeit ist, dass ein fachkundiger Dritter damit die erforderlichen Aktivitäten durchführen kann.

Die Dokumentation darf keinesfalls vertrauliche Informationen (z.B. Zertifikatsdaten) enthalten, sondern dem Leser nur die Information liefern, wie er an diese Informationen gelangt.

Als erste Maßnahme zur Qualitätssicherung sollte die Dokumentation von einem Kollegen gelesen und auf Verständlichkeit, Vollständigkeit und Umsetzbarkeit geprüft werden. Darüber hinaus sollte die gesamte Dokumentation im Rahmen von Abstimmungsgesprächen, dem IT-Notfallteam übersichtsweise vorgestellt und innerhalb dieser Gruppe abgestimmt werden.

4.2 Inhalt der Dokumentation und Aufbewahrungsorte

Die Notfalldokumentation von KUNDE besteht aus den im Anhang (siehe Anhang 1: Notfalldokumentation) aufgeführten Bestandteilen. Die verantwortlichen Personen müssen dafür Sorge tragen, dass die Dokumentation in ihrem Zuständigkeitsbereich in angemessenen Abständen geprüft und bei Änderungsbedarf an den in der Tabelle aufgeführten Orten komplett mit der neuen Version aktualisiert wird. An unterschiedlichen Orten muss immer der aktuelle Stand der Dokumentation aufbewahrt werden.

Sofern weitere Aufbewahrungsorte für Teile der Dokumentation als erforderlich angesehen werden, so ist dies in der Tabelle zu ergänzen, um eine lückenlose Aktualisierung zu gewährleisten.

4.3 Notfallausstattung

Aktuell wird für die Bewältigung von Notfällen keine Ausstattung in Form von Räumen, Technik oder sonstigem Equipment vorgehalten, die exklusiv für Notfälle zur Verfügung steht. Stattdessen wird im Notfall mit Priorität auf ausgewählte Räume und Ausstattung zurückgegriffen, d.h. das IT-Notfallteam überwacht im Bedarfsfall die planmäßig vorgesehene Nutzung. Eine Übersicht der vorgehaltenen Notfallausstattung ist im Anhang aufgeführt.

Der IT-Notfallmanagement-Koordinator ist zuständig dafür, dass die erforderliche Ausstattung vorhanden bzw. funktionsfähig ist. Darüber hinaus ist er verantwortlich dafür, die Erfordernis dedizierter Notfallausstattung zu prüfen und deren Beschaffung vorzuschlagen bzw. zu initiieren.

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.

Für eine umfassende Beratung kontaktieren Sie uns gerne.

Bereit, Ihr ISMS aufzubauen?

Lassen Sie uns gemeinsam starten!

Kontaktieren Sie uns jetzt für eine individuelle Beratung und Unterstützung.