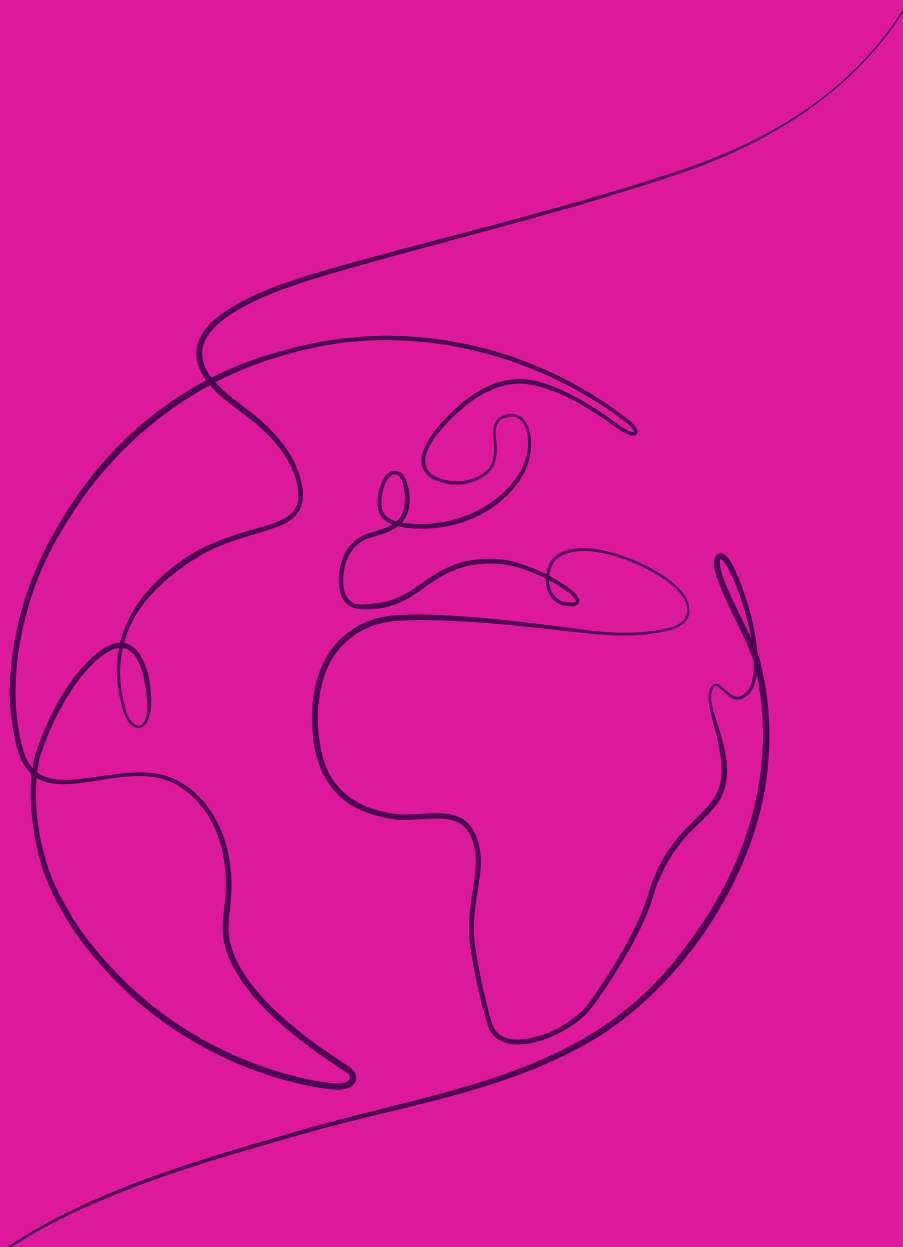
beazley

Snapshot Report Deutschland 2023

Risiko und Resilienz in volatilen Zeiten



Executive Summary

Der Krieg in der Ukraine, die rasante technologische Entwicklung und der zunehmende Fokus auf ESG-Themen (Environmental, Social, Governance) fordern deutsche Unternehmensleiter wie nie zuvor. Angesichts der unsicheren geopolitischen Lage in Europa, gestiegenen Kosten, Produktionseinbrüchen und einer Rezession[1] untersuchen wir die Risiken, auf die sich Führungskräfte zunehmend unvorbereitet fühlen.

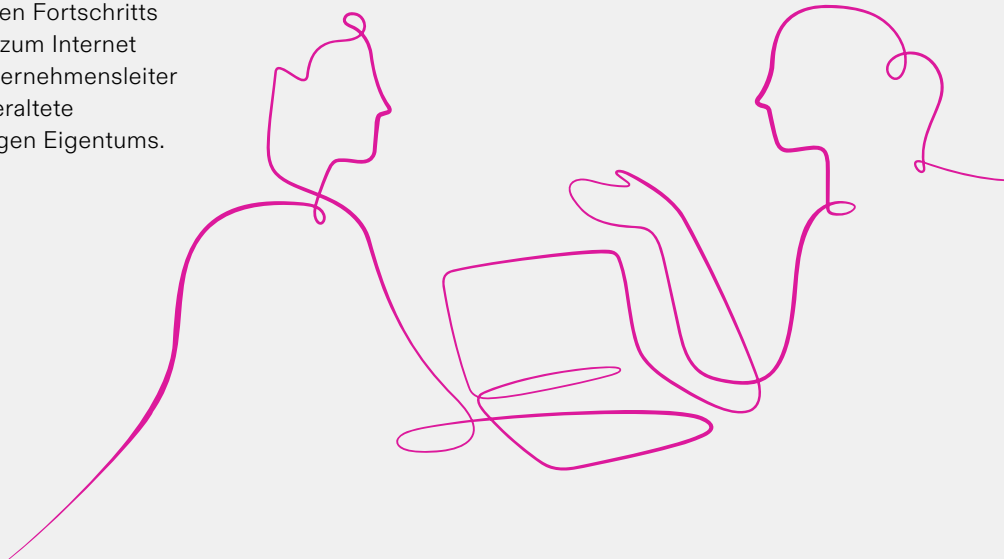
Der Bericht basiert auf einer Umfrage mit 250 Unternehmensleitern und Führungskräften sowie Versicherungsnehmern aus 10 Branchen in Deutschland und ist mit Kommentaren erfahrener, lokaler Experten angereichert. Er beleuchtet die aktuelle Haltung in Unternehmen zu Bedrohungen für die Wirtschaft durch den Krieg in der Ukraine sowie die Einstellung zu unmittelbaren Risiken.

Unsere Untersuchung zeigt, dass 28 Prozent der befragten Führungskräfte in Deutschland Cyberrisiken als primäre Gefahr bewerten. Die Einschätzung der Befragten vergleicht auch die unterschiedliche Auffassungen von Unternehmensleitern in Deutschland zu denen in Frankreich und Spanien bezüglich Cyberrisiken und der Beurteilung der Fähigkeiten sie zu mindern.

Angesichts des rasanten technologischen Fortschritts – von künstlicher Intelligenz (KI) bis hin zum Internet der Dinge (IoT) – konzentrieren sich Unternehmensleiter zunehmend auf die Bedrohung durch veraltete Technologie sowie den Diebstahl geistigen Eigentums.

Es bleibt abzuwarten, ob kleinere und mittlere Unternehmen, vor allem solche, die nicht über die finanziellen Mittel größerer Konkurrenten verfügen, in den kommenden Jahren mithalten können.

Unternehmen müssen auch mit einer Reihe neuer ESG-Vorschriften Schritt halten, wie der Corporate Sustainability Reporting Directive (CSRD), der Corporate Sustainability Due Diligence Directive (CSDDD) und den European Sustainability Reporting Standards (ESRS), die alle bis 2024 umgesetzt werden sollen. Die schnelle Neuordnung erfordert viel Aufmerksamkeit, und Unternehmen fühlen sich durch die Zunahme der ESG-bezogenen Bürokratie auf lokaler und globaler Ebene stark belastet.

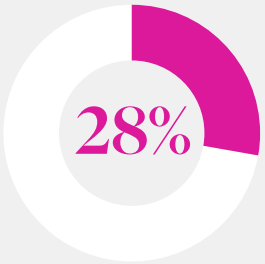


[1] Deutsche Wirtschaft in Rezession: Zahl der Erwerbstätigen sinkt erstmals seit zehn Monaten – n-tv.de

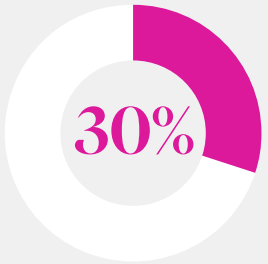
Diese Bedrohungen nehmen weiter zu und treten immer häufiger auf. Daher kommt Versicherern eine entscheidende Rolle zu - sie müssen Unternehmen dabei unterstützen, die richtigen Strategien zu entwickeln, um auf die Hürden von morgen angemessen vorbereitet zu sein und somit die Risiken zu mindern. Es ist eine lange Tradition deutscher Unternehmen, auf Herausforderungen zu reagieren und gestärkt daraus hervorzugehen. Um das auch heute zu schaffen, müssen Führungskräfte Risiken in ihrem gesamten Umfeld verstehen und Maßnahmen ergreifen, um sie sowohl jetzt als auch auf lange Sicht zu mindern.

Während Unternehmen sich von den Folgen der Pandemie erholt haben, stehen sie heute vor einer Reihe neuer Herausforderung, die andere Vorkehrungen und Schutzmaßnahmen erfordern. Das hat unter anderem zur Folge, dass 42 Prozent der befragten Führungskräfte jetzt Versicherungsoptionen mit Krisenmanagement erwägen, um ihre Resilienz zu erhöhen.

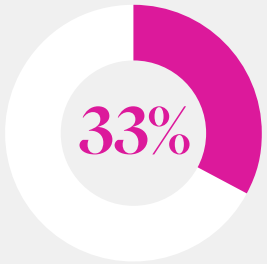
Zentrale Erkenntnisse unserer Studie zur Sicht von Unternehmensleitern in Deutschland zu aktuellen Risiken:



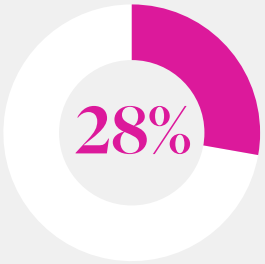
sehen Cyberrisiken als zentrales Thema an



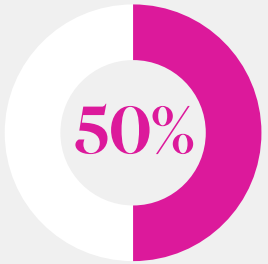
fühlen sich heute nicht auf die Bedrohung durch Cyberrisiken vorbereitet. Bei kleineren Unternehmen mit einem Jahresumsatz von weniger als 1 Million Euro sind es sogar 42 Prozent.



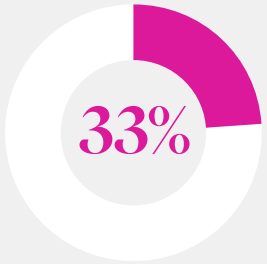
planen, im Jahr 2023 in die Verbesserung ihrer Cybersicherheit zu investieren



halten Cyberkriminalität und technologische Obsoleszenz für die beiden größten Risikoherausforderungen



der Führungskräfte aus der Fertigungsindustrie sehen in der technologischen Obsoleszenz die größte Gefahr für ihr Unternehmen



stufen ESG als ihre größte Sorge ein, da die Fristen für eine Reihe von ESG-Vorschriften, die 2024 in Kraft treten sollen, näher rücken

Inhalt

Cyberrisiken: Hauptsorge der Vorstände

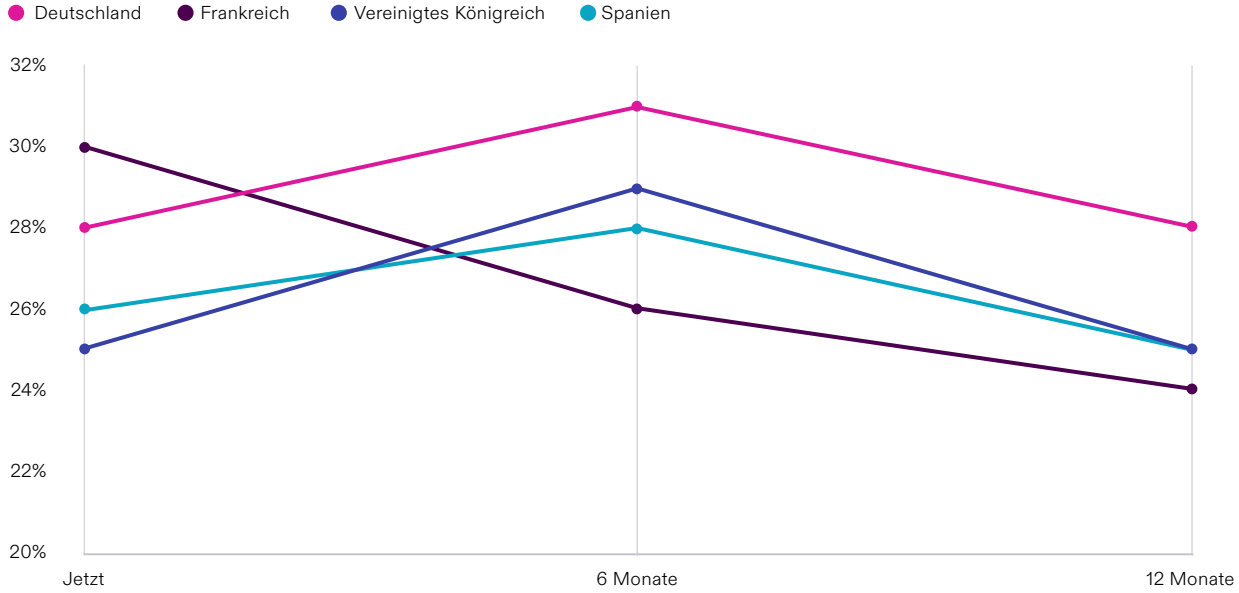
Nach dem Einmarsch Russlands in die Ukraine wurden einige deutsche Unternehmen Opfer mehrerer aufsehenerregender Angriffe von kriminellen Gruppen, wie Killnet. Diese Gruppen haben es auf Organisationen in der gesamten Wirtschaft abgesehen, von Behörden über Finanzdienstleister[2] bis hin zum Luftfahrtsektor.

Im Februar hob die deutsche Innenministerin Nancy Faeser die Alarmstufe auf „sehr hoch“ an und warnte, dass sich das Land nun an der Frontlinie einer Flut von russischen Sabotage-, Desinformations- und Spionageangriffen befinde. Weitere Warnungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) haben das Risiko unterstrichen, und Unternehmen beginnen nun, das Ausmaß der Internetkriminalität[3] zu begreifen.

Von allen Risiken, mit denen deutsche Vorstände konfrontiert sind, steht Cyberkriminalität an erster Stelle: 28 Prozent nennen das als zentrales Risikothema. Sie gehen auch davon aus, dass diese Bedrohung andauern wird. Während ihre Kollegen in Frankreich, Spanien und dem Vereinigten Königreich der Meinung sind, dass die Gefahr abnehmen werde, gehen 28 Prozent der Führungskräfte davon aus, dass sie langfristig weiterhin Cyberkriminellen ausgesetzt sein werden.

Deutsche Unternehmen sehen Cyberrisiken anders als ihre europäischen Mitbewerber

Prozentsatz der Vorstandsmitglieder, die Cyberrisiken im Laufe der Zeit als ihr Hauptrisiko einstufen



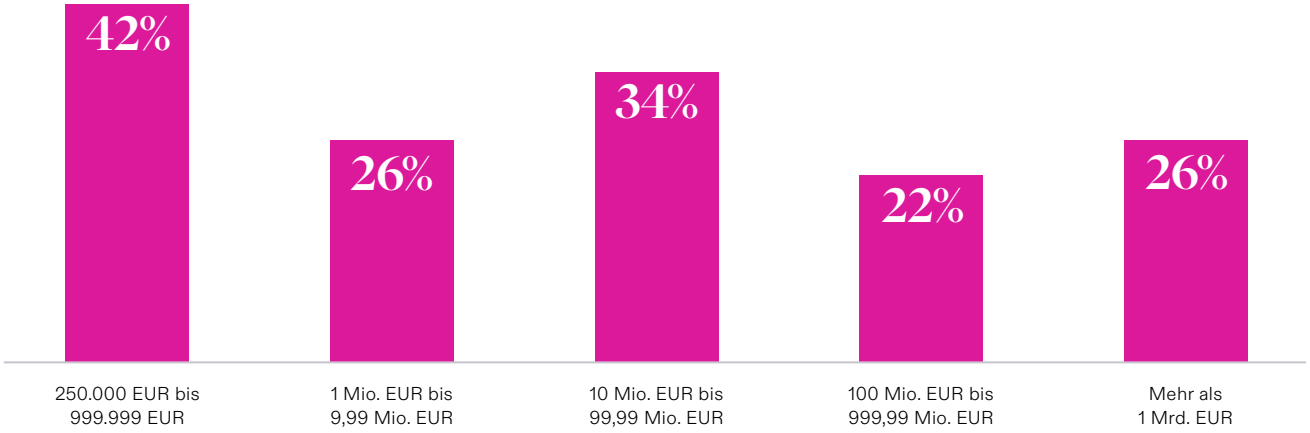
[2] Russian hackers launch cyberattack on Germany in Leopard retaliation | Euronews
[3] German cyber agency warns threat situation is ‘higher than ever’ | therecord.media

Die Besorgnis der Unternehmensleiter spiegelt sowohl die zunehmende Raffinesse von Cyberangriffen als auch die steigende Zahl von Attacken mit höheren finanziellen Schäden sowie Imageschäden wider. Daten des BSI zeigen, dass Cybererpressung, etwa durch Ransomware, die größte Bedrohung für deutsche Unternehmen darstellt. Die nimmt weiter zu, weil Hacker immer neue Taktiken einsetzen. Eine Methode, die in Deutschland und ganz Europa immer häufiger auftritt, ist das sogenannte „Bricking“, aus dem Englischen „brick“ zu Deutsch „Ziegelstein“: Hierbei werden elektronische Geräte irreparabel beschädigt und so zu einem „Ziegelstein“.[4]

Obwohl Führungskräfte sich der aktuellen Cyberbedrohung bewusst sind, fühlt sich fast ein Drittel der Unternehmensleiter in Deutschland (30 Prozent) nicht auf die Bedrohung durch Cyberrisiken vorbereitet. Bei kleineren Unternehmen mit einem Jahresumsatz von weniger als 1 Million Euro sind es sogar 42 Prozent. Deswegen plant mehr als jedes dritte deutsche Unternehmen (33 Prozent), im kommenden Jahr in eine verbesserte Cybersicherheit zu investieren – bei mittelständischen Unternehmen mit einem Jahresumsatz zwischen 1 und 10 Millionen Euro sind es 44 Prozent.

Deutsche Kleinunternehmen fühlen sich durch Cyberrisiken besonders gefährdet

Prozentsatz deutscher Vorstandsmitglieder, die sich auf Cyberrisiken nicht vorbereitet fühlen, nach Jahresumsatz des Unternehmens



Kriminelle Gruppen werden immer raffinierter, ändern ihre Taktiken und erhöhen ihre Forderungen. Erpresserische Praktiken sind in Deutschland mittlerweile gang und gäbe, und Cyberkriminelle versuchen, Unternehmen so viel Schaden wie möglich zuzufügen.“

Christian Taube
Head of Cyber Services International, Beazley

[4] HP rushes to fix bricked printers after faulty firmware update | bleepingcomputer.com

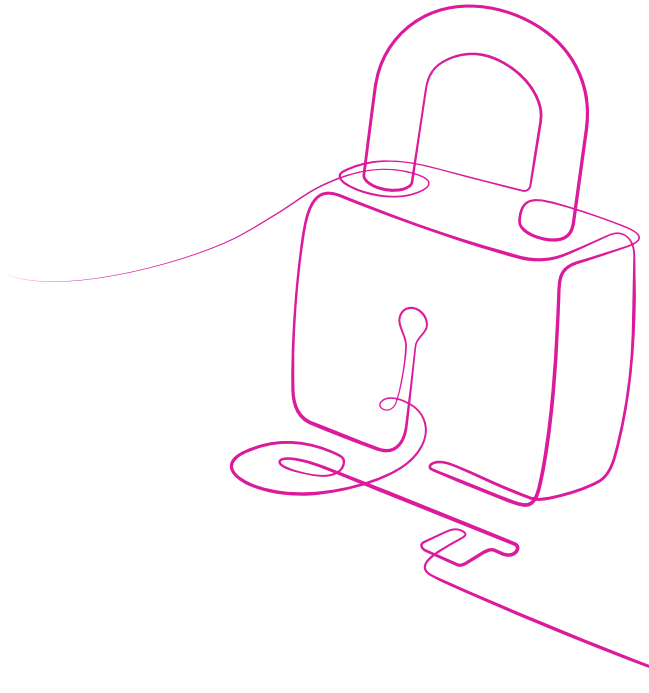
Angesichts neuer krimineller Taktiken müssen Unternehmen ihre Strategien für die Cybersicherheit weiterentwickeln. Die Beteiligung von Nationalstaaten an Cyberangriffen und kriminellen Organisationen wird auf absehbare Zeit weiterhin im Mittelpunkt der Aufmerksamkeit von Unternehmensleitern stehen. Bei dieser sich ständig verändernden Bedrohung ist Wachsamkeit besonders entscheidend. Andernfalls drohen Unternehmen finanzielle Schäden und ein erheblicher Imageschaden.“

Gesine Froese
Head of Cyber & Tech DACH,
Beazley

Cyberversicherung – Vorbeugung ist Teil der Lösung

In den letzten Jahren hat sich der Wert einer Cyberversicherung zweifelsfrei erwiesen: Versicherer mussten bereits auf eine Flut von Vorfällen reagieren und zahlten allein für Ransomware-Schäden Milliardenbeträge aus. Das hat es Unternehmen in Nordamerika, Großbritannien und Asien ermöglicht, sich wieder zu erholen und sie vor erheblichen finanziellen Folgen bewahrt, die sie sonst erlitten hätten. Deutsche Unternehmen haben ebenso wie ihre europäischen Kollegen erst spät erkannt, wie wichtig es ist, sich gegen diese Bedrohung zu schützen und welche Rolle eine Cyberversicherung hat: bei der Vorbereitung und Bewältigung von Cybervorfällen oder bei der Wiederherstellung nach einem Angriff. Experten müssen weiterhin auf die Risiken hinweisen und erklären, wie wichtig es ist, wachsam zu bleiben und weiterhin in eine umfassende Risikostrategie zur Cybersicherheit zu investieren und sie durchzusetzen.

Unternehmensleiter müssen sich auch darauf verlassen können, dass ihr Risikomanagement fähig ist, die Gefahr eines erfolgreichen Cyberangriffs so weit wie möglich zu minimieren. Es ist ein zentrales Ziel von Beazley, Kunden die Werkzeuge an die Hand zu geben, die sie benötigen, um in Sachen Cybersicherheit immer einen Schritt voraus zu sein. Denn wir wissen, dass Prävention, Vorbereitung und Reaktion bei der Versicherung von Cyberrisiken entscheidend und untrennbar sind.



ESG-Risiken erreichen ihren Höhepunkt

Die Bestimmungen für die ESG-Berichterstattung (Environmental, Social, Governance) werden immer umfassender und betreffen jedes Jahr mehr Unternehmen.

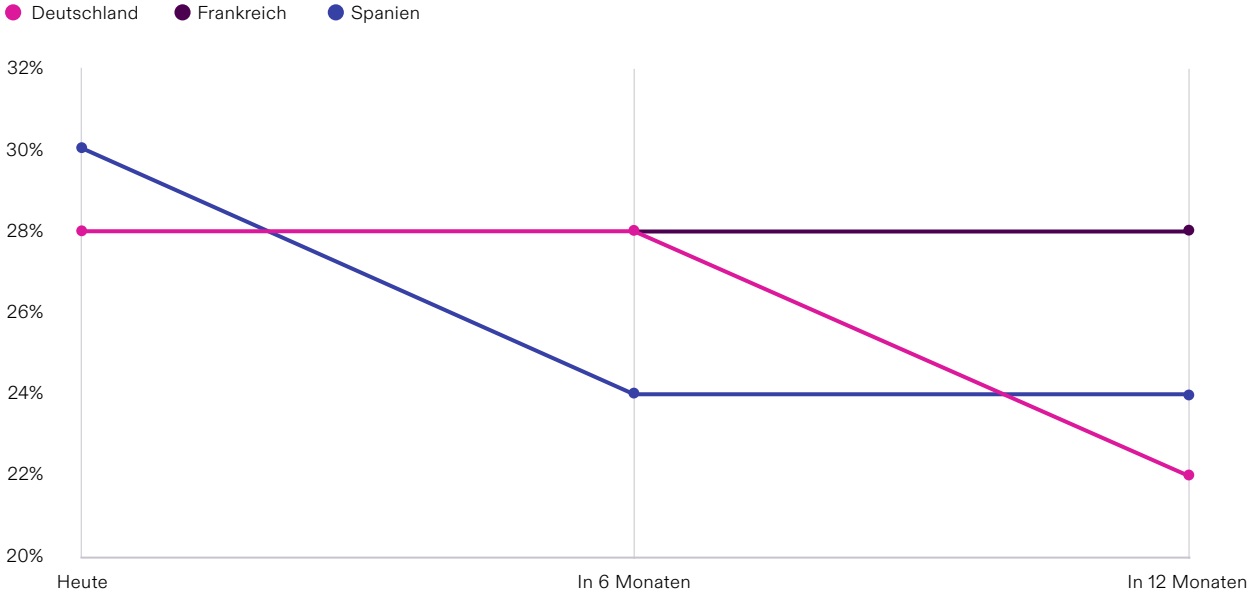
ESG-Regulierung ist ein globales Phänomen: Länder versuchen, ihre Industrien in Richtung Klimaneutralität zu bewegen und das Greenwashing-Risiko durch transparentere Berichterstattung zu verringern. Dabei wird die Anpassung an die Vorschriften immer schwieriger, insbesondere in der EU, wo immer mehr Regulierungen in Kraft treten.

Das erste Inkrafttreten einer Reihe von Verordnungen, von der CSRD über die CSDDD bis zu den ESRS5, ist für 2024 vorgesehen und rückt schnell näher. Bei Nichteinhaltung drohen schwere Strafen, von öffentlicher Anklage bis hin zu Geldstrafen – bisher ohne Obergrenze. Dabei ist es keine Option, sich nicht an die ESG-Regulierung zu halten: Selbst wer sich der Umwelt nicht verpflichtet fühlt, darf die Finanzen und den Ruf des Unternehmens nicht riskieren.

Das bevorstehende Inkrafttreten rückt in den Mittelpunkt der Aufmerksamkeit, und fast ein Viertel (24 Prozent) der deutschen Unternehmensleiter stuft ESG heute als ihr größtes Risiko ein.

Besorgnis über ESG-Risiken in den Vorstandsetagen deutscher Unternehmen wird ihren Höhepunkt erreichen und abnehmen

Prozentsatz der Vorstandsmitglieder, die der Meinung sind, dass ESG das größte Risiko für sie darstellt



ESG-Herausforderungen sind hier, um zu bleiben. Ich glaube nicht, dass wir in absehbarer Zeit eine neue Normalität erreichen werden, bei der sich die Unternehmen entspannt zurücklehnen können, weil sie alle rechtlichen Anforderungen auf unbestimmte Zeit erfüllt haben. Es besteht ein breiter Konsens darüber, dass der Klimawandel und Cyberrisiken die beiden systemischen globalen Risiken sind, denen die Gesellschaft heute gegenübersteht."

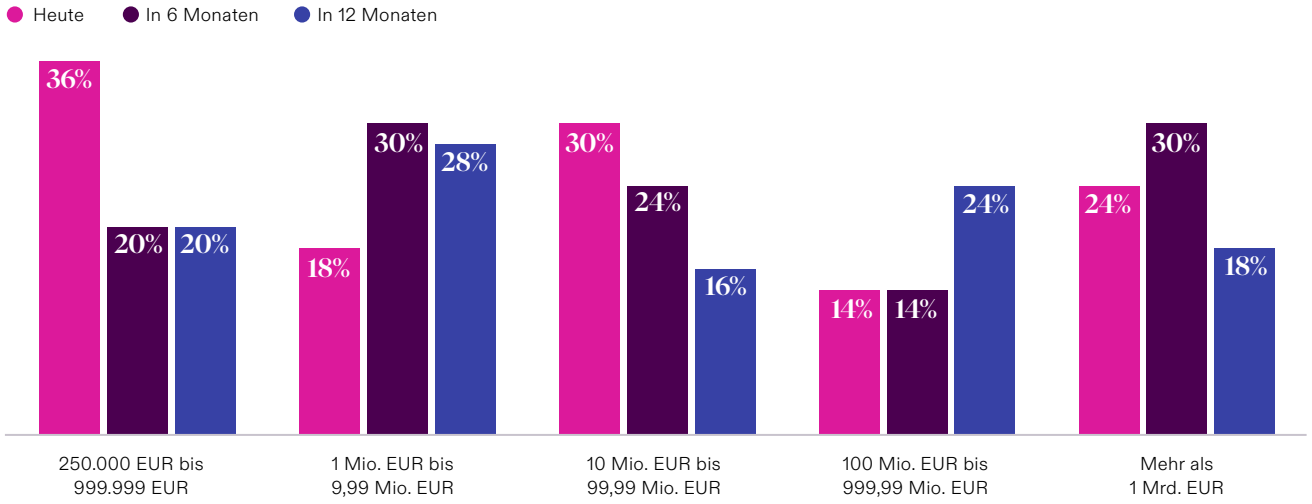
Henning Schaloske
Partner, Clyde & Co.

Unternehmen unterschiedlicher Größe stehen unter unterschiedlichem Druck: Größere, komplexere Organisationen mit größeren Budgets werden ganze Teams zur Verfügung haben, um ESG-Compliance-Pläne umzusetzen, da sie unter dem Druck des nahen Inkrafttretens der Verordnungen stehen. Kleinere Unternehmen verfügen meist über weniger Ressourcen und stehen aufgrund der späteren Frist unter weniger Druck, Veränderungen sofort umzusetzen, sodass sie tendenziell weniger gut vorbereitet sein werden. Für die CSRD-Bestimmungen gelten beispielsweise gestaffelte Fristen je nach Unternehmensgröße: Börsennotierte Unternehmen mit mehr als 500 Beschäftigten müssen ab 2024 Bericht erstatten, gefolgt von großen nicht börsennotierten Unternehmen im Jahr 2025 und KMU ab 2026[5].

KMU, deren ESG-Reporting-Fristen weiter in der Zukunft liegen, werden den Druck in den nächsten 12 Monaten stärker zu spüren bekommen als ihre größeren Konkurrenten. Etwas mehr als ein Viertel (27 Prozent) der Unternehmen mit einem Jahresumsatz von weniger als 10 Millionen Euro stufen ESG heute als ihr größtes Risiko ein. In 12 Monaten wird dieser Wert leicht auf 24 Prozent fallen.

Unternehmensleiter verschiedener Ertragsklassen nehmen ESG-Risiken stark unterschiedlich wahr

Prozentsatz der Vorstandsmitglieder deutscher Unternehmen, die der Meinung sind, dass ESG das größte Risiko für sie darstellt – nach Jahresumsatz des Unternehmens



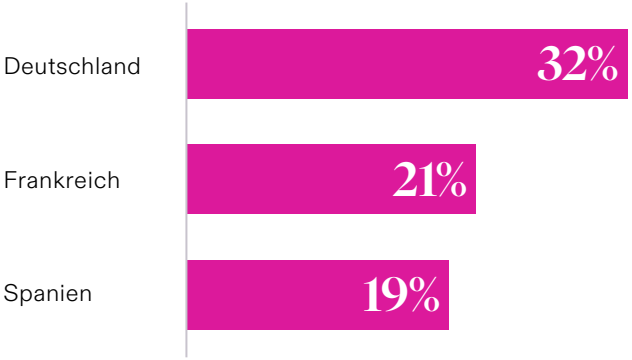
[5] CSR - Corporate Sustainability Reporting Directive (CSRD) | csr-in-deutschland.de

Schlechte Aussichten bei Untätigkeit in "S" und "G

Während Führungskräfte in Deutschland unseren Untersuchungen zufolge im Allgemeinen weniger über ESG-Risiken besorgt zu sein scheinen als ihre französischen und spanischen Kollegen, geben sie umgekehrt auch an, sich ESG-Risiken stärker ausgesetzt zu fühlen. Fast ein Drittel (32 Prozent) der Unternehmensleiter in Deutschland gab an, dass sie nicht auf ESG-Risiken vorbereitet sind, verglichen mit etwa einem Fünftel der Führungskräfte in Frankreich (21 Prozent) und Spanien (19 Prozent).

Vorstände in Deutschland fühlen sich weniger gut auf ESG-Risiken vorbereitet

Prozentsatz der Vorstandsmitglieder, die sich auf ESG-Risiken nicht vorbereitet fühlen, nach Land



Angesichts der Flut von Vorschriften, mit denen europäische Unternehmen konfrontiert sind, forderte der französische Präsident Emmanuel Macron die EU auf, die Umsetzung der ESG-Vorschriften auszusetzen.[6] Seine Forderung, die von europäischen Unternehmen unterstützt wird, könnte auch darauf zurückzuführen sein, dass die sozialen und Governance-Verbesserungen, die die Unternehmen erzielen sollen, noch nicht definiert sind, obwohl die Risiken, die sich aus dem Fehlen strenger Governance-Verfahren ergeben, immer deutlicher werden.

Anstelle formeller Vorschriften oder staatlich verordneter S- und G-Ziele werden Rechtsfälle, die vor Gericht verhandelt werden, den Präzedenzfall dafür schaffen, wie andere Unternehmen behandelt werden, deren Verhalten bemängelt wird. Ein Beispiel hierfür wären die Razzien bei der DWS Gruppe, der Vermögensverwaltungssparte der Deutschen Bank, im vergangenen Jahr: Die Untersuchung von Greenwashing-Vorwürfen könnte zu erheblichen Geldstrafen für die Gruppe führen, wie der Vorstandsvorsitzende der DWS, Stefan Hoops, Anfang des Jahres erklärte.[7]

„ESG ist für Unternehmensvorstände ein wichtiger Teil der Risikoerwägung. Gesetzgeber, Kunden, Mitarbeiter und Investoren erwarten zunehmend glaubwürdige ESG-Programme mit messbaren Zielen. Gute Unternehmensführung, ein verantwortungsbewusster Umgang mit dem gesellschaftlichen und ökologischen Fußabdruck und eine faire Behandlung von Mitarbeitern und Partnern sind jetzt gesetzlich vorgeschrieben, und wenn das nicht umgesetzt wird, stellt es ein finanzielles und geschäftliches Risiko sowie ein Reputationsrisiko dar."

Ulrich Schaller
Manager – Financial Lines (Deutschland), Beazley

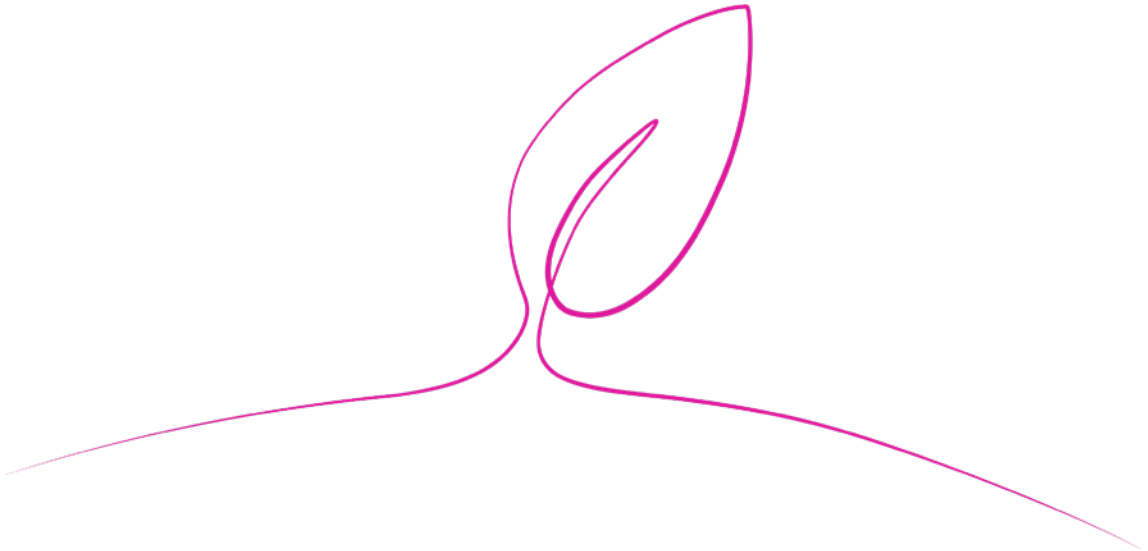
[6] Green Deal: Macron will „Pause" in der EU-Gesetzgebung | EURACTIV.de
[7] Deutsche Bank's DWS May Be Facing Greenwashing Fines, CEO Says | bloomberglaw.com

Von strafrechtlichen Ermittlungen bis hin zu Strafen und zivilrechtlicher Haftung sendet die Verfolgung dieser Fälle die deutliche Botschaft, dass mit den Compliance-Anforderungen nicht zu spaßen ist und dass die Konsequenzen für jedes wahrgenommene Fehlverhalten in Deutschland und Europa durchgesetzt werden.“

Henning Schaloske
Partner, Clyde & Co.

Auch der Ruf aus einer gut informierten Öffentlichkeit wird immer lauter: Organisierte Aktivitäten von Klima-Aktionsgruppen wie „Letzte Generation“ versprechen noch mehr Störungen in den kommenden Monaten, wie es der „Sommerplan 2023“ der Gruppe verspricht.[8] Die Klimaaktivisten werden von der Öffentlichkeit nicht nur zahlenmäßig unterstützt, sondern auch mit erheblichen Spenden in Höhe von etwa 400.000 Euro, um Protestaktionen gegen diejenigen zu finanzieren, deren Handlungen sie als umweltschädlich erachten. Unternehmen, die sich in der Schusslinie befinden, könnten erhebliche Geschäftsunterbrechungen erleiden, wenn Demonstranten ihre Standorte blockieren, und/oder ihren Ruf schädigen. Während der Druck an verschiedenen Fronten zunimmt, sind deutsche Unternehmen mit einer überwältigenden Anzahl von Forderungen nach ESG-Maßnahmen konfrontiert und müssen sicherstellen, dass die Risikobewertungen gründlich sind und mit den Zeiten Schritt halten.

Weil Umweltrisiken von außen so stark in den Mittelpunkt gerückt sind, ist es wichtig, Kunden zu unterstützen, die solche Risiken aktiv managen. Die Versicherungsbranche kann mehr tun, um ihr Angebot hervorzuheben: Von der Haftpflichtversicherung für Vorstandsmitglieder und leitende Angestellte bis hin zum Reputationsrisiko und anderen Haftpflichtversicherungen für das Management kann eine Versicherung Unternehmen helfen, Umweltrisiken und die potenziell kostspieligen Auswirkungen von Greenwashing und anderen klimabezogenen Rechtsstreitigkeiten zu bewältigen.



[8] Klimaaktivismus: Letzte Generation plant gezielte Aktionen gegen Vermögende | Zeit.de

Die Zukunft des Mittelstands

Der Mittelstand und seine Rolle in der deutschen Wirtschaft ist weltweit Gegenstand unzähliger betriebs- und volkswirtschaftlicher Vorlesungen gewesen.

Er wird bewundert und studiert. Er beschäftigt 55 Prozent[9] der deutschen Erwerbstätigen und trägt 52,6 Prozent zur Wirtschaftsleistung bei. Den Mittelstand als KMU zu definieren, wäre zu einfach. Es geht nicht nur um die Größe, sondern auch um Eigentum, Fokus und Spezialisierung. Dieser Begriff steht für einen Teil der deutschen Wirtschaft, dessen Produkte heute weltweit für ihre überragende Güte geschätzt werden. Die Gedanken der Vorstandsmitglieder im gesamten Mittelstand konzentrieren sich zunehmend auf die Gefahr der technologischen Obsoleszenz ihrer Unternehmen. Der Sektor, dessen Markenzeichen die Innovation ist, hat Angst vor der Technologie von morgen.

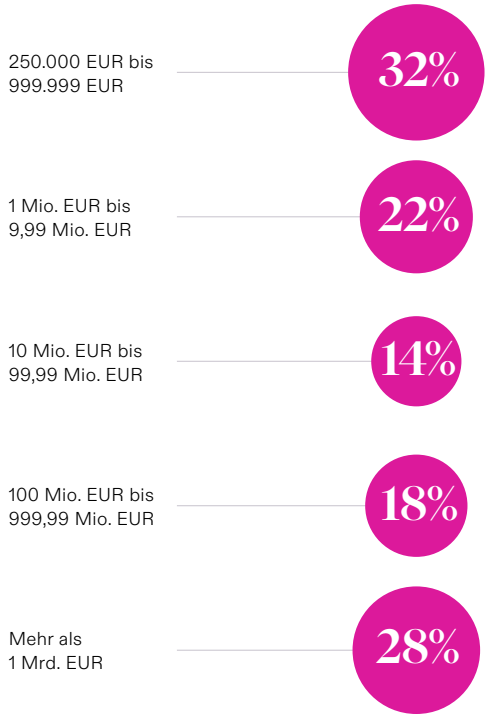
Mehr als sieben von zehn deutschen Unternehmen (72 Prozent) sehen im Scheitern, mit Innovationen Schritt zu halten, eine zentrale Bedrohung für ihr Geschäft. Neben der Cyberkriminalität (28 Prozent) wird die technologische Obsoleszenz als das größte Risiko angesehen, dem sie ausgesetzt sind.

Ob es sich nun um bahnbrechende Fortschritte handelt oder um die eher alltägliche Modernisierung von Systemen, der technologische Wandel bedroht nun einen Sektor, der sich in schwierigen Zeiten bewährt und durch Produktinnovationen hervorgetan hat.

Das Aufkommen von KI und die Entwicklung von IoT-Technologien stellen langfristige Bedrohungen dar, für die sich deutsche Unternehmen, insbesondere solche am unteren Ende des Umsatzspektrums, schlecht gerüstet fühlen. Fast ein Drittel der Unternehmen (32 Prozent) mit einem Umsatz zwischen 250.000 und 999.999 Euro fühlt sich nicht darauf vorbereitet, sich an die Bedrohung durch neue Technologien anzupassen.

Große Unternehmen in Deutschland fühlen sich besser auf die Bedrohung durch technologische Obsoleszenz vorbereitet

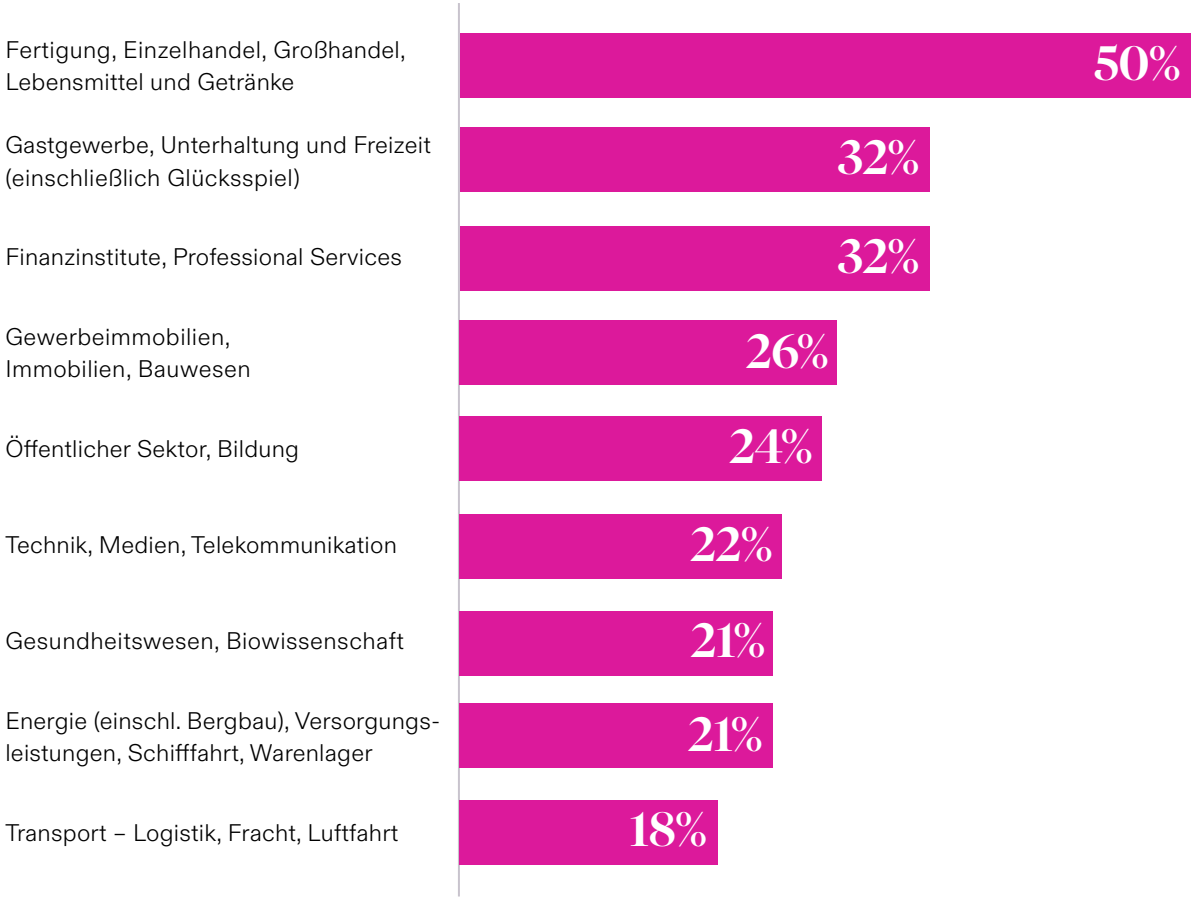
Prozentsatz der deutschen Vorstandsmitglieder, die sich derzeit auf technologische Obsoleszenz nicht vorbereitet fühlen, nach Jahresumsatz des Unternehmens



[9] 55 % in kleinen und mittleren Unternehmen tätig - Statistisches Bundesamt | destatis.de

Drohende Technologiekrise bei deutschen Herstellern

Prozentsatz deutscher Vorstandsmitglieder, die sich auf Cyberrisiken nicht vorbereitet fühlen, nach Jahresumsatz des Unternehmens



Der deutsche Mittelstand besteht hauptsächlich aus Herstellern. Immer mehr physische Güter interagieren mit digitalen Anwendungen, insbesondere durch IoT-Technologie. Die Hälfte der deutschen Hersteller (50 Prozent) sieht darin die größte Bedrohung für ihr Unternehmen, mehr als in jeder anderen Branche in allen von uns untersuchten Ländern.

Deutsche Vorstandsmitglieder in der Gastgewerbe-, Unterhaltungs- und Freizeitbranche fühlen sich am wenigsten auf die Bedrohung durch die technologische Obsoleszenz vorbereitet.

Die Einsicht, dass die Industrie vernetzte Technologien integrieren muss, ist ein Grundsatz für das Zukunftsprojekt Industrie 4.0 der Bundesregierung,[10] der sicherstellen soll, dass die verarbeitende Industrie des Landes ihre Vorrangstellung behält und sich an neue Innovationen anpasst.

Für die deutsche Wirtschaft besteht sowohl ein wirtschaftlicher Nutzen als auch ein demografischer Zwang, neue Technologien zu integrieren, die eine Automatisierung der industriellen Basis ermöglichen. KI und andere technologische Innovationen könnten eine Alternative zur menschlichen Arbeitskraft darstellen und so dem demografischen Wandel entgegen wirken. Die Übernahme dieser Innovationen stellt jedoch eine neue Angriffsfläche für mittelständische Unternehmen dar. Da diese Technologien vernetzt sind, vergrößern sich die Einfallstüren für Cyberkriminelle, die sich Zugang zu Unternehmensnetzwerken verschaffen wollen.

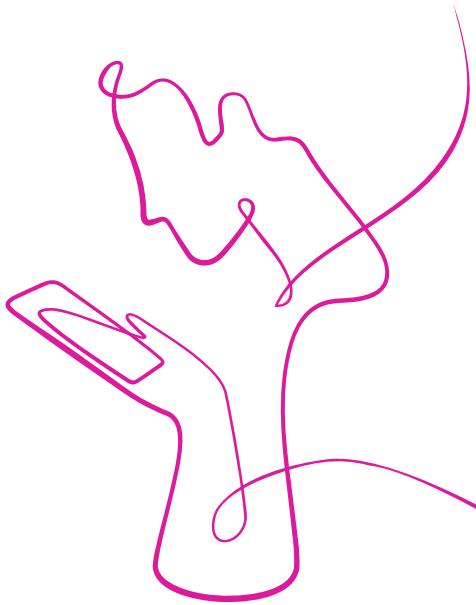
[10] Industrie 4.0 | BMBF

Deutsche Unternehmen sind traditionell sehr datenschutzbewusst; dieser Fokus muss sich nun auch auf die Produktgestaltung übertragen. Cybersicherheitsexperten sollten bereits in der Entwicklungsphase und während des gesamten Produktlebenszyklus einbezogen werden, um die soliden Datenschutzstandards zu wahren, die deutsche Unternehmen typischerweise eingehalten haben.“

Gesine Froese
Head of Cyber & Tech DACH,
Beazley

Die Einführung neuer Technologien führt auch dazu, dass bewährte Methoden der Produktentwicklung überprüft werden. Bei den meisten Herstellern wurde die Cybersicherheit in der Phase der Produktentwicklung bisher nicht berücksichtigt. Ihre Waren schienen keine Technologie zu enthalten, die dies erfordern würde. Aber die Integration von neuer Technologie bedeutet auch die Integration neuer Risiken. Idealerweise wird im Produktdesign Cybersicherheit von Anfang an mit berücksichtig werden. Derzeit ist es jedoch für viele deutsche Unternehmen Herausforderung genug, mit Sicherheitspatches und der Modernisierung ihrer bestehenden IT-Systeme Schritt zu halten. Ob Unternehmen scheitern, weil sie es versäumt haben, mit der technologischen Entwicklung Schritt zu halten, hängt davon ab, ob sie Bedrohungen erkennen und Innovationen annehmen, die ihr Geschäftsmodell unterstützen.

Vorstände im deutschen Mittelstand können die Herausforderung meistern, indem sie IoT und KI einsetzen und Innovationen in ihrem einzigartigen industriellen Ökosystem vorantreiben. Dafür müssen Unternehmen grundlegende Maßnahmen einführen, routinemäßige IT-Sicherheit aufrechterhalten und die Notwendigkeit erkennen, die Widerstandsfähigkeit gegen Cyberrisiken in die Produktgestaltung einzubeziehen. Heutige Risiken jetzt anzugehen, macht die größeren Risiken von morgen einfacher zu bewältigen.



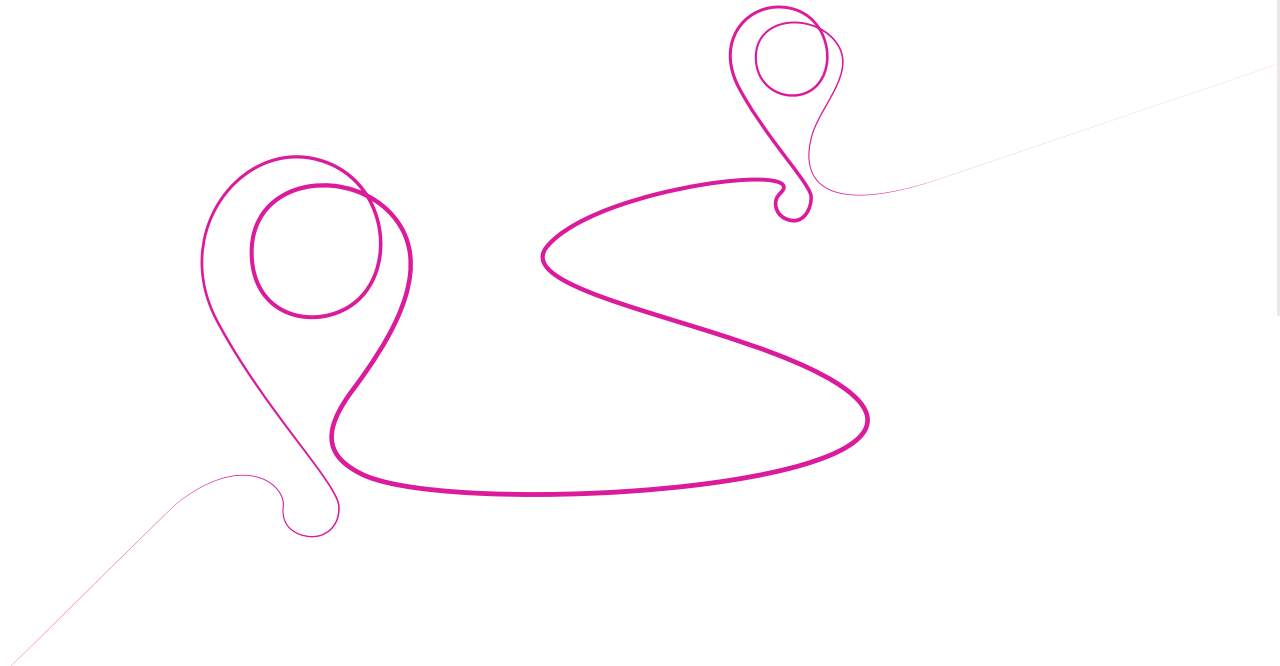
Auf der Suche nach leichteren Zielen

Sehr große Unternehmen haben inzwischen die Bedrohung durch Cyberkriminalität erkannt, und viele haben eine Reihe von Maßnahmen ergriffen, um sich gegen diese Bedrohung zu wappnen – von verbesserter Cybersicherheit bis hin zu maßgeschneidertem Versicherungsschutz. Sie sind zwar nach wie vor gefährdet, aber zu einem schwierigeren Ziel für Cyberbanden geworden, die auf das schnelle Geld aus sind.

Daher verlagern Kriminelle ihren Fokus nun auf kleinere Ziele. Dabei geht es sowohl darum, mittelständische Unternehmen direkt anzugreifen, als auch darum, über sie in die Netzwerke und dadurch in die Supply Chain größerer Unternehmen einzudringen.

Denn die Unternehmen sind digital miteinander vernetzt: Die digitalen Lieferketten multinationaler Organisationen umfassen Unternehmen aller Größenordnungen. Wenn ein Unternehmen am Ende der Kette stark in seine Sicherheit investiert hat, können Cyberkriminelle nach schwächeren Einstiegspunkten entlang der Kette suchen.

Auch erkennen Cyberkriminelle Schwachstellen immer schneller und nutzen die als Einfallstor in Unternehmensnetzwerke. Folglich müssen sich Organisationen noch mehr anstrengen, diese Risiken unter Kontrolle zu halten. Sie brauchen mehrere Verteidigungsschichten, um im Falle eines erfolgreichen Cyberangriffs, das schlimmste zu verhindern.



Eine Defence-in-Depth-Strategie, bei der die Risikominderung im Vordergrund steht und die durch eine solide Versicherungspolice unterstützt wird, ist für die Sicherheit heutiger IT-Systeme unerlässlich.“

Christian Taube
Head of Cyber Services International, Beazley

Methodik

Über die Studio Risiko und Resilienz

Im Februar 2023 haben wir das Marktforschungsunternehmen Opinion Matters beauftragt, die Meinungen von mehr als 750 Unternehmensleitern und Versicherungsnehmern von international tätigen Unternehmen mit Sitz in Deutschland, Frankreich und Spanien (250 in jedem Land) zu erfragen. Die Umfrageteilnehmer wurden zu ihren Ansichten über Versicherer und Versicherungen sowie über zwei Risikokategorien befragt:

- **Cyber und Technologie** – umfasst die Gefahr von Unterbrechungen, technologischer Obsoleszenz, Cyberrisiken und des Diebstahls geistigen Eigentums.
- **Geschäftlich** – einschließlich Instabilität der Lieferkette, Betriebsunterbrechungen, Vorstandsrisiken, Kriminalität, Reputations- und Arbeitgeberrisiken sowie Nichteinhaltung von ESG-Vorschriften und Berichterstattungspflichten.

Die befragten Unternehmen gehörten zu gleichen Teilen folgenden Unternehmensgrößen an: 250.000 EUR–1 Mio. EUR, 1.000.001 EUR–10 Mio. EUR, 10.000.001 EUR–100 Mio. EUR, 100.000.001 EUR–1 Mrd. EUR, mehr als 1 Mrd. EUR.

Eine Mindestzahl von 25 Befragten pro Land und Wirtschaftszweig repräsentierten die befragten Unternehmen, die in diesen Branchen tätig sind:

- Gesundheitswesen, Biowissenschaften
- Fertigung, Einzelhandel, Großhandel, Lebensmittel und Getränke
- Gewerbeimmobilien, Immobilien, Bauwesen
- Gastgewerbe, Unterhaltung und Freizeit (einschließlich Glücksspiel)
- Finanzinstitute, Professional Services
- Energie- und Versorgungsunternehmen (einschließlich Bergbau), Schifffahrt und Lagerhaltung
- Öffentlicher Sektor, Bildung
- Technik, Medien, Telekommunikation
- Transport – Logistik, Fracht, Luftfahrt

Mitwirkende

Christian Taube
Head of Cyber Services, Beazley

Gesine Froese
Head of Cyber & Tech DACH, Beazley

Ulrich Schaller
Manager – Financial Lines (Deutschland), Beazley

Henning Schaloske
Partner, Clyde & Co

Mehr erfahren

Die in dieser Veröffentlichung enthaltenen Beschreibungen dienen lediglich vorläufigen Informationszwecken. Deckungen können von Beazley Syndikaten bei Lloyd's oder Beazley Insurance dac oder Lloyd's Insurance Company ("Lloyd's Brussels") gezeichnet werden und variieren je nach den länderspezifischen gesetzlichen Anforderungen und können in einigen Ländern nicht verfügbar sein. Deckungen sind in den USA nur auf Surplus-Lines-Basis über zugelassene Surplus-Lines-Makler erhältlich. Der genaue Versicherungsschutz, der durch die in dieser Mitteilung beschriebenen Produkte gewährt wird, unterliegt den Bestimmungen und Bedingungen der jeweils ausgestellten Police. Die Veröffentlichung und Übermittlung der hierin enthaltenen Informationen ist nicht als Aufforderung zum Abschluß einer Versicherung für ein US-Risiko gedacht.

beazley

Insurance. Just different.