MOONROC

HOFFNUNG IST KEINE STRATEGIE –

Warum man Cyberrisiken ganzheitlich angehen muss!

www.moonroc.de

HOFFNUNG IST KEINE STRATEGIE –

Warum man Cyberrisiken ganzheitlich angehen muss!

AUTOREN

Patrick Natus
Luisa Küffner
Detlev Henze

www.moonroc.de

MOONROC
ADVISORY PARTNERS

MOONROC INSTITUTE OF
ECONOMIC RESEARCH

Inhalt

In der heutigen, immer stärker digitalisierten und vernetzten Wirtschaft stehen Unternehmen vor vielen Herausforderungen. Dabei entwickelt sich eine wachsende Bedrohung immer mehr zu einer wirklichen Gefahr für Organisationen: Cyberangriffe. Die Risiken dieser Bedrohung sind allgegenwärtig und betreffen Organisationen jeder Branche und Größe. Doch während die Angreifer immer professioneller werden, hinken viele Unternehmen mit ihren Schutzmaßnahmen hinterher. Vor diesem Hintergrund werden der im Januar 2025 in Kraft tretende Digital Operational Resilience Act (DORA) und die Verankerung von entsprechenden Schutzmechanismen in der Informationssicherheits-Governance (ISG) der Unternehmen zunehmend an Bedeutung gewinnen. In diesem Artikel zeigen wir auf, wie eine effektive ISG dazu beiträgt, ein Schutzschild gegen digitale Gefahren aufzubauen.

1. Cyberrisiken in der deutschen Wirtschaft: Die stetige Zunahme von Cyberattacken ist immer häufiger auf organisierte Kriminalität zurückzuführen

Die aktuelle Bitkom-Studie zum Wirtschaftsschutz 2024, die zum zehnten Mal in Zusammenarbeit mit dem Bundesamt für Verfassungsschutz erstellt wurde, stützt sich auf repräsentative Daten von über 1.000 deutschen Unternehmen aus verschiedenen Branchen. Das Ergebnis ist alarmierend. Im Untersuchungszeitraum zwischen Frühjahr 2023 und 2024 waren 81% der deutschen Unternehmen von schwerwiegenden Sicherheitsvorfällen betroffen.[(1)]
Diese reichten von Datendiebstahl und IT-Geräteverlusten bis hin zu Industriespionage und Sabotage. Die Angriffe kamen sowohl aus dem In- als auch aus dem Ausland. Besonders alarmierend: 70% der betroffenen Firmen konnten die Täter der organisierten Kriminalität zuordnen.[(2)]

Aber nicht nur, dass die Gefahr durch externe Attacken deutlich zugenommen hat, gleichzeitig ist das Wissen der eigenen Mitarbeiter bezüglich Cybersicherheit immer noch als sehr überschaubar einzustufen. Laut einer Umfrage zur Cybersicherheit unter 5.000 Beschäftigten in Deutschland bewerten 41% derjenigen, die sich selbst als Personen mit hoher IT-Sicherheitskompetenz einschätzen, das Risiko als sehr hoch, ein Opfer von Cyberkriminalität oder Datendiebstahl zu werden.[(3)] Etwa ein Drittel der befragten Grundgesamtheit zeigt Unsicherheiten im Umgang mit Phishing und Datendiebstahl, mobiler Datensicherheit sowie der Gefahr durch Ransomware. Diese Lücken machen Unternehmen anfällig für Angriffe, die durch menschliches Fehlverhalten begünstigt werden.[(4)]

(1) Bitkom Studie zum Thema Wirtschaftsschutz 2024, S. 3
(2) Bitkom Studie zum Thema Wirtschaftsschutz 2024, S. 8
(3) G DATA CyberDefense AG: „Cybersicherheit in Zahlen – Lernen. Wissen. Handeln“, 2024, S. 8
(4) G DATA CyberDefense AG: „Cybersicherheit in Zahlen – Lernen. Wissen. Handeln“, 2024, S. 13

Der dadurch entstandene wirtschaftliche Schaden für Unternehmen in Deutschland ist beispiellos. Insgesamt wurden in dem oben genannten Zeitraum Schäden in Höhe von 266,6 Milliarden Euro verzeichnet.
Cyberattacken erwiesen sich dabei als besonders verheerend und verursachten mehr als zwei Drittel der gesamten Schäden – konkret 178,6 Milliarden Euro, was einem Anstieg von 30 Milliarden Euro im Vergleich zum entsprechenden Vorjahreszeitraum entspricht (siehe Abbildung 1).

Das restliche Drittel bezieht sich auf IT-Geräteverluste, Industriespionage & Sabotage.[5]
Besonders häufig nannten Unternehmen als Ursachen für diese Schäden Ransomware (31%), Phishing-Attacken (26%), Angriffe auf Passwörter (24%) und die Infizierung mit Schadsoftware (21%).[6]

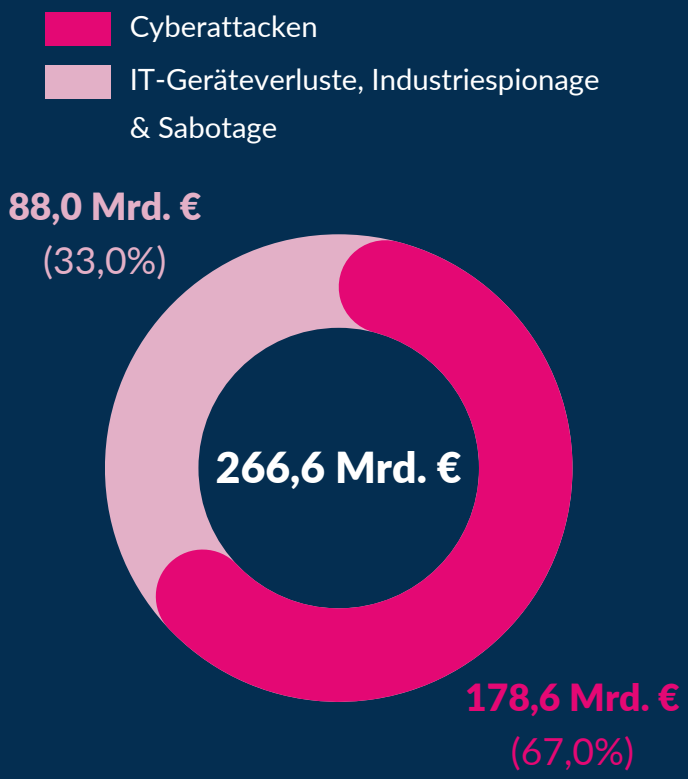

Abbildung 1: Schaden verursacht durch Cyberattacken in Deutschland zwischen Frühjahr 2023 und 2024

Die Herausforderung durch Cyberattacken wird in Zukunft voraussichtlich noch weiter zunehmen:

54% der Führungskräfte deutscher Unternehmen schätzen, dass das Risiko von Cyberangriffen und Datenklau in den kommenden Jahren stark steigen wird. Zum Vergleich: 2011 waren es lediglich 5%, die diese Einschätzung teilten – ein Anstieg um mehr als das Zehnfache, der die wachsende Dringlichkeit des Problems eindrucksvoll widerspiegelt.[7]

Trotz oder gerade wegen dieses Bewusstseins fühlen sich 65% der durch Bitkom befragten Unternehmen durch Cyberangriffe in ihrer Existenz bedroht (siehe Abbildung 2). Es sind aber lediglich 53% aller befragten Unternehmen der Ansicht, dass sie ausreichend auf solche Angriffe vorbereitet sind.[8]

Diese Diskrepanz verdeutlicht eine massive Verschärfung der Bedrohungslage für die deutsche Wirtschaft und unterstreicht die dringende Notwendigkeit, Schutzmaßnahmen weiter zu intensivieren.

(5) Bitkom Studie zum Thema Wirtschaftsschutz 2024, S. 13
(6) Bitkom Studie zum Thema Wirtschaftsschutz 2024, S. 15
(7) G DATA CyberDefense AG: „Cybersicherheit in Zahlen – Lernen. Wissen. Handeln“, 2024, S. 68
(8) Bitkom Studie zum Thema Wirtschaftsschutz 2024, S. 14

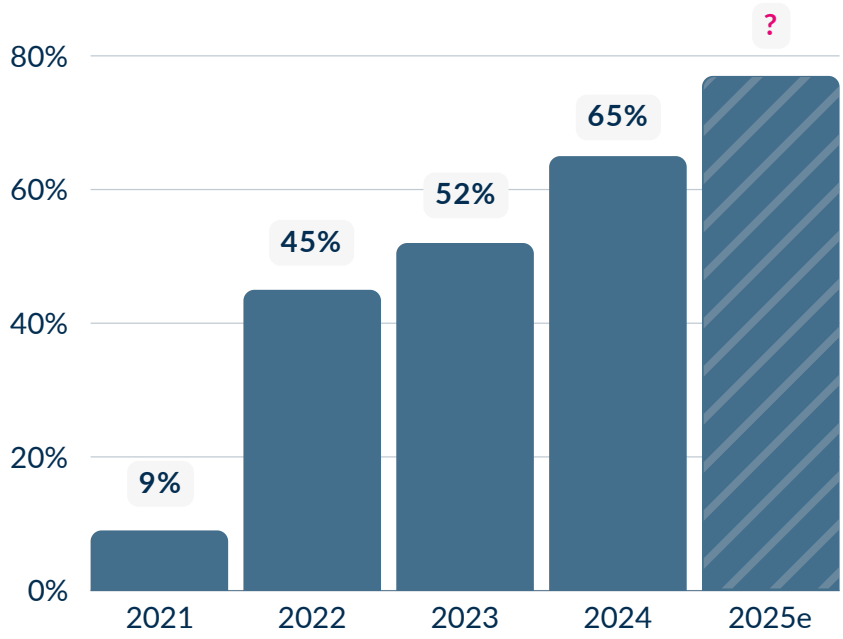

Abbildung 2: Anteil der Unternehmen, die sich durch potenzielle Cyberangriffe bedroht fühlen

Detlev Henze, Experte für den Bereich Informationssicherheit, schätzt die aktuelle Bedrohungslage für deutsche Unternehmen in Bezug auf Cyberangriffe wir folgt ein:

> *Die Bedrohungslage für deutsche Unternehmen durch Cyberangriffe nimmt stetig zu, da Cyberkriminelle immer professioneller werden und staatlich unterstützte Angreifer zunehmend gezielte und komplexe Attacken durchführen. Trotz dieser wachsenden Gefahr sind die Abwehrmaßnahmen vieler Unternehmen unzureichend: IT-Sicherheitsbudgets sind oft zu gering, es fehlt an spezialisierter Expertise und Sicherheitslücken bleiben aufgrund veralteter Systeme und fehlender Schulungen der Mitarbeiter bestehen. Diese Diskrepanz zwischen der ständig steigenden Bedrohung und den unzureichenden Sicherheitsvorkehrungen führt dazu, dass Unternehmen immer anfälliger für beliebige und insbesondere schwere Angriffe werden, was sowohl finanzielle Verluste als auch langfristige Reputationsschäden zur Folge hat.*
>
> **Detlev Henze**
> Gründer und ehem. Geschäftsführer der TÜV TRUST IT GmbH

2. Regularien zur Cybersicherheit: Ein starker Rahmen für eine effektivere Abwehr!

Die wachsende Bedrohung durch Cyberangriffe und daraus resultierende Informationssicherheitsvorfälle haben nicht nur Unternehmen und Organisationen vor erhebliche Herausforderungen gestellt, sondern auch den Druck auf Regierungen und Aufsichtsbehörden weltweit erhöht, effektivere Schutzmaßnahmen und gesetzliche Rahmenbedingungen zu schaffen. Diese sind notwendig, da viele Unternehmen ohne klare gesetzliche Anforderungen und Vorgaben die erforderlichen Maßnahmen zur Cybersicherheit nicht konsequent umsetzen. Die Regulierungen zielen daher nicht nur auf den Schutz der Wirtschaft und der betroffenen Organisationen ab, sondern auch auf die Gewährleistung der nationalen Sicherheit und den Schutz der individuellen Rechte und Interessen, also dem Schutz der Gesellschaft und des Individuums. Um der zunehmenden Komplexität und den weitreichenden Folgen von Cyberrisiken gerecht zu werden, wurden in den vergangenen Jahren verschiedene regulatorische Anforderungen an die Wirtschaft entwickelt.

Die drei bekanntesten sind die Network and Information Security Directive (EU) 2022/2555 (NIS2-Richtlinie), der Digital Operational Resilience Act (DORA) und der Cyber Resilience Act (CRA), welche wir nachfolgend kurz gegenüberstellen.

Übersicht der wesentlichen regulatorischen Anforderungen zur Cybersicherheit

	NIS2	DORA	CRA
Gültig seit / ab	17.10.2024	17.01.2025	2027
Geltungsbereich	Kritische Sektoren in der EU (wichtige und wesentliche Einrichtungen) Firmen mit ≥ 50 MA[9] und 10 Mio. € Jahresumsatz in 18 Sektoren	Finanzunternehmen & IKT[10]-Drittdienstleister in der EU Alle Finanzunternehmen, jedoch sind Vorgaben von Größe abhängig	Akteure im Bereich digitaler Produkte in der EU Alle Hersteller, Händler & Importeure von Produkten mit digitalen Elementen
Ziel	Erhöhung der Cyber-sicherheitsstandards & Stärkung der Zusammen-arbeit innerhalb der EU	Sicherstellung der digitalen Widerstandsfähigkeit im Finanzsektor	Erhöhung der Cyber-sicherheit von Produkten mit digitalen Komponenten in der gesamten EU
Fokusbereiche	› Cybersicherheits-anforderungen › Management von Cyberrisiken › Meldepflicht für Sicherheitsvorfälle › Nationale und EU-weite Zusammenarbeit	› Cybersicherheits-anforderungen › Risikomanagement › Berichterstattung über Vorfälle › IKT-Risiken › Schutz vor Drittanbieter	› Sicherheits-anforderungen für Hardware & Software › Pflichten für Hersteller › Überwachung der Lebenszyklus-Sicherheit › Verantwortlichkeiten für Sicherheitsvorfälle
Sanktionen / Bußgelder	7-10 Mio. € oder 1,4-2% des weltweiten Vorjahresumsatzes	≤ 10 Mio. € oder 5% des weltweiten Vorjahresumsatzes	≤ 15 Mio. € oder ≤ 2,5% des weltweiten Vorjahresumsatzes

Abbildung 3: Gegenüberstellung NIS2, DORA, CRA

Obwohl NIS2, DORA und CRA alle einen wichtigen Beitrag zur Cybersicherheit und Resilienz in den unterschiedlichen Sektoren leisten, fokussiert sich dieser Artikel auf DORA. Dabei liegt der Schwerpunkt insbesondere auf der Bedeutung von DORA für den Finanzsektor, da dieser aufgrund seiner systemrelevanten Rolle und der hohen Abhängigkeit von digitalen Infrastrukturen besonders anfällig für Cyberbedrohungen ist. Ab dem 17. Januar 2025 müssen Finanz-unternehmen und ihre Informations- und Kommunikationstechnologie (IKT)-Drittdienst-leister strikte Sicherheitsvorgaben einhalten, um den steigenden Bedrohungen im Bereich der IKT gerecht zu werden.

(9) Mitarbeiter
(10) Informations- und Kommunikationstechnologie

Die Verordnung wurde erlassen, um Lücken in der bestehenden Regulierung des Finanzsektors zu schließen, die zuvor nur fragmentarische Vorgaben für die operationelle Resilienz und den Umgang mit IKT-Risiken enthielt. DORA bietet erstmals einen einheitlichen Rahmen, der sicherstellt, dass Finanzunternehmen in der gesamten EU hohe Sicherheitsstandards einhalten und somit resilienter gegen digitale Bedrohungen werden.

Zu den zentralen Anforderungen, die DORA an Finanzunternehmen stellt, gehören:

1. **IKT-Risikomanagement:**
   Finanzinstitute sind verpflichtet, einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen zu etablieren. Dieser Rahmen muss aus klar definierten Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokollen und -Tools bestehen. Ziel ist es, Risiken und Schwachstellen in digitalen Prozessen systematisch zu identifizieren, zu bewerten und durch entsprechende Maßnahmen zu minimieren.

2. **Berichterstattung über IKT-Vorfälle:**
   Finanzunternehmen sind verpflichtet, einen klaren Prozess zur Erkennung, Behandlung und Meldung von IKT-bezogenen Vorfällen einzurichten. Dabei muss die Meldung schwerwiegender Vorfälle unverzüglich an eine zentrale Behörde erfolgen, die von jedem Mitgliedstaat als nationale Meldestelle benannt wird.

3. **Prüfung der digitalen Betriebsstabilität:**
   Finanzunternehmen müssen ein umfassendes Programm zur Sicherstellung der digitalen Resilienz entwickeln, implementieren und regelmäßig überprüfen. Dieses Programm umfasst die Vorbereitung auf den Umgang mit IKT-bezogenen Vorfällen und die Durchführung verschiedener Tests zur Überprüfung der digitalen Widerstandsfähigkeit. Dabei ist sicherzustellen, dass die Tests von unabhängigen internen oder externen Parteien durchgeführt werden. Dies dient der praxisnahen Vorbereitung auf den Ernstfall.

4. **Steuerung und Überwachung von Risiken durch IKT-Drittanbieter:**
   Finanzunternehmen müssen eine Strategie für das Risiko von Drittanbietern entwickeln, die klare Leitlinien für die Nutzung von IKT-Dienstleistungen enthält, insbesondere für solche, die kritische oder wichtige Funktionen unterstützen. Für die Überprüfung ist ein Informationsregister mit allen vertraglichen Vereinbarungen zu führen.

5. **Förderung des Informationsaustauschs:**
   Finanzunternehmen sollen relevante Sicherheitsinformationen untereinander austauschen, um von den Erfahrungen anderer zu profitieren und gemeinsame Bedrohungen effizienter abzuwehren. Hierbei kann ein zeitnaher Informationsaustausch mit den Behörden und weiteren Unternehmen für diese essenziell sein.

3. Verankerung von DORA in der Informationssicherheits-Governance (ISG): Der Schlüssel zur Stärkung der Cyber-Resilienz

DORA sollte nicht nur als eine gesetzliche Vorgabe gesehen werden, sondern muss als zentrales Element in der ISG eines Unternehmens verankert werden. Die ISG bildet einen zentralen Bestandteil der Unternehmensführung und dient der Absicherung von Informationen innerhalb eines Unternehmens. Sie stellt sicher, dass Sicherheitsstrategien, -richtlinien und -prozesse im Einklang mit den unternehmerischen Zielen und Anforderungen stehen. Als Teil der übergreifenden Corporate Governance hat die ISG das Ziel, ein einheitliches Schutzniveau für alle Unternehmensbereiche zu gewährleisten und den IT-Bereich so auszurichten, dass er den geschäftlichen Bedürfnissen gerecht wird.

Als Leitlinie unterstützt DORA die ISG, die organisatorischen und technischen Maßnahmen zu definieren, die notwendig sind, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen. Die ISG legt den Rahmen fest, um Risiken zu minimieren und die Sicherheitsstrategien entsprechend den geschäftlichen Anforderungen zu gestalten. Genau hier stellt DORA durch ihre Abbildung sicher, dass Unternehmen nicht nur finanzregulatorische Anforderungen erfüllen, sondern auch resilient gegenüber digitalen Bedrohungen sind. DORA hilft, klare Richtlinien und Standards zu implementieren, die es ermöglichen, Informations-Assets effektiv zu schützen und gleichzeitig den regulatorischen Vorgaben gerecht zu werden.

Aktuelle Umfragen zeigen, dass in vielen Unternehmen ein signifikantes Bewusstsein für IT-Sicherheit besteht, jedoch häufig das Engagement und Verständnis für die Thematik fehlen. So glauben 34% der IT-Sicherheitsverantwortlichen, dass das Thema IT-Sicherheit erst dann an Bedeutung gewinnt, wenn bereits Probleme aufgetreten sind.[(11)] Zudem stimmen 65% von 500 befragten Unternehmen in Deutschland zu, dass Normen und Standards den Schutz vor Cyberangriffen kontinuierlich verbessern. Jedoch empfinden 56% die Einhaltung dieser Standards als mit zu viel Aufwand verbunden. Außerdem haben 48% Schwierigkeiten, relevante Normen und Standards zu identifizieren, und 40% empfinden diese als zu technisch und schwer verständlich.[(12)] Diese Daten unterstreichen die Notwendigkeit einer robusten ISG.

Durch die Abbildung der DORA Vorgaben in der ISG wird ein notwendiges Rahmenwerk geschaffen, das Leitplanken setzt und alle Mitarbeiter aktiv einbindet. Dies fördert ein gemeinsames Bewusstsein für die IT-Sicherheit, um den Herausforderungen der Cybersecurity erfolgreich zu begegnen. So können Unternehmen sicherstellen, dass alle Mitarbeiter die Relevanz von Informationssicherheit erkennen und mittragen.

(11) G DATA CyberDefense AG: „Cybersicherheit in Zahlen – Lernen. Wissen. Handeln“, 2024, S. 18
(12) G DATA CyberDefense AG: „Cybersicherheit in Zahlen – Lernen. Wissen. Handeln“, 2024, S. 73

> *Eine ISG ist entscheidend, weil sie Cybersicherheit als strategisches Ziel in alle Unternehmensebenen integriert, klare Verantwortlichkeiten schafft und fundierte Risikobewertungen ermöglicht. Durch diese strukturierte Herangehensweise wird die Reaktionsfähigkeit auf Bedrohungen verbessert, die langfristige Resilienz des Unternehmens gestärkt und die Einhaltung von Regularien wie DORA sichergestellt.*
>
> **Detlev Henze**
> Gründer und ehem. Geschäftsführer der TÜV TRUST IT GmbH

4. Informationssicherheits-Governance (ISG): Eine klare Struktur als Erfolgsfaktor zur Stärkung der Unternehmensresilienz

Eine solide ISG ist die Basis für die effektive Umsetzung von Informations- und Cybersicherheitsmaßnahmen sowie die Sicherstellung eines langfristig verlässlichen Sicherheitsniveaus. Als Rahmenwerk setzt die ISG klare Leitlinien für die strategische Ausrichtung und die operative Umsetzung von Cybersicherheitsmaßnahmen. Sie stellt sicher, dass alle Maßnahmen zur Informationssicherheit in Übereinstimmung mit den Unternehmenszielen und regulatorischen Vorgaben, wie dem Digital Operational Resilience Act (DORA), erfolgen. Weiterhin gewährleistet sie eine abgestimmte Zusammenarbeit aller Beteiligten, die Cybersicherheit als gemeinsames Ziel verfolgen, um die Widerstandsfähigkeit des Unternehmens gegenüber digitalen Bedrohungen nachhaltig zu stärken.

Ein klar definiertes Funktionsmodell für ISG und IS-Management kann als Orientierung dienen, um die notwendigen Themen im Unternehmen effektiv zu adressieren. Aus diesem generischen Modell kann ein individuelles, auf das Unternehmen zugeschnittenes ISG-Modell entwickelt werden.

Aufbau eines individuell zugeschnittenen ISG-Modells

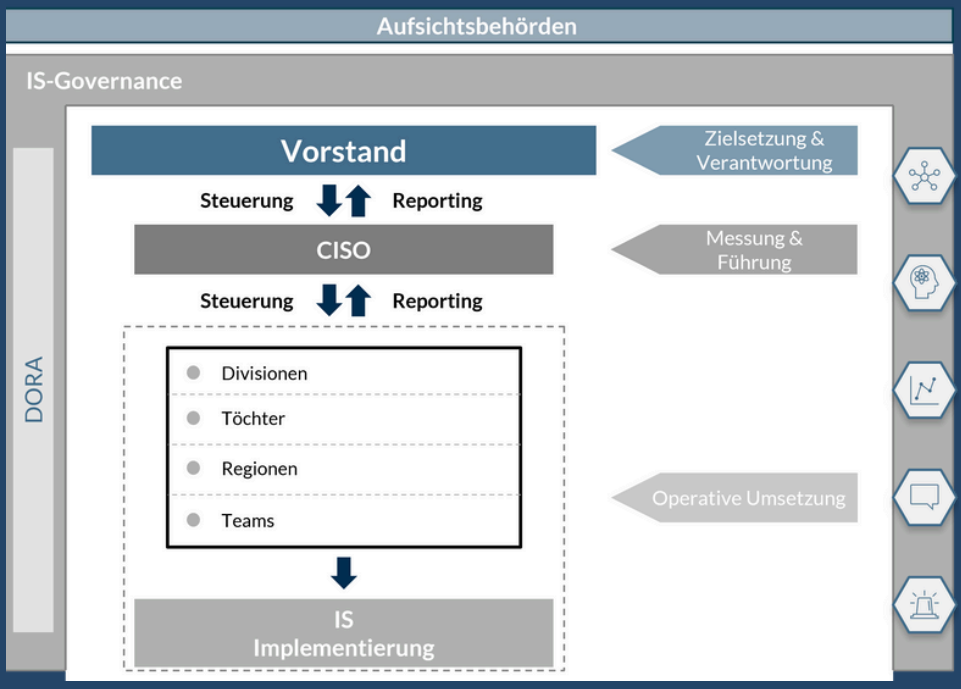

Abbildung 4: MOONROC ISG-Modell

Das in Abb. 4 dargestellte ISG-Modell beschreibt die Verantwortlichkeiten und Steuerungsmechanismen und umfasst alle wesentlichen Governance-Funktionen. An oberster Stelle stehen die Aufsichtsbehörden, die die gesetzlichen und regulatorischen Anforderungen erlassen und deren Erfüllung kontrollieren. Sie üben eine übergeordnete Kontrollfunktion aus und überprüfen, ob die Organisation stets im Einklang mit den geltenden Vorschriften arbeitet. Der Vorstand, der die zentrale Verantwortung für die ISG trägt, legt strategische Ziele fest und steuert auf dieser Basis in Kooperation mit dem CISO die informationssicherheitsspezifischen Maßnahmen. Der CISO fungiert als Schnittstelle zwischen dem Vorstand und den Bereichen, in denen die operative Umsetzung der Informationssicherheitsmaßen stattfindet.

Dabei erfolgen ein regelmäßiges Reporting an den Vorstand und eine intensive Diskussion darüber, ob die durchgeführten Maßnahmen mit den festgelegten Zielen übereinstimmen. Dies gilt insbesondere in Bezug auf sich verändernde Vorschriften, bei denen die ISG sicherstellen muss, dass Erweiterungen und Anpassungen integriert und mögliche Widersprüche transparent gemacht und aufgelöst werden. Operative Einheiten wie Divisionen, Tochtergesellschaften, Regionen und Teams sind für die praktische Umsetzung der Maßnahmen verantwortlich.

Insgesamt verdeutlicht das Modell die klare Struktur von Informationswegen und Verantwortlichkeiten, die von den Aufsichtsbehörden über den Vorstand und den CISO bis hin zu den operativen Einheiten reichen.

In der folgenden Abbildung werden die fünf wesentlichen inhaltlichen Bausteine einer ISG veranschaulicht.

Relevante Bausteine einer ISG

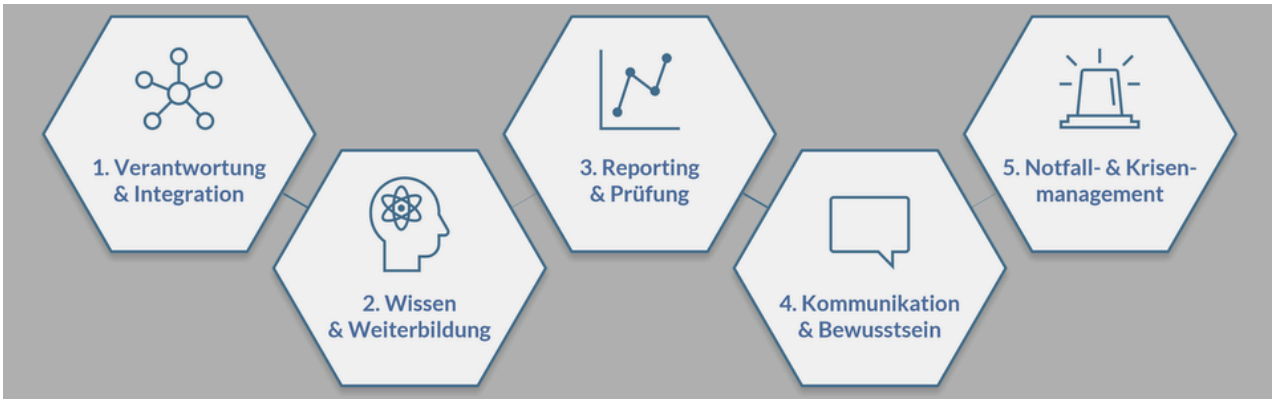

Abbildung 5: Fünf relevante Bausteine einer ISG

1. Verantwortung und Integration

Die oberste Unternehmensführung trägt die letztendliche Verantwortung für Informations- und Cybersicherheit, die nun fest in die Unternehmensstrategie integriert werden muss.[13] Darüber hinaus wird mit der Einführung von DORA die persönliche Haftung der Vorstandsmitglieder erheblich ausgeweitet. Vorstände können nun für grobe Fahrlässigkeit oder vorsätzliche Verstöße gegen die Vorgaben der Verordnung haftbar gemacht werden.[14] Daher ist es essenziell, Strukturen zu schaffen, die sicherstellen, dass das Unternehmen handlungsfähig bleibt und seinen regulatorischen Pflichten nachkommt. Dies beinhaltet insbesondere die Bereitstellung ausreichender Ressourcen, um den regulatorischen und selbst gesetzten Kontrollmaßnahmen gerecht zu werden. Der Vorstand muss die regulatorischen Vorgaben genau kennen und verstehen; eine bloße Delegation der Aufgaben reicht nicht aus. Informations- und Cybersicherheit müssen regelmäßig auf der Agenda der Vorstandssitzungen stehen, eine kontinuierliche Auseinandersetzung mit den Themen ist zu gewährleisten und schnelle, fundierte Reaktionen auf neue Bedrohungen sind zu ermöglichen.

2. Wissen und Weiterbildung

Die Unternehmensführung ist verpflichtet, fundierte Kenntnisse im Bereich der Informationssicherheit und Cybersicherheit zu erwerben, regelmäßig zu aktualisieren und diesen Wissenserwerb nachzuweisen.[15]

(13) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates, Artikel 5
(14) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates, Artikel 50
(15) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates, Artikel 13

Dies kann durch zielgerichtete, auf die spezifischen Anforderungen der Führungsebene abgestimmte Schulungen gewährleistet werden. Ergänzend dazu sollten regelmäßige Sitzungen des Vorstands stattfinden, bei denen interne sowie externe Experten über die aktuelle Sicherheitslage und neuesten Entwicklungen berichten. Der Austausch zwischen den Fachleuten und der Führungsebene ermöglicht es, aufkommende Risiken frühzeitig zu erkennen und entsprechende Maßnahmen zu diskutieren. Ein stets aktuelles Lagebild ist hierbei ein wertvolles Instrument zur Entscheidungsfindung.

3. Reporting und Prüfung

DORA legt einen besonderen Fokus auf eine starke ISG-Struktur, die sicherstellt, dass alle IKT-bezogenen Prozesse im Unternehmen klar definiert und effektiv überwacht werden.[16] Daher ist ein effektives Reporting-System unverzichtbar, um den aktuellen Status der Informationssicherheit transparent darzustellen. Es muss sowohl technische und prozessuale als auch strategische Aspekte umfassen und die Entscheidungsgrundlage für das Management bieten. Dashboards, die abgestimmte relevante KPIs[17] und OKRs[18] zur Cybersicherheit visualisieren, sind hierbei eine wertvolle Unterstützung. Hinzu kommen regelmäßige Status- und Standortbestimmungen durch interne und externe Audits, priorisierte Penetrationstests und Schwachstellenanalysen. Diese sind notwendig, um Sicherheitsmaßnahmen zu überwachen, den Reifegrad zu ermitteln und diesen kontinuierlich zielgerichtet zu verbessern. Die Ergebnisse dieser Prüfungen müssen im Reporting aufbereitet werden, um Fortschritte sowie identifizierte Risiken darzustellen.

4. Kommunikation und Bewusstsein

Eine effektive Cybersicherheitsstrategie erfordert eine klare und transparente Kommunikation innerhalb des Unternehmens. Cybersicherheit muss als unternehmerische Priorität verstanden werden, die fest in der Unternehmensstrategie verankert ist und nicht lediglich als technische Herausforderung. Ein strukturiertes Kommunikationsmodell sollte sicherstellen, dass alle Mitarbeiter – unabhängig von ihrer Position oder Abteilung – rechtzeitig und verständlich über sie betreffende Sicherheitsinformationen informiert werden. Die Mitarbeiter müssen verstehen, dass sie Teil der Sicherheitskultur, der Sicherheitshygiene sind und ihren Beitrag liefern müssen. Dabei ist es wichtig, dass der Wissensstand der Mitarbeiter regelmäßig überprüft und aktualisiert wird. Die Kommunikation und Wissensvermittlung müssen dabei zielgruppengerecht erfolgen, sodass Mitarbeiter auf allen Ebenen über die erforderlichen Kenntnisse verfügen, um verantwortungsvoll mit der Informationssicherheit umzugehen. Dieses Verständnis und die Eigenverantwortung muss durch regelmäßige Schulungen, Workshops und Informationskampagnen fester Bestandteil der Unternehmenssicherheitsstrategie sein.

---

(16) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates, Artikel 5
(17) Key-Performance-Indicators
(18) Objectives and Key Results

MOONROC Mehr-Ebenen-Kommunikationsmodell

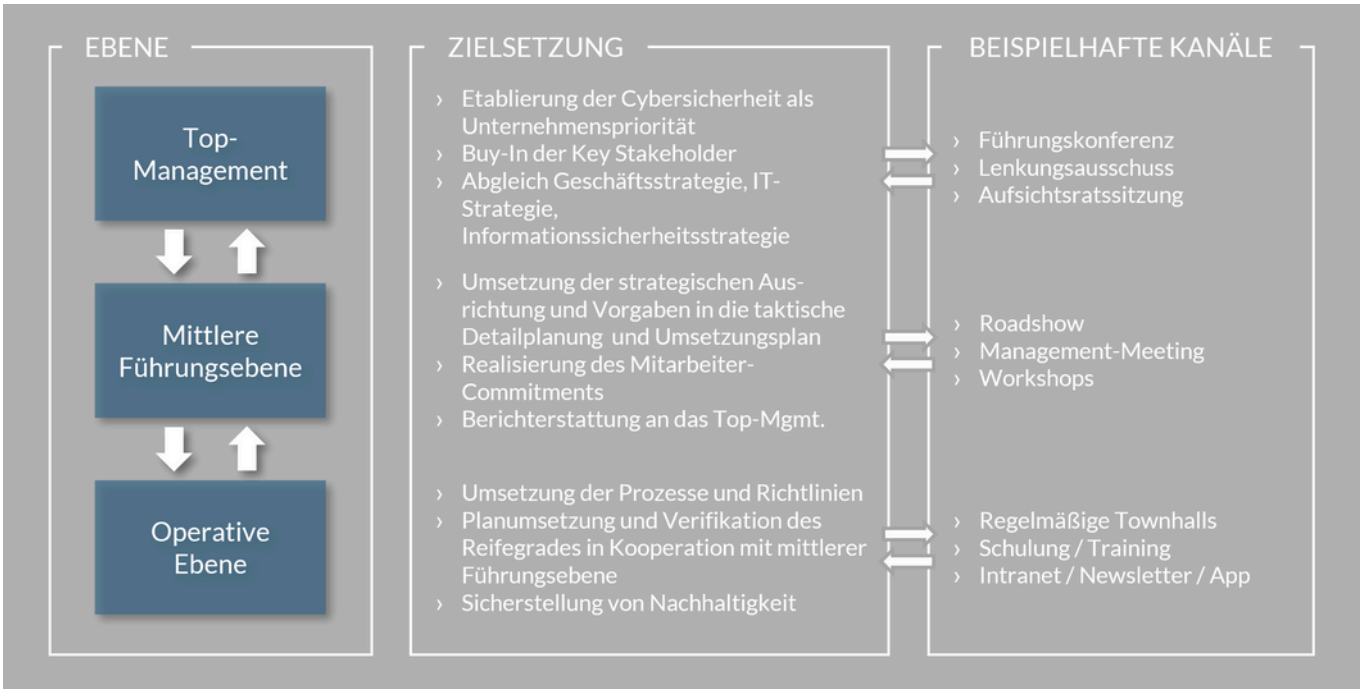

Abbildung 6: Zielsetzung und beispielhafte Kanäle innerhalb einer Mehr-Ebenen-Kommunikation

Ziel ist, dass diese Maßnahmen dazu beitragen, ein unternehmensweites Bewusstsein für die Risiken und Herausforderungen im Bereich der Cybersicherheit zu schaffen und die Sicherheitskultur nachhaltig zu stärken.

5. Notfall- und Krisenmanagement

Ein wesentlicher Bestandteil ist die Erstellung, laufende Aktualisierung und Kommunikation von Notfallplänen sowie die regelmäßige Durchführung von Notfallübungen. Diese proaktiven Vorbereitungen ermöglichen es, im Fall eines Sicherheitsvorfalls, der sich zu einem schwerwiegenden Ereignis entwickeln kann, schnell und effektiv zu reagieren.

Sollte sich der Vorfall zu einer Krise ausweiten, ist es von entscheidender Bedeutung, dass klare Strukturen und Prozesse vorhanden sind, um die Situation zu bewältigen. Die Übersicht und Handlungssicherheit müssen zu jeder Zeit gewährleistet sein. Dies erfordert klare Regelungen, die festlegen, wie der zuständige Krisenstab zusammengesetzt ist, wann und wer ihn einsetzt, wann und von wem er informiert wird und welche Entscheidungswege einzuhalten sind. Weiterhin müssen „Cybersecurity-Krisenstabsübungen“ unter Einbeziehung der Unternehmensführung regelmäßig durchgeführt werden, um die Handlungsfähigkeit für den Krisenfall sicherzustellen. Diese Übungen helfen, die Entscheidungsprozesse zu erproben und Schwachstellen in der Krisenreaktion frühzeitig zu identifizieren und zu beheben.

Durch die Etablierung einer umfassenden und wirksamen ISG wird die Grundlage geschaffen, ein auf die spezifischen Bedürfnisse des Unternehmens abgestimmtes, angemessenes Sicherheitsniveau sicherzustellen. Dieses Vorgehen bietet nicht nur Schutz vor digitalen Bedrohungen, sondern schafft auch Handlungssicherheit auf allen Ebenen – besonders im Falle des Auftretens eines Sicherheitsvorfalls.

Eine solide ISG sorgt für klare Zuständigkeiten und festgelegte Prozesse. Nur dies ermöglicht eine schnelle und effiziente Reaktion. Im Extremfall geht es um das Überleben der Geschäftsaktivitäten oder des Unternehmens. Hier werden zudem weitere Prozesse angebunden, z.B. BCP[19] und DRP.[20] Darüber hinaus gewährleistet sie, dass das Unternehmen proaktiv, also bereits in der Planungs-/ Strategiephase, auf neue regulatorische Anforderungen reagiert. Sie gewährleistet, dass Transparenz und Flexibilität in der Einhaltung und Anpassung an sich verschärfende Vorschriften geschaffen werden. Potenzielle Konflikte zwischen unterschiedlichen Regularien werden durch die ISG frühzeitig erkannt und adressiert.

Zudem stellt eine starke Governance sicher, dass bestehende Defizite im angestrebten Sicherheitsniveau und -reifegrad frühzeitig identifiziert und geschlossen werden können, sowohl in der Tiefe als auch in der Breite der Sicherheitsstrategie. Somit wird ein holistischer Schutz des Unternehmens vor digitalen Bedrohungen adressiert und gleichzeitig ein wirtschaftlich sinnvolles und langfristig tragfähiges Sicherheitskonzept etabliert, welches einen faktenbasierten Risikoappetit und die Ressourcenverfügbarkeit transparent darstellt

Detlev Henze
Gründer und ehem. Geschäftsführer der TÜV TRUST IT GmbH

(19) Business-Continuity-Plan
(20) Disaster Recovery Plan

5. Informationssicherheits-Governance (ISG): Was ist konkret zu tun?

Im Rahmen unserer Analyse haben wir die aktuelle Gefahrenlage durch Cyberangriffe sowie die relevanten regulatorischen Vorgaben und deren Bedeutung für Vorstände und Unternehmen eingehend betrachtet. Hieran schließt sich nun die Frage an, wie Unternehmen diesen neuen Rahmenbedingungen begegnen sollten und was konkret zu tun ist.

> *Viele Unternehmen haben bereits solide Sicherheitsstrukturen etabliert, doch die ständige Weiterentwicklung der Bedrohungslage und die Komplexität der Regulierungen erfordern kontinuierliche Anpassungen und Optimierungen. Die Unternehmensleitung muss immer wieder drei grundsätzliche Fragen stellen:*
>
> 1. *Reifegrad – Wo stehen wir bzgl. unserer Sicherheit?*
> 2. *Risikoappetit und -akzeptanz – Was ist unsere Zielsetzung?*
> 3. *Sicherheitsstrategie und Transparenz – Wie erreichen wir dieses Ziel?*
>
> *Zur Beantwortung dieser Fragen ist es hilfreich, eine neutrale Außenperspektive hinzuzuziehen, die eine potenzielle Betriebsblindheit vermeidet. Nur aus einer Innensicht heraus wird man keine objektiven Antworten entwickeln können und sich gefährlicherweise subjektiv sicher „fühlen". Das ist wie „Hoffnung" und „Sicherheit" in einem Satz zu erwähnen.*
>
> **Detlev Henze**
> Gründer und ehem. Geschäftsführer der TÜV TRUST IT GmbH

In Anbetracht dieser Überlegungen empfehlen wir ein dreistufiges Vorgehensmodell, welches das Top-Management dabei unterstützt, den Anforderungen von DORA gerecht zu werden und die ISG zu stärken.

Dreistufiges Vorgehensmodell zur Stärkung der ISG

Abbildung 7: Drei Schritte zu einer effektiven und robusten ISG

IDer erste Schritt zielt darauf ab, eine umfassende Übersicht über die aktuelle ISG zu gewinnen. Diese Übersicht wird mit einem **Quick Assessment** des Informationssicherheits-Managements erreicht, welches auf den zuvor definierten fünf Elementen einer ISG basiert (siehe Abbildung 7). In einer ersten Bestandsaufnahme werden die bestehenden Sicherheitsmaßnahmen und die Sicherheitskultur innerhalb des Unternehmens analysiert. Dadurch werden gezielt Stärken, Schwächen und potenzielle Lücken in der Compliance zu DORA identifiziert. Der Fokus dieses Quick Assessments liegt auf der Ebene des Top-Managements und der Sicherstellung der Verantwortungsübernahme bzw. der Transparenz der persönlichen und unternehmerischen Konsequenzen im Falle des Ereigniseintritts. Operative Einheiten stehen dabei nicht im Vordergrund; stattdessen werden strukturelle und strategische Vorstandsthemen adressiert, um eine effektive und nachhaltige Sicherheitsstrategie zu gewährleisten.

Auf Basis dieser Analyse wird gemeinsam der **Soll-Zustand** der ISG definiert. Hierbei werden spezifische Ziele und Maßnahmen entwickelt, die exakt auf die DORA-Vorgaben abgestimmt sind. Durch den Einsatz individueller KPIs, OKRs und Metriken wird es dem Top-Management ermöglicht, den Fortschritt in der Informationssicherheit messbar zu machen und somit eine fundierte und faktenbasierte Entscheidungsbasis für das weitere Vorgehen zu schaffen. Darüber hinaus wird sichergestellt, dass alle relevanten gesetzlichen und regulatorischen Anforderungen und die damit verbundenen Implikationen transparent vorliegen. Dies gibt dem Top-Management die Möglichkeit, sicher und risikoarm zu agieren. Gleichzeitig werden Haftungsrisiken minimiert und der Reifegrad der ISG systematisch verbessert. Dadurch wird das Management in seiner Verantwortung sowohl gestärkt als auch gleichzeitig geschützt. Es handelt nachweislich faktenbasiert, risikoorientiert und risikomitigierend.

Im letzten Schritt, in der **Implementierungsplanung**, wird eine neue, effiziente ISG etabliert, die alle (vorstandsrelevanten) DORA-Anforderungen erfasst und steuert. Es werden klare Richtlinien und Verantwortlichkeiten definiert, um die Akzeptanz der neuen Governance in der gesamten Organisation zu fördern. Durch gezielte Kommunikation und regelmäßiges Feedback werden alle Stakeholder eingebunden, wodurch eine reibungslose Umsetzung gewährleistet wird. Das Ergebnis ist eine robuste ISG, die nicht nur aktuellen Anforderungen gerecht wird, sondern die Organisation auch langfristig auf zukünftige Herausforderungen vorbereitet.

Kontaktieren Sie uns.

Sie möchten eine vertiefte Diskussion zum Thema Informationssicherheit führen oder Ihre Erfahrungen mit uns teilen? Ein offener und vertrauensvoller Austausch ist uns ein großes Anliegen. Lassen Sie uns gemeinsam daran arbeiten, Ihre ISG zu stärken und den Weg zu dauerhaftem Erfolg und Sicherheit zu ebnen.

MOONROC Advisory Partners GmbH
Steinsdorfstraße 14
80538 München
E-Mail: company@moonroc.de
Internet: www.moonroc.de

Über die Autoren.

Patrick Natus
Managing Partner (MOONROC)

Patrick Natus ist ein führender Experte in Transformationsfragen. In zahlreichen Projekten in Deutschland und im europäischen Ausland lag sein inhaltlicher Schwerpunkt auf den Themen Strategie und Transformation. Die Begleitung großer organisatorischer und personeller Veränderungen gehört zu seinem Spezialgebiet.

Luisa Küffner
Consultant (MOONROC)

Luisa Küffner ist Strategy Consultant bei MOONROC und spezialisiert auf den Financial Services Sektor. Mit umfangreicher Erfahrung in strategischen IT- und Transformationsprojekten hat sie Unternehmen erfolgreich bei der Umsetzung ihrer digitalen und operativen Ziele unterstützt.

Detlev Henze
Gründer und ehem. Geschäftsführer (TÜV TRUST IT GmbH)

Detlev Henze ist seit über 25 Jahre Experte im Bereich Informations- und Cybersecurity. Als Gesellschafter und Geschäftsführer hat er mit der TÜV TRUST IT GmbH einen namhaften und großen Anbieter für Security-Beratung und -Prüfung aufgebaut und etabliert. In seiner leitenden Konzernfunktion hat er erfolgreich Konzern-Neustrukturierungen geplant und umgesetzt. Organisatorische Veränderungen, der Aufbau und die Implementierung von Governance-Modellen sowie die Führungsentwicklung gehören zu den Bereichen, in denen er zahlreiche Kunden erfolgreich unterstützt hat.

Haftungsausschluss

Die Darstellungen und Analysen in diesem Bericht stellen, soweit nicht anders vorhanden, Schätzungen dar. Trotz größter Sorgfalt können sich die Inhalte, Daten und Informationen inzwischen verändert haben. Eine Haftung oder Garantie für die Korrektheit, Aktualität und Vollständigkeit der zur Verfügung gestellten Inhalte, Daten und Informationen kann nicht übernommen werden. Des Weiteren behält sich MOONROC das Recht vor, Änderungen oder Ergänzungen der bereitgestellten Inhalte, Daten und Informationen jederzeit vorzunehmen.

www.moonroc.de