# Warum Informationssicherheit in der Verantwortung des C-Levels liegt und nicht alleinige Aufgabe der IT-Abteilung ist.


**Herausgeber**

mabs4.0 Deutschland GmbH
Südring 133
42579 Heiligenhaus

Telefon: +49 2056 267 9059
E-Mail: kontakt@mabs40.com

Internet: http://mabs40.de.com

# Inhalt

# Vorwort

Liebe/r Leser/in,

herzlichen Dank für Ihr Interesse an unserem Portfolio.

Die **mabs4.0 Deutschland GmbH** aus der Nähe Düsseldorfs ist ein Beratungshaus mit dem spezifischen Fokus auf **IT- & Informationssicherheit, Datenschutz und das Business Process Management**.

Als solches unterstützen wir erfolgreich unsere Kunden unter anderem bei der Umsetzung und Einführung von **Informationssicherheitsmanagementsystemen (ISMS) wie beispielsweise gemäß ISO27001, BSI-Grundschutz oder TISAX® unter Berücksichtigung der DSGVO.**

Auch das parallele Management verschiedenster, meist ineinandergreifender Normen („Multi-Normen-Management“) kann dabei in den Mittelpunkt rücken.

Unser erfahrenes Team unterstützt Sie beratend als auch umsetzend mit nachgewiesener Expertise und langjährige Erfahrungen bei den für Sie notwendigen Ausarbeitungen und Anpassungen.

Unser Ziel ist es, unsere Kunden als Partner in Augenhöhe nach seinem tatsächlichen Bedarf zu unterstützen.

Unsere Leistungen orientieren sich immer nach der benötigten Angemessenheit und Wirtschaftlichkeit.

Kontaktieren Sie uns gerne und unverbindlich für ein erstes kostenloses Beratungsgespräch. Gerne kommen wir auch zu Ihnen und bewerten mit Ihnen Ihre Herausforderungen.

Herzliche Grüße

*Geschäftsführer der mabs4.0 Deutschland GmbH*
Eric Schneider

# Über die mabs4.0 Deutschland GmbH

Die mabs4.0 Deutschland GmbH (kurz: mabs) ist ein international agierender und unabhängiger Düsseldorfer Spezialist für

- IT & Informationssicherheit, Cybersicherheit,
- Integrierte Managementsysteme und
- Business Process Management.

Mit nachgewiesener Expertise behandelt die mabs die gesetzlichen und normativen Anforderungen zur Informationssicherheit, wie das deutsche IT- & Informationssicherheitsgesetz oder die EU-DSGVO genauso wie Kunden- und Normanforderungen (z.B. TISAX® oder ISO27001) oder Maßnahmen der Digitalisierung (z.B. Cybersicherheit) und setzt diese erfolgreich gemeinsam mit Ihren Kunden um.

Die häufig hinzukommenden verschiedenen, teils bestehenden, Anforderungen aus Umweltschutz (z.B. ISO 14001), Qualitätsnormen (ISO 9001), Arbeitssicherheit (ISO 45001) oder weiterer Anforderungen können zudem in einem integrierten Managementsystem (IMS) erfasst werden.

Anhängige oder betroffene Prozesse und Strukturen werden durch unsere Experten bei Bedarf analysiert und modelliert.

mabs unterstützt seine Kunden aus den Branchen Automotive, Industrie & Maschinenbau, Dienstleistungen, Banking, Telekommunikation, Gesundheitswesen und Pharmazie in ihren Vorhaben mit Augenmaß und schafft so transparente Projektstrukturen und echten Kundennutzen.

# Unser USP

Wir bei mabs haben uns auf unsere Fachkompetenzen fokussiert und bauen diese stetig weiter aus. Mehr als 50 Jahre Praxis- und Projekterfahrung in unterschiedlichen Branchen haben uns gelehrt, dass stabile Organisationsprozesse das Ausfallrisiko von IT- & Informationssicherheit gestützten Wertschöpfungsketten minimiert.

Wir sind hoch qualifiziert, erfahren und motiviert – unser Ziel ist es, Ihre Organisation bestmöglich ganzheitlich einzubinden, um Ihre Resilienz zu stärken. Wir sind nicht die klassischen Berater, wir sind Ihr Partner und Verbündeter zur Sicherung Ihrer Informationswerte.

Mit mabs zusammenzuarbeiten bedeutet immer effizient und mit Augenmaß gemeinsam passende Lösungen für Ihre Organisation zu finden. Fokussiert und zielgerichtet. Wir bringen best practise mit und helfen Ihnen Fehler zu vermeiden und einen Schritt voraus zu sein.

Wir sind Profis in dem, was wir tun, wo wir nicht die Experten sind, arbeiten wir mit den Profis aus unserem Netzwerk zusammen.

Unsere Experten hören Ihnen zu. Nicht um zu antworten, sondern um zu verstehen.

○ Etablierte Prozesse und Verantwortlichkeiten ○ Kostenminimierung ○ Nachweise der Erfüllung von Kundenanforderungen ○ Nachweis der Erfüllung von normativen und gesetzlichen Anforderungen ○ Haftungsreduzierung ○ Wettbewerbsvorteile ○ Minimierung von Risiken und möglichen Schäden

## Zusammenfassung

Viele Unternehmenslenker gehen davon aus, dass IT- & Informations- sowie Cybersicherheit alleinige Aufgabe der IT-Abteilung ist.

Dies ist es jedoch definitiv nicht! Die Verantwortung für den Schutz der Informationswerte liegt unzweifelhaft auf der Seite des C-Level Managements. Die Umsetzung der IT- & Informations- sowie Cybersicherheit erfolgt dabei durch alle Unternehmensebenen.

IT- & Informations- sowie Cybersicherheit kann nur gewährleistet werden, wenn sowohl technische als auch organisatorische Maßnahmen ineinandergreifen und sich sinnvoll ergänzen.

Hierzu gehören beispielsweise gut geschulte Mitarbeiter, klare Rahmenbedingungen zur Nutzung von Betriebsmitteln, die Kenntnis über mögliche Risiken und deren Eintrittswahrscheinlichkeit sowie klare Handlungsanweisungen für den Fall eines Sicherheitsereignis, um nur einige Punkte zu nennen.

Mit einem Informationssicherheitsmanagementsystems (ISMS) etabliert das C-Level Management ein wirksames Instrument, um das Schutzniveau der gesamten Organisation zu erhöhen, zu messen und stetig dem Bedarf anzupassen.

## Die Bedeutung von Informationssicherheit im Unternehmenskontext

In einer Ära zunehmender Digitalisierung und Vernetzung stehen Unternehmen nicht nur vor unbegrenzten Möglichkeiten, sondern auch vor wachsenden Herausforderungen. Cyberangriffe haben sich zu einer omnipräsenten Bedrohung entwickelt, die Organisationen aller Größenordnungen betrifft. Die Frage, die sich nun stellt, ist nicht, ob ein Unternehmen Ziel eines Angriffs wird, sondern vielmehr, wann und in welcher Form.

Die Verantwortung für die Sicherheit von Unternehmensinformationen kann nicht allein auf den Schultern der IT-Abteilung ruhen. Vielmehr liegt es im Interesse des Managements, eine umfassende Strategie zur Informationssicherheit zu entwickeln und zu implementieren. Das Management, insbesondere das C-Level, spielt eine entscheidende Rolle in der Gestaltung dieser Sicherheitsstrategie. Es steht nicht nur im Mittelpunkt der Verantwortung für die Gesamtleitung des Unternehmens, sondern trägt auch die Verantwortung dafür, dass Informationen und Daten angemessen geschützt sind.

Die Digitalisierung hat die Dynamik von Unternehmensabläufen transformiert, wodurch das Management zunehmend in der Pflicht steht, die Sicherheitsagenda anzuführen. C-Levels müssen nicht nur die technischen Aspekte der Informationssicherheit verstehen, sondern auch die strategischen und geschäftlichen Auswirkungen von Sicherheitsentscheidungen berücksichtigen. Eine fundierte Sicherheitsstrategie ist nicht nur eine Verteidigungsmaßnahme gegen potenzielle Bedrohungen, sondern auch ein integraler Bestandteil des langfristigen Erfolgs und der Widerstandsfähigkeit eines Unternehmens.

In den folgenden Abschnitten werden wir genauer darauf eingehen, warum die Verantwortung für Informationssicherheit nicht allein in den Händen der IT-Abteilung liegen kann, sondern eine Führungsaufgabe ist, die das gesamte C-Level-Management einbeziehen muss.

## Die Rolle des C-Levels in der Informationssicherheit

Die Herausforderungen der Informationssicherheit erfordern eine ganzheitliche Herangehensweise, die über die Grenzen der IT-Abteilung hinausgeht. Das C-Level-Management trägt eine zentrale Verantwortung, nicht nur für die finanzielle Leistungsfähigkeit des Unternehmens, sondern auch für die Sicherung und den Schutz seiner wertvollsten Ressource: Informationen.

In der heutigen digitalen Landschaft ist Informationssicherheit keine isolierte technische Angelegenheit mehr, sondern ein integraler Bestandteil der Unternehmensstrategie. Das C-Level muss sich bewusst sein, dass Cyberangriffe nicht nur finanzielle Verluste nach sich ziehen können, sondern auch den eigenen Ruf schädigen können und das Vertrauen der Kunden gefährden. Eine erfolgreiche Sicherheitsstrategie erfordert daher die enge Zusammenarbeit des Managements mit der IT-Abteilung und anderen relevanten Stakeholdern.

Die Rolle des C-Levels besteht nicht nur darin, Sicherheitsrichtlinien zu genehmigen, sondern aktiv eine Sicherheitskultur zu fördern. Das Management muss den Ton für eine proaktive Haltung gegenüber Informationssicherheit setzen und klare Erwartungen an alle Mitarbeiter kommunizieren. Durch das Verständnis der geschäftlichen Auswirkungen von Sicherheitsentscheidungen kann das C-Level sicherstellen, dass Ressourcen effektiv eingesetzt werden und dass Sicherheitsmaßnahmen die geschäftlichen Ziele unterstützen.

Beispiele erfolgreicher Unternehmen zeigen, dass eine starke Beteiligung des Managements an der Informationssicherheit nicht nur die Widerstandsfähigkeit gegenüber Cyberbedrohungen stärkt, sondern auch das Vertrauen der Kunden und Partner festigt. Die Entscheidungen des C-Levels prägen die Sicherheitskultur des gesamten Unternehmens und tragen dazu bei, eine robuste Verteidigungslinie gegenüber den komplexen Bedrohungen der digitalen Ära aufzubauen. Im nächsten Abschnitt werden wir näher darauf eingehen, wie das C-Level aktiv zur Bewusstseinsbildung im Unternehmen beitragen kann.

## Bewusstseinsbildung im Unternehmen

Die Verantwortung des C-Levels in Bezug auf Informationssicherheit geht weit über die Festlegung von Richtlinien und die Freigabe von Ressourcen hinaus. Eine der entscheidenden Aufgaben ist die Förderung eines starken Sicherheitsbewusstseins in der gesamten Organisation. In einer Welt, in der Mitarbeiter oft die erste Verteidigungslinie gegen Cyberangriffe sind, ist es unerlässlich, dass jeder im Unternehmen die Bedeutung von Informationssicherheit versteht und aktiv dazu beiträgt.

Das C-Level muss eine führende Rolle bei der Initiierung von Schulungs- und Sensibilisierungsmaßnahmen übernehmen. Dies bedeutet nicht nur, Mitarbeiter über potenzielle Bedrohungen aufzuklären, sondern auch ein Bewusstsein für sicherheitsrelevante Praktiken im täglichen Arbeitsumfeld zu schaffen. Schulungen sollten nicht auf die IT-Abteilung beschränkt sein, sondern alle Abteilungen und Hierarchieebenen einbeziehen, um ein gemeinsames Verständnis und eine kohärente Sicherheitskultur zu etablieren.

Das C-Level kann durch klare Kommunikation und Vorbildfunktion einen bedeutenden Beitrag zur Bewusstseinsbildung leisten. Die Führungsebene sollte Sicherheitsrichtlinien nicht nur vorgeben, sondern sie selbst aktiv praktizieren. Dies trägt dazu bei, eine Atmosphäre des Vertrauens zu schaffen und zeigt den Mitarbeitern, dass Informationssicherheit eine Priorität auf höchster Ebene ist.

Zusätzlich zu Schulungen und Richtlinien sollte das C-Level einen offenen Dialog über Sicherheitsbedenken fördern. Mitarbeiter müssen sich sicher fühlen, Sicherheitsvorfälle zu melden, ohne negative Konsequenzen zu fürchten. Ein transparenter Austausch fördert eine Kultur der Zusammenarbeit und ermöglicht es dem Unternehmen, schnell auf neue Bedrohungen zu reagieren.

Im nächsten Abschnitt werden wir uns damit befassen, warum der Aufbau eines umfassenden Informationssicherheitsmanagementsystems (ISMS) unerlässlich ist und wie das C-Level in diesem Prozess eine entscheidende Rolle spielt.

## Aufbau eines Informationssicherheitsmanagementsystems (ISMS)

Die Bedrohungen im Bereich der Informationssicherheit erfordern mehr als nur punktuelle Maßnahmen. Ein umfassender Ansatz ist unabdingbar, um die Komplexität der heutigen digitalen Landschaft zu bewältigen. Hier kommt das Informationssicherheitsmanagementsystem (ISMS) ins Spiel, und das C-Level-Management spielt eine zentrale Rolle bei dessen Aufbau und Implementierung.

Das ISMS bildet das Rückgrat einer erfolgreichen Sicherheitsstrategie und bietet einen systematischen Rahmen für die Identifikation, Bewertung und Behandlung von Sicherheitsrisiken. International anerkannte Standards wie die ISO 27001 legen die Grundlagen für ein wirksames ISMS fest. Die Verantwortung des C-Levels besteht darin, sicherzustellen, dass das Unternehmen ein solches System einführt und konsequent aufrechterhält.

Der Prozess beginnt mit einer gründlichen Risikoanalyse, bei der potenzielle Bedrohungen und Schwachstellen identifiziert werden. Das C-Level muss sicherstellen, dass alle relevanten Abteilungen eingebunden sind und dass die Risikobewertung den geschäftlichen Kontext angemessen berücksichtigt. Basierend auf den Ergebnissen werden dann Sicherheitsrichtlinien und -maßnahmen entwickelt.

Die aktive Beteiligung des C-Levels ist entscheidend, um sicherzustellen, dass diese Richtlinien nicht nur auf dem Papier existieren, sondern auch in der Praxis umgesetzt werden. Die Allokation von Ressourcen für Schulungen, Technologien und regelmäßige Sicherheitsaudits liegt in der Verantwortung des Managements. Das C-Level muss sicherstellen, dass diese Ressourcen effektiv genutzt werden, um eine robuste Verteidigung gegen Cyberbedrohungen aufzubauen.

Ein weiterer wesentlicher Aspekt des ISMS ist die kontinuierliche Verbesserung. Das C-Level sollte sicherstellen, dass das Unternehmen auf Veränderungen in der Bedrohungslage und im technologischen Umfeld flexibel reagieren kann. Die Überprüfung und Aktualisierung des ISMS sollten regelmäßige Bestandteile der Unternehmenspraxis sein, um sicherzustellen, dass die Sicherheitsstrategie immer auf dem neuesten Stand ist.

Im nächsten Abschnitt werden wir genauer darauf eingehen, warum organisatorische Maßnahmen oft genauso wichtig sind wie technische Maßnahmen im Kampf gegen Cyberangriffe.

## Organisatorische Maßnahmen vs. Technische Maßnahmen

In der komplexen Welt der Informationssicherheit sind technische Maßnahmen allein oft nicht ausreichend, um Cyberbedrohungen abzuwehren. Die Organisationsstruktur und -kultur spielen eine entscheidende Rolle bei der Schaffung einer widerstandsfähigen Verteidigungslinie. Das C-Level-Management muss verstehen, warum organisatorische Maßnahmen genauso wichtig sind wie technische, wenn es darum geht, das Unternehmen vor Cyberangriffen zu schützen.

Organisatorische Maßnahmen beziehen sich auf die Entwicklung und Umsetzung von Sicherheitsrichtlinien, -verfahren und -prozessen. Hierzu zählen Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter, klare Richtlinien für den Umgang mit sensiblen Informationen und die Implementierung von Mechanismen zur Überwachung und Bewertung der Sicherheitsleistung.

Das C-Level spielt eine Schlüsselrolle bei der Festlegung dieser organisatorischen Maßnahmen. Es ist nicht nur für die Genehmigung von Richtlinien verantwortlich, sondern muss auch sicherstellen, dass diese im gesamten Unternehmen verstanden und befolgt werden. Durch klare Kommunikation und Schulungen trägt das C-Level dazu bei, eine Sicherheitskultur zu fördern, in der jeder Mitarbeiter ein aktiver Akteur im Schutz des Unternehmens wird.

Ein weiterer wichtiger Aspekt organisatorischer Maßnahmen ist das Risikomanagement. Das C-Level muss sicherstellen, dass das Unternehmen Risiken systematisch bewertet und Strategien zur Risikobehandlung entwickelt. Dies erfordert nicht nur ein Verständnis der technischen Aspekte von Sicherheit, sondern auch ein Bewusstsein für geschäftliche Risiken und Auswirkungen.

Im Gegensatz dazu konzentrieren sich technische Maßnahmen auf die Implementierung von Sicherheitstechnologien und -infrastrukturen. Während diese zweifellos wichtig sind, um Bedrohungen auf technischer Ebene abzuwehren, sollten sie nicht isoliert betrachtet werden. Das C-Level muss sicherstellen, dass technische Maßnahmen nahtlos in die organisatorischen Strukturen integriert sind und dass sie den geschäftlichen Anforderungen entsprechen.

Im nächsten Abschnitt werden wir genauer darauf eingehen, warum organisatorische Maßnahmen oft entscheidender sind als technische Maßnahmen im Kontext der Informationssicherheit.

## Die Kosten der Vernachlässigung von Informationssicherheit

Die Vernachlässigung von Informationssicherheit kann gravierende finanzielle Auswirkungen auf Unternehmen haben. Cyberangriffe und Datenverluste können nicht nur zu unmittelbaren finanziellen Verlusten führen, sondern auch zu langfristigen Schäden für die Reputation und das Vertrauen der Kunden. Das C-Level-Management muss verstehen, dass die Kosten der Vernachlässigung von Informationssicherheit weit über die unmittelbaren finanziellen Auswirkungen hinausgehen.

Direkte Kosten von Cyberangriffen umfassen oft die Wiederherstellung von Daten, die Behebung von Sicherheitslücken und die Implementierung neuer Sicherheitsmaßnahmen. Diese finanziellen Belastungen können jedoch vergleichsweise gering sein im Vergleich zu den indirekten Kosten. Hierzu zählen der Verlust von Kundenvertrauen, Reputationsrisiken, rechtliche Konsequenzen und regulatorische Strafen.

Der Ruf eines Unternehmens kann durch einen einzigen Cyberangriff erheblich geschädigt werden, und es kann Jahre dauern, bis das Vertrauen der Kunden wiederhergestellt ist. Kunden, die das Gefühl haben, dass ihre Daten nicht ausreichend geschützt sind, neigen dazu, zu Wettbewerbern abzuwandern, was langfristige finanzielle Verluste nach sich zieht. Das C-Level muss daher Informationssicherheit als einen wesentlichen Bestandteil des Markenwertes und der Kundenbeziehung betrachten.

Darüber hinaus sind Unternehmen in vielen Branchen gesetzlichen und regulatorischen Anforderungen unterworfen. Datenverstöße können zu erheblichen Geldstrafen führen, und das C-Level trägt maßgeblich zur Umsetzung von Datenschutzvorgaben bei, obwohl die Verantwortung bei der obersten Geschäftsführung verbleibt. Die Nichteinhaltung kann nicht nur drastische finanzielle Sanktionen, sondern auch rechtliche Konsequenzen für die Führungsebene selbst nach sich ziehen.

Investitionen in Informationssicherheit sollten daher nicht nur als Kosten, sondern als strategische Maßnahme betrachtet werden, um langfristige finanzielle und reputationsbezogene Risiken zu minimieren. Das C-Level spielt hierbei eine entscheidende Rolle, indem es sicherstellt, dass die notwendigen Ressourcen für Informationssicherheit bereitgestellt werden und dass diese Investitionen mit den geschäftlichen Zielen des Unternehmens in Einklang stehen.

Im nächsten Abschnitt werden wir näher darauf eingehen, warum es entscheidend ist, dass das C-Level Informationssicherheit nicht nur als technische Angelegenheit betrachtet, sondern als einen integralen Bestandteil der Unternehmensstrategie.

## Der schnelle Return on Investment (ROI) und die Unverzichtbarkeit eines ISMS

Die Investition in ein Informationssicherheitsmanagementsystem (ISMS) ist nicht nur eine präventive Maßnahme gegen potenzielle Bedrohungen, sondern auch ein Schlüssel für einen zeitnahen Return on Investment (ROI). Das C-Level-Management muss verstehen, dass die Implementierung eines ISMS nicht nur eine Kostenbelastung darstellt, sondern eine strategische Entscheidung ist, die sich schnell positiv auf die finanzielle Gesundheit und den langfristigen Erfolg des Unternehmens auswirkt.

Ein gut strukturiertes ISMS bietet unmittelbare Vorteile, darunter eine effizientere Ressourcennutzung, Reduzierung von Sicherheitsrisiken und die Möglichkeit, schneller auf sich ändernde Bedrohungen zu reagieren. Diese Faktoren tragen dazu bei, Betriebsunterbrechungen zu minimieren und die Gesamtleistung des Unternehmens zu optimieren.

Die Implementierung eines ISMS führt zu einer verbesserten Sicherheitslage, was wiederum das Vertrauen der Kunden stärkt. Kunden werden sich bewusster für Sicherheitsfragen sensibilisiert, und ein nachweisbares Engagement für den Schutz ihrer Daten wird zu einer stärkeren Kundenbindung führen. Der positive Einfluss auf den Kundenvertrauensfaktor manifestiert sich nicht nur in der Kundenbindung, sondern auch in einem potenziellen Zuwachs neuer Kunden, die Sicherheit als einen wesentlichen Faktor bei der Auswahl ihrer Geschäftspartner betrachten.

Des Weiteren ermöglicht ein gut durchdachtes ISMS dem Unternehmen, regulatorische Anforderungen effizient zu erfüllen. Die Vermeidung von Geldstrafen und rechtlichen Konsequenzen aufgrund von Nichteinhaltung stellt eine unmittelbare finanzielle Einsparung dar. Das C-Level muss erkennen, dass die Investition in Informationssicherheit nicht nur eine ethische Verpflichtung ist, sondern auch einen klaren wirtschaftlichen Nutzen bringt.

Zusammengefasst ist die Implementierung eines ISMS nicht nur eine sicherheitsbezogene Notwendigkeit, sondern ein strategisches Muss. Der schnelle ROI, die Stärkung der Kundenbeziehungen und die Erfüllung regulatorischer Anforderungen sind unmittelbare und messbare Vorteile, die das C-Level in die Pflicht nehmen, Informationssicherheit als integralen Bestandteil der Unternehmensstrategie zu etablieren.

Im abschließenden Abschnitt werden wir die Schlüsselpunkte zusammenfassen und einen Appell an das C-Level richten, um die Verantwortung für Informationssicherheit als strategischen Geschäftsvorteil zu erkennen und zu übernehmen.

## Fazit

Informationssicherheit ist nicht nur eine technische Herausforderung, sondern ein fundamentaler Bestandteil der Unternehmensstrategie. Das C-Level-Management trägt eine entscheidende Verantwortung, nicht nur in der Leitung des Unternehmens, sondern auch im Schutz seiner wertvollsten Ressource: **Informationen**.

Es ist unbestreitbar, dass die Bedrohungen durch Cyberangriffe zunehmen und dass die Vernachlässigung von Informationssicherheit erhebliche finanzielle und reputationsbezogene Risiken mit sich bringt. In diesem Kontext ist das C-Level aufgerufen, Informationssicherheit als strategischen Geschäftsvorteil zu betrachten und entsprechende Maßnahmen zu ergreifen.

Die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) ist dabei nicht nur eine präventive Maßnahme, sondern eine Investition mit einem schnellen Return on Investment. Ein gut strukturiertes ISMS verbessert nicht nur die Sicherheitslage, sondern stärkt auch das Kundenvertrauen, minimiert Betriebsunterbrechungen, verringert das finanzielle Risiko und ermöglicht die effiziente Erfüllung regulatorischer Anforderungen.

**Die Handlungsempfehlung an das C-Level lautet daher klar:** Übernehmen Sie die Verantwortung für Informationssicherheit als einen integralen Bestandteil der Unternehmensstrategie. Investieren Sie in den Aufbau eines umfassenden ISMS, fördern Sie eine Sicherheitskultur im gesamten Unternehmen und Setzen Sie klare Maßstäbe für Sicherheitsstandards. Nur durch ein proaktives Engagement auf höchster Ebene kann das Unternehmen nicht nur gegen aktuelle Bedrohungen gewappnet sein, sondern auch langfristig erfolgreich und widerstandsfähig bleiben.

Die digitale Ära erfordert eine neue Denkweise, in der Informationssicherheit nicht als lästige Pflicht, sondern als strategischer Wettbewerbsvorteil betrachtet wird. Das C-Level hat die Macht und Verantwortung, diesen Wandel voranzutreiben und die Sicherheit des Unternehmens in die Hände derer zu legen, die die Gesamtverantwortung tragen: Das Top-Management.

## Weitere Whitepaper

Weitere interessante Whitepaper zu dem Themen IT & Informations- sowie Cybersicherheit erhalten Sie im Downloadbereich unserer Internetseite.

https://mabs40.de.com/download/

Selbstverständlich können Sie uns auch unverbindlich telefonisch oder per E-Mail kontaktieren.

Gerne stehen wir Ihnen für ein erstes kostenloses Gespräch zu Verfügung.

# Disclaimer



mabs vertreibt keine Produkte und ist daher in Empfehlungen frei von eigenen oder fremden Verkaufsinteressen.