LÜNENDONK


Lünendonk®-Studie 2022

# Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Eine Studie der Lünendonk & Hossenfelder GmbH
in Zusammenarbeit mit

KPMG

# Inhaltsverzeichnis

# Vorwort

Mario Zillmann
Partner

Liebe Leserinnen, liebe Leser,

eine so hohe Aufmerksamkeit wie in der Zeit der Corona-Krise hatte die IT-Security noch nie. Der Wechsel vieler Beschäftigter in die Homeoffices stellte Security-Verantwortliche vor die Herausforderung, die privaten Endgeräte und Internetverbindungen in die Security-Architektur einzubinden. Gleichzeitig nahmen mit zunehmender Digitalisierung der Kundenschnittstellen im Zusammenhang mit den Lockdowns und der Kontaktbeschränkungen die Anforderungen an die Sicherheit der kundenbezogenen Daten zu. Nicht nur im Handel, sondern auch in klassischen Business-to-Business-Märkten wie dem Maschinenbau oder der Chemieindustrie wurden E-Commerce-Plattformen sehr schnell sehr relevant.

Doch damit nicht genug: Zahlreiche Unternehmen nahmen die Corona-Krise zum Anlass, ihre Geschäftsprozesse und Geschäftsmodelle auf veränderte Kunden- und Marktanforderungen auszurichten, Stichwort: digitale Transformation. In der Folge werden unter anderem immer mehr Geschäftsprozesse in der Cloud abgebildet und sind untereinander – immer häufiger auch unternehmensübergreifend – vernetzt.

Das alles stellt neue Anforderungen an die IT-Security, vor allem weil die potenzielle Angriffsfläche mit zunehmender Digitalisierung immer größer wird. So beobachtet Lünendonk, dass sich die IT-Security rasant weiterentwickelt, hin zu einem Stabilisierungsfaktor für die Resilienz eines Unternehmens. Tatsächlich erfordern immer mehr Unternehmensrisiken unmittelbar eine wirksame Security-Architektur: Sicherstellung der Produktions- und Logistikketten und Vermeidung von Cyber-Angriffen auf die Operational Technology, Schutz der Nutzerinnen und Nutzer softwarebasierter Produkte vor externer Manipulation, die Sicherung kritischer Infrastrukturen vor Hackerangriffen oder aber auch die Einhaltung der EU-DSGVO und der damit verbundene Schutz von Kundendaten.

Neue Dynamik in die Cyber-Bedrohungspotenziale kommt seit März 2022 durch den Russland-Ukraine-Krieg. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt bereits vor einer Zunahme der Bedrohung durch russische Hackergruppen auf deutsche Unternehmen.

Da die Gespräche für diese Studie zwischen Januar und März 2022 stattgefunden haben, sind die Auswirkungen des Russland-Ukraine-Konflikts auf die Sicherheitslage der untersuchten Unternehmen nur sehr eingeschränkt enthalten. Die deutliche Mehrheit der Gespräche fand im Januar und Februar 2022 statt.

## VORWORT

### Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Die vorliegende Lünendonk®-Studie wirft einen umfassenden Blick auf den Stand der Cyber Resilienz in unterschiedlichen Branchen. 140 Verantwortliche für IT-Security wurden dazu telefonisch von Lünendonk befragt. Die Studie ist in Kooperation und fachlicher Zusammenarbeit mit KPMG entstanden.

Ausgenommen von der Analyse wurden der öffentliche Sektor und Finanzdienstleister. Explizit für den Finanzdienstleistungssektor haben Lünendonk und KPMG eine separate Studie zum Stand der Cyber Resilienz erstellt.

Kern der vorliegenden Studie ist die Frage, wie sich die teilnehmenden Unternehmen hinsichtlich der Absicherung ihrer Unternehmensnetzwerke aufgestellt sehen, welche Folgen die zunehmende Cloud-Transformation auf die IT-Sicherheit hat und in welche Security-Bereiche investiert werden soll.

Wir wünschen Ihnen eine interessante und nützliche Lektüre!

Herzliche Grüße

Mario Zillmann

# Methodik

Diese Studie basiert auf 140 Gesprächen vor allem mit CIOs, CTOs und CISOs aus Unternehmen unterschiedlicher Branchen.

Die Gespräche zu dieser Studie fanden ausschließlich telefonisch statt. Neben der Perspektive der IT- und Security-Verantwortlichen wurden auch für das operative Geschäft verantwortliche Managerinnen und Manager befragt. Untersucht wurden unterschiedliche Branchen – mit Ausnahme des öffentlichen Sektors sowie der Finanzdienstleistungsbranche. Hinsichtlich der Branchenverteilung wurde auf einen ausgewogenen Mix geachtet, um aussagekräftige Branchenergebnisse in der Studie darstellen zu können. Die befragten Unternehmen sind sowohl mittelständische Unternehmen ab einem Umsatz von 250 Millionen Euro als auch Konzerne mit Umsätzen von mehr als 1 Milliarde Euro.

## METHODIK DER STUDIE

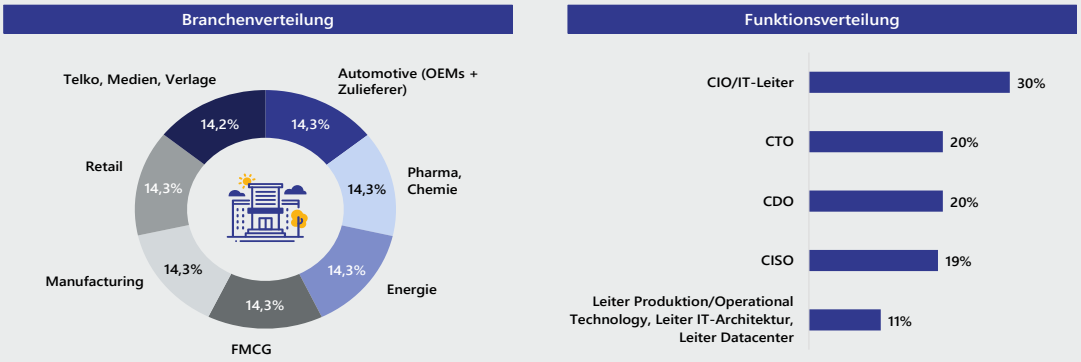


Abb. 1: Branchenverteilung und Funktionsverteilung; Alle Teilnehmer; n = 140

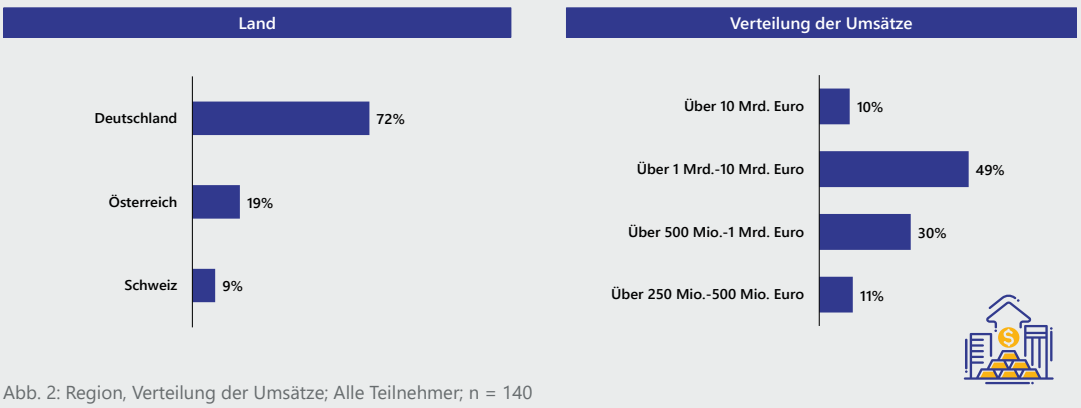


Abb. 2: Region, Verteilung der Umsätze; Alle Teilnehmer; n = 140

# Management Summary

- Die Gefahr, Opfer eines professionellen Cyber-Angriffs zu werden, wird von 82 Prozent der untersuchten Unternehmen als hoch eingestuft. Vor allem in der Industrie wird das Bedrohungspotenzial als überdurchschnittlich hoch angesehen. Gleichzeitig schätzen sich 94 Prozent der Studienteilnehmer jedoch als gut aufgestellt ein, um Hackerangriffe frühzeitig zu erkennen und abzuwehren. Da die Angriffe jedoch immer professioneller werden und Angreifende häufig bereits lange vor dem eigentlichen Angriff im Unternehmen sind, ist es bei einem entdeckten Angriff oft längst zu spät.

- Die größte Sorge haben die Unternehmen vor Ransomware und Phishing-Mails (57 %), vor der Nutzung unautorisierter Geräte (53 %) und DDoS-Attacken (51 %). Tatsächlich hat laut dem Report „Die Lage der IT-Sicherheit in Deutschland 2021" vom Bundesamt für Sicherheit in der Informationstechni (BSI), die Zahl an Ransomware deutlich zugenommen, ebenso wie die Professionalität der DDoS-Attacken, um Lösegeld zu erpressen. Aber auch aufgrund technischer Schulden wie Schwachstellen in den Legacy-Systemen ergibt sich aus Sicht von 48 Prozent der Befragten die Gefahr schwerwiegender Angriffe auf die IT-Infrastruktur und die Daten.

- Auffällig an den Antworten im Rahmen der Studie ist, dass ein Drittel (33 %) der Unternehmen bisher noch keine regelmäßigen Statusmessungen der IT-Security vornimmt. Immerhin planen 24 Prozent, dies in den kommenden Jahren anzugehen – bleiben 9 Prozent, die eine regelmäßige IT-Security-Statusmessung auch in Zukunft nicht für relevant erachten. Auch die Überprüfung des Security-Status mittels Pentesting wird zurzeit nur von 54 Prozent der Unternehmen regelmäßig vorgenommen.

- Infolge zunehmender Digitalisierung der Kundenschnittstellen und unternehmensübergreifender Geschäftsmodelle (z. B. Industrie 4.0, IoT) enden IT-Security-Strategien in 59 Prozent der befragten Unternehmen nicht mehr an den eigenen Unternehmensgrenzen, sondern beziehen sich auf das gesamte Ökosystem. Vor allem die Unternehmen aus den Branchen Automotive und Manufacturing betrachten IT-Security deutlich häufiger als unternehmensübergreifenden Ansatz.

**82 %**

stufen die Gefahr eines Cyber-Angriffes als hoch ein.

**57 %**

sehen Ransomware und Phishing-Mails als größte Gefahr.

**54 %**

nutzen Pentesting für die Überprüfung des Security-Status.

**59 %**

sehen IT-Security als unternehmens-übergreifenden Ansatz.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

- Auch durch den stetig wachsenden Softwareanteil in Produkten nehmen die Sicherheitsanforderungen während der Produktnutzung zu. Dabei geht es beispielsweise um den Schutz kundenbezogener Daten, aber auch um die Vernetzung digitaler Produkte mit der Unternehmens-IT. Die Angriffsfläche wird somit größer. Allerdings findet Security by Design bisher nur bei 43 Prozent der befragten Unternehmen im Design digitaler Produkte Berücksichtigung.

- Die Cloud spielt für die Bewertung der IT-Sicherheit eine wichtige Rolle. 96 Prozent der untersuchten Unternehmen verfügen bereits über eine Cloud-Strategie beziehungsweise werden bis 2023 eine klare Cloud-Strategie entwickelt und umgesetzt haben. Aus der zunehmenden Cloud-Nutzung ergibt sich aus Sicht von 61 Prozent der Befragten zwar eine Erhöhung des IT-Sicherheitsniveaus, aber auch gleichzeitig die Notwendigkeit, in die IT-Sicherheit und den Aufbau einer ganzheitlichen IT-Sicherheitsarchitektur zu investieren.

- Infolge der zunehmenden Bedrohungslage, aber auch aufgrund einer Cloud Governance steigen die Budgets für IT-Security in den kommenden zwei Jahren teilweise sehr stark an. Die größten Zuwächse finden sich im Bereich des Identifizierens von Schwachstellen: 76 Prozent der befragten Unternehmen werden ihre Budgets für die Früherkennung potenzieller Cyber-Risiken und -Angriffe um bis zu 10 Prozent erhöhen. Den zweiten großen Block für Budgeterhöhungen bildet die Prävention, also die Antizipation und Abwehr von Cyber-Angriffen. Hier wollen 15 Prozent ihre Ausgaben sogar um mehr als 10 Prozent steigern.

- Mit zunehmender strategischer Relevanz von IT-Security im Kontext der Digitalisierung bei gleichzeitig steigender Bedrohungslage müssen IT-Security-Aufgaben immer professioneller erbracht werden. Das geht allerdings in einem großen Teil der Unternehmen nicht allein aus eigener Kraft: Über 40 Prozent sehen rund um IT-Security einen hohen Bedarf an externen Dienstleistungen. Managed Services gewinnen dabei an Bedeutung: Während 25 Prozent der Unternehmen bereits Managed Security Services nutzen, planen weitere 59 Prozent, in Zukunft Security-Aufgaben auszulagern. Vor allem E-Mail-Security, Identity & Access Management und Endpoint Security sind beliebte Themen für die Vergabe an einen Managed Security Service Provider.

**Nur 43 %**

berücksichtigen Security-by-Design bei der Softwareeinführung.

**96 %**

verfügen bereits über eine Cloud-Strategie bzw. führen diese bis 2023 ein.

**10 % mehr Budget**

für die Bereiche Früherkennung und Prävention von Cyber-Angriffen

**25 %**

der Unternehmen nutzen bereits Managed Security Services.

# Unternehmen im Fokus von Cyber-Kriminalität

Cyber-Kriminalität hat sich mit fortschreitender Digitalisierung zu einer der größten Bedrohungen für Unternehmen entwickelt. Laut dem Report „Die Lage der IT-Sicherheit in Deutschland 2021" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wurde im Jahr 2021 eine deutliche Ausweitung cyberkrimineller Erpressungsmethoden registriert. Vor allem die Zahl der Schadsoftware-Varianten ist um 144 Millionen neue Varianten weiter gestiegen. Auffällig war auch die steigende Anzahl professioneller Angriffe durch Bot-Netzwerke und Sicherheitslücken in Microsoft Exchange. Bots werden beispielsweise für das Ausspionieren persönlicher Informationen, aber auch für die Verbreitung weiterer Schadprogramme von infizierten Rechnern aus genutzt.

**144 Mio.**
neue Schadsoftware-Varianten wurden im Jahr 2021 registriert.

Eine große Angriffswelle gab es im Dezember 2021 durch eine Sicherheitslücke in der Protokollierungsbibliothek für Java-Anwendungen, besser bekannt unter Log4j. Diese Sicherheitslücke gilt als eine der größten bisher entdeckten Schwachstellen in der Geschichte des Internetzeitalters. Besonders bedrohlich war, dass sich Hackerinnen und Hacker sehr einfach Zugang zu den Servern und Daten verschaffen und massiv Daten abziehen konnten.

Dieses Beispiel zeigt exemplarisch, dass Hackerangriffe Unternehmen mitten in ihre Lebensader treffen und das Potenzial haben, Teile der Systeme und Prozessketten für eine gewisse Zeit stillzulegen.

Die Cyber-Gefahr kommt von immer mehr Seiten – von innen wie auch von außen – und die Angriffe verfolgen sehr unterschiedliche Ziele. Während es kriminellen Organisationen darum geht, die Server ihrer Ziele in ihre Gewalt zu bekommen und Lösegeld zu erpressen, wollen Staaten oder Wettbewerber beispielsweise an sensible Informationen gelangen oder ganz gezielt konkurrierenden Unternehmen schaden. So berichteten im vergangenen Jahr einige Pharma-Unternehmen, die in der Corona-Krise an Impfstoffen gearbeitet haben, von einer massiven Zunahme an Cyber-Angriffen – vermutlich mit dem Ziel, an Forschungsergebnisse zu kommen oder die Produktion lahmzulegen und die Unternehmen damit zu erpressen. Auch Hersteller von Medizintechnik sind häufiger Cyber-Angriffen ausgesetzt. Die Angriffe finden auch immer intensiver und professioneller von Hackergruppen aus Osteuropa, Russland, China oder Nordkorea statt, vor allem auf industrielle Ziele.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Aber auch von den Beschäftigten der Unternehmen selbst gehen mit zunehmender digitaler Kommunikation Gefahren aus – häufig unbewusst durch immer professionellere Phishing-Kampagnen oder durch die Nutzung privater Endgeräte innerhalb der Unternehmensnetzwerke. Laut einer Studie des Digital- und IT-Branchenverbandes Bitkom beginnt der Großteil der Angriffe mit dem sogenannten Social Engineering, worunter die Manipulation von Beschäftigten verstanden wird. Die Angreifenden gehen dabei sehr strukturiert vor und versuchen unter anderem durch gefälschte E-Mails oder Telefonanrufe an sensible Daten wie Passwörter zu gelangen. Besonders „beliebt" sind Phishing-Mails und CEO-Fraud.

Im Grunde sind Cyber-Attacken wie militärische Angriffe über mehrere Stufen strukturiert. So suchen sich Angreifende zunächst ihre Ziele aus („identify the targets") und wählen die passenden Angriffswerkzeuge (z. B. Malware) aus. Anschließend wird, beispielsweise über Social Engineering, Malware verteilt und sich Zugang zum Ziel verschafft, indem beispielsweise Mitarbeiter oder Mitarbeiterin Phishing-Mails öffnen. Ihre Wirkung erzielt die Schadsoftware aber erst dann, wenn sie auch tatsächlich auf technische Schwachstellen trifft. Erst dann erfolgt die Installation der Schadsoftware und das Warten auf den passenden Zeitpunkt für den Angriff. Cyber-Angriffe passieren häufig dann, wenn sie einen möglichst hohen Schaden anrichten – beispielsweise wenn Online-Aktionen geplant sind, im Saisongeschäft oder wenn größere Events wie Hauptversammlungen angekündigt werden. Die Folge: Unternehmen wiegen sich oft in trügerischer Sicherheit, obwohl Cyber-Kriminelle längst in ihre IT-Systeme vorgedrungen sind und unbemerkt Schadsoftware installieren konnten.

Eine gefühlte Sicherheit entsteht häufig auch dadurch, dass zwar entsprechende organisatorische, technologische und prozessuale Maßnahmen wie 2-Faktor-Identifizierung, Aufbau von Security Operation Centers, die Einführung einer Cloud Security Governance oder Security-Monitoring-Systeme eingeführt sind; in einer digitalisierten und global vernetzten Welt reichen diese Maßnahmen jedoch nicht mehr aus. Die großen Hackerangriffe der jüngeren Vergangenheit zeigen, dass sich Unternehmen viel stärker auf das frühzeitige Identifizieren möglicher Cyber-Angriffe fokussieren sollten.

# Größere Bedrohungslage im digitalen Zeitalter

Gleich zu Beginn der Studie tut sich ein erstes Spannungsfeld auf: 37 Prozent der Befragten schätzen die Bedrohungslage, dass ihr Unternehmen Opfer eines Cyber-Angriffs werden kann, als sehr hoch ein, weitere 45 Prozent noch als eher hoch. Unter dem Eindruck der größeren IT-Sicherheitslücken, die sich in den letzten Jahren aufgetan haben, ist diese Sichtweise auch gut nachvollziehbar. Nur 18 Prozent gehen von einer geringen Bedrohungslage aus. Etwas sicherer fühlen sich die Befragten aus dem Mittelstand – also aus Unternehmen mit weniger als 1 Milliarde Euro Umsatz: Von ihnen schätzen 28 Prozent die Bedrohungslage für ihr Unternehmen als gering ein, während neun von zehn der Befragten aus Unternehmen mit mehr als 1 Milliarde Euro Umsatz ein hohes Gefährdungspotenzial wahrnehmen.

## DIE BEDROHUNGSLAGE, OPFER EINES HACKERANGRIFFS ZU WERDEN, WIRD VON DEN MEISTEN UNTERNEHMEN ALS HOCH EINGESCHÄTZT

**Wie schätzen Sie aktuell die Bedrohungslage für Ihr Unternehmen ein, Opfer eines professionellen Hackerangriffs zu werden?**

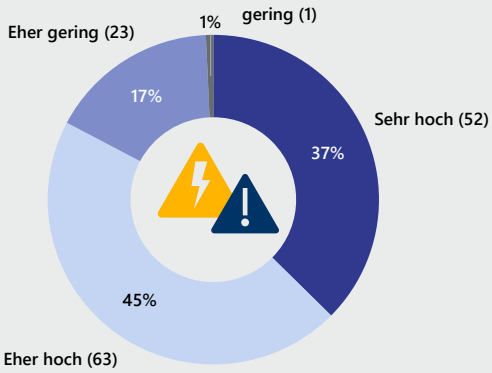


Abb. 3: Frage: Wie schätzen Sie aktuell die Bedrohungslage für Ihr Unternehmen ein, Opfer eines professionellen Hackerangriffs zu werden?; Alle Teilnehmer; Häufigkeitsverteilung; n = 139

## GROSSE SORGE BESTEHT VOR PROFESSIONELLEN HACKERANGRIFFEN

Eine besonders große Gefahr geht laut den Befragten von Ransomware/Phishing-E-Mails (67 %) und der Nutzung unautorisierter Devices (63 %) aus. Der Faktor Mensch ist somit aus Sicht der befragten IT- und Security-Verantwortlichen eines der größten Sicherheitsrisiken. Tatsächlich erfolgen laut Microsoft Security Report 2021 über zwei Drittel der Cyber-Angriffe durch Social Engineering, also den Versand täuschend echt anmutender E-Mails

(Phishing-Mails) an Mitarbeitende, um diese dazu zu bringen, unabsichtlich Schadsoftware zu nutzen. Die Angriffsmethoden sind mittlerweile sehr ausgereift und reichen von Phishing-Mails bis hin zum CEO-Fraud. Dabei verfolgen die Angreifer bei solchen Kampagnen das Ziel, die Mitarbeitenden mit täuschend echten Mails und Webseiten zu manipulieren und die Cyber-Schutzwälle zu überwinden. Bereits an dieser Stelle zeigt sich, dass IT-Security nicht nur rein technologisch betrachtet werden darf.

**Zwei Drittel**
der Cyber-Angriffe erfolgt über Phishing-Mails an Mitarbeitende.

61 Prozent der Befragten befürchten ferner, dass DDoS-Attacken (Distributed-Denial-of-Service-Attacke) schwerwiegende Folgen für ihre Unternehmen haben können. Tatsächlich zielen diese Angriffe darauf ab, die Geschäftsaktivitäten der Opfer lahmzulegen oder Daten abzugreifen und sie dadurch massiv zu schädigen. Das BSI warnt regelmäßig vor einer deutlichen Zunahme von Lösegelderpressungen. DDoS-Angriffe kommen zwar im Vergleich zu Phishing-Angriffen seltener vor, dennoch ist der durch sie verursachte Schaden deutlich größer, wie einige Fälle in den letzten Jahren gezeigt haben. Bei einem DDoS-Angriff wird ein Online-Dienst mit großen Mengen an Daten geflutet und somit gestört, sodass kein Benutzerzugriff mehr möglich ist. Dazu werden in der Regel mehrere Rechner beziehungsweise IT-Systeme infiltriert und mit Malware infiziert, sodass gesamte Prozessketten lahmgelegt werden. Daher ist die Sorge vor DDoS-Attacken besonders hoch.

48 Prozent der Befragten halten es darüber hinaus für wahrscheinlich, dass aufgrund von technischen Schwachstellen in den IT-Systemen – sogenannte technische Schulden – Sicherheitslücken genutzt werden, um unbemerkt an die Server und Daten vorzudringen. Da viele Unternehmen über einen hohen Anteil historisch gewachsener IT-Legacy verfügen, ist dieser Aspekt in den letzten Jahren mit zunehmender Digitalisierung und der damit verbundenen Anbindung an das Internet zu einem großen Problem geworden. Problematisch sind hier vor allem veraltete Codes und Mängel im Design und in der Konfiguration, wodurch sich für professionelle Hackerinnen und Hacker Angriffsziele ergeben. Vor allem in den befragten mittelständischen Unternehmen sehen überdurchschnittliche viele Befragte (57 %), dass Schwachstellen in den IT-Systemen es leichter machen, in die Systeme vorzudringen. Unter den Unternehmen mit mehr als 1 Milliarde Euro Umsatz sind nur 41 Prozent der Befragten dieser Auffassung.

Trotz dieser Vielzahl an möglichen Angriffsszenarien hält ein großer Teil der Befragten ihre eigenen Unternehmensnetzwerke für ausreichend abgesichert. Nur 33 Prozent sehen Schwachstellen in der Absicherung und Kontrolle ihrer Netzwerke als mögliche Ursache von Cyber-Angriffen. Allerdings deuten die Antworten auch darauf hin, dass in einigen Branchen die Unternehmensnetzwerke als nicht so sicher eingeschätzt werden. So sehen 45 Prozent der Befragten aus Automotive-Unternehmen und sogar 60 Prozent derjenigen aus der Manufacturing-Industrie ihre Unternehmensnetzwerke als unzureichend

abgesichert. Interessanterweise wird in diesen beiden Branchen auch die Gefahr von Insider-Bedrohungen von deutlich mehr Unternehmen als höher angesehen als im Durchschnitt aller untersuchten Branchen. Demnach halten 61 Prozent der Befragten von Automotive-Unternehmen und 50 Prozent derjenigen von Manufacturing-Unternehmen Datendiebstähle durch (ehemalige) Mitarbeitende oder Geschäftspartnerinnen und Geschäftspartner für wahrscheinlich.

## EIN GROSSER TEIL DER BEFRAGTEN RECHNET MIT CYBER-ATTACKEN AUF IHR UNTERNEHMEN

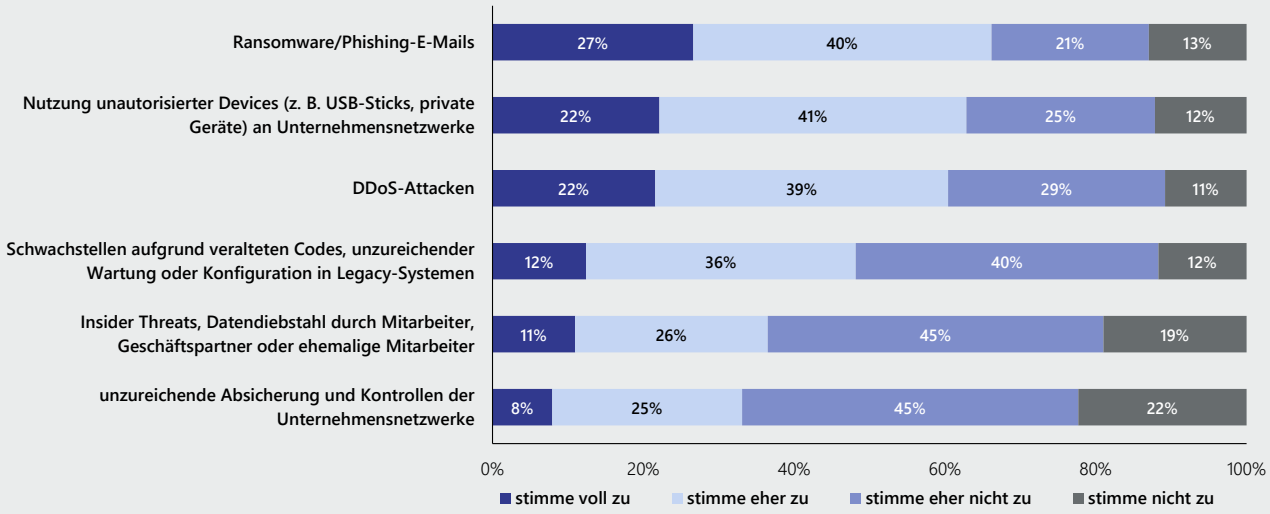


Abb. 4: Frage: Für wie wahrscheinlich halten Sie es, dass Ihr Unternehmen in den kommenden zwei Jahren aufgrund der folgenden Ereignisse einem schwerwiegenden Angriff zum Opfer fällt, durch....?; Alle Teilnehmer; Häufigkeitsverteilung: n = 137

## EINSCHÄTZUNGEN ZU DEN FOLGEN VON CYBER-ANGRIFFEN

Welche Folgen haben Hackerattacken für die befragten Unternehmen? Diese Frage sollte im Anschluss an die Frage nach den Gefährdungsquellen evaluiert werden. Nur 6 Prozent gehen im Falle eines Cyber-Angriffs von einem geringen Schaden aus (siehe Abbildung 6). 94 Prozent erwarten demnach eine ganze Reihe an Konsequenzen – teilweise mit erheblichen Business Impact wie die Störung von Liefer- und Produktionsketten oder Datendiebstahl.

Am häufigsten – von 87 Prozent der Befragten – wurden hohe Image- und Reputationsschäden als Konsequenz von Hackerangriffen genannt. Vor allem die Befragten aus den Sektoren Automotive, Handel, Manufacturing und Telekommunikation/Medien/Verlage waren überdurchschnittlich häufig dieser Meinung.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

75 Prozent der Unternehmen befürchten ferner den Abfluss von Kundendaten. Besonders in Branchen, die sehr viele Daten von Endkonsumentinnen und -konsumenten sammeln, wie Konsumgüterhersteller (84 %) und Telekommunikation/Medien/Verlage (90 %), aber auch in der Manufacturing-Industrie bestehen überdurchschnittlich häufig Befürchtungen, dass Kundendaten infolge von Cyber-Angriffen verloren gehen können. Grundsätzlich ist der Schutz von Kundendaten spätestens seit der EU-DSGVO-Gesetzgebung ein besonders hohes Gut, das es zu schützen gilt – vor allem je stärker sich Unternehmen mit digitalen Geschäftsmodellen der Online-Welt öffnen und Kunden ihre Daten in Cloud-Umgebungen hinterlassen.

**75 %**

sehen den Abfluss von Kundendaten als große Bedrohung von Cyber-Angriffen.

Dass kritische Unternehmensdaten – beispielsweise Patente, Produktinformationen oder Finanzdaten – von Hackern erbeutet werden, ist eine Sorge, die immerhin 73 Prozent der Befragten teilen. Im Zusammenhang mit Datendiebstahl stehen häufig auch Lösegeld-erpressungen – die auch laut BSI im Jahr 2021 enorm zugenommen haben. 58 Prozent der Befragten bewerten die Gefahr von Lösegeldforderungen als hoch. Überdurchschnittlich häufig sehen die Befragten aus den Branchen Automotive, Energie, Handel und Telekommunikation/Medien/Verlage eine Gefährdung durch Lösegelderpressung.

### EINE MEHRHEIT BEFÜRCHTET UMSATZEINBUSSEN AUFGRUND VON CYBER-ANGRIFFEN

Der Ausfall von Produktionsanlagen verbunden mit Umsatzeinbußen ist ein Thema, das nur für produzierende Unternehmen relevant ist; daher wurde auch nur den Teilnehmenden aus solchen Unternehmen die Frage gestellt, inwieweit sich Cyber-Angriffe auf die Produktion auswirken.

Aus Sicht von 67 Prozent der untersuchten Industrieunternehmen würde sich ein Cyber-Angriff unmittelbar auf die Produktionsprozesse – also die Operational Technology (OT) – auswirken. Tatsächlich steht die OT mit zunehmender Digitalisierung der Produktentwicklungs- und Fertigungsprozesse besonders im Fokus, da einerseits Produkte wie Maschinen, Werkzeuge, aber auch Transportfahrzeuge einen immer größeren Softwareanteil (Embedded Systems) aufweisen und andererseits die OT im Zuge von IoT-basierten Prozessen immer stärker mit den Backend-IT-Prozessen vernetzt wird, wodurch sich neue Angriffspunkte ergeben.

Ebenso hat das hohe Wachstum der mit dem Internet verbundenen Dinge und Objekte (IoT) Sicherheitslücken in sehr vielen Unternehmen offengelegt – vor allem im Bereich der kritischen OT-Prozesse, denn im Zuge der Industrie 4.0 wird die OT sukzessive in der Cloud abgebildet (Digital Twin) und OT und IT vernetzen sich immer stärker. Dadurch ergeben sich neue Angriffspunkte auf kritische Infrastrukturen und Produktionsstätten, was zur Folge hat, dass die Security-Architekturen angepasst werden müssen. Die Bedrohung

der Produktionsprozesse sehen vor allem die befragten Industrieunternehmen aus den Sektoren Automotive (75 %) und Manufacturing (95 %).

Korrespondierend hierzu zeigt die Lünendonk®-Studie „Der Markt für Engineering Services in Deutschland", für die überwiegend Industrieunternehmen befragt wurden, dass die OT-/IT-Vernetzung für 53 Prozent der befragten Unternehmen derzeit neben der digitalen Produktentwicklung eine der größten Herausforderungen der digitalen Transformation darstellt. Vor diesem Hintergrund ist für 43 Prozent Cyber Security eines der Top-Technologiefelder der nächsten zwei Jahre.

## EXKURS: DIGITALISIERUNG DER OPERATIONAL TECHNOLOGY FÜHRT UNTER ANDEREM ZU INVESTITIONEN IN CYBER SECURITY

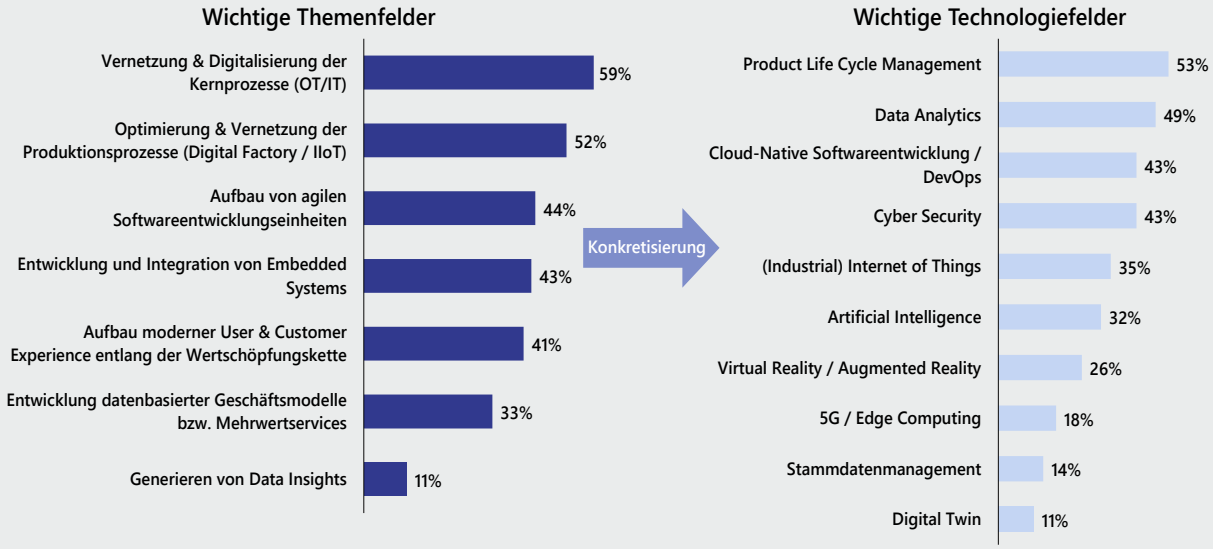


Abb. 5: Frage: Was sind in den kommenden zwei Jahren die Themenfelder / Technologiefelder, mit denen sich Ihr Unternehmen im Engineering beschäftigt?; Alle Teilnehmer; Häufigkeitsverteilung; n = 100
Quelle: Lünendonk-Studie®: "Der Markt für Engineering Services in Deutschland", Oktober 2021

Ebenfalls große Sorge haben 63 Prozent der Unternehmen bezüglich möglicher Umsatzeinbußen durch die Nichteinhaltung von Lieferverpflichtungen, wenn es infolge von Cyber-Attacken zu Ausfällen in den Lieferketten kommt. Auch hier teilen die Befragten aus den Branchen Automotive (85 %), Manufacturing (78 %) und Handel (70 %) signifikant häufiger die Befürchtung. 37 Prozent der Befragten stimmen dagegen nicht zu, dass Hackerangriffe das Potenzial haben, die Lieferketten empfindlich zu stören. Überdurchschnittlich viele aus den Branchen Chemie/Pharma (40 %) und Energie (68 %) halten Umsatzeinbußen aufgrund von Störungen in den Lieferketten durch Cyber-Angriffe dagegen eher für unwahrscheinlich.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Bei der Bewertung dieser Einschätzungen geht es aus Sicht von Lünendonk weniger um die Gefahr einer Störung der Lieferketten als solche, sondern eher um die Vertragsbedingungen bei Nichterfüllung von Lieferungen.

### NEBEN IMAGE- UND REPUTATIONSSCHÄDEN BEFÜRCHTEN DIE UNTERNEHMEN VOR ALLEM DEN ABFLUSS VON DATEN

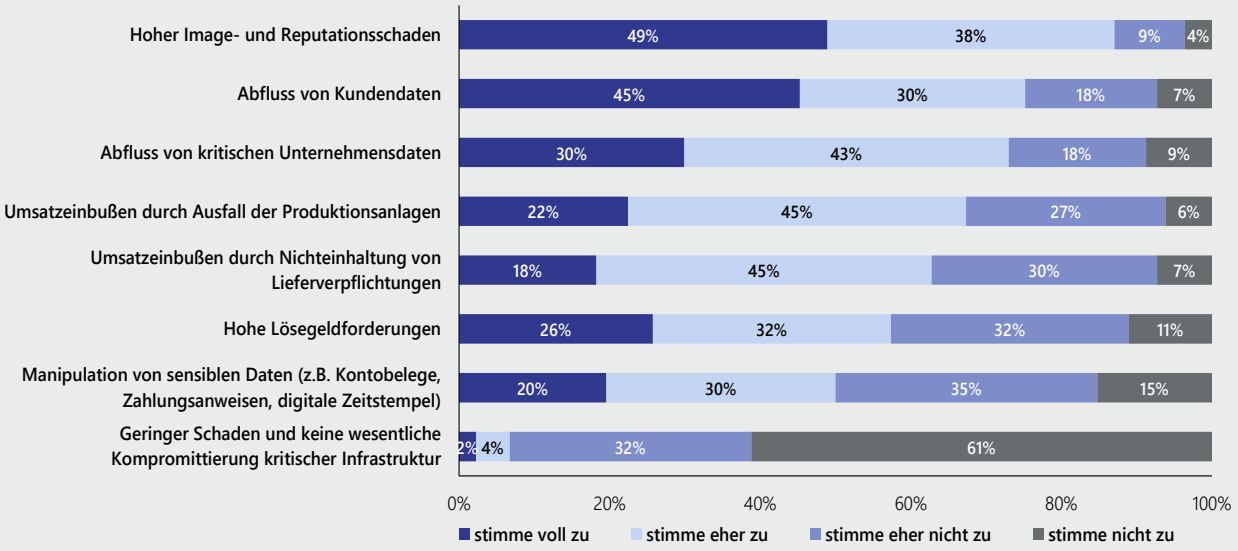


Abb. 6: Frage: Welche konkreten Folgen hätte aus Ihrer Sicht ein Cyber-Angriff für Ihr Unternehmen?; Alle Teilnehmer; Häufigkeitsverteilung; n = 98

### WIDERSPRUCH: UNTERNEHMEN FÜHLEN SICH DURCH CYBER-ANGRIFFE BEDROHT, ABER GLEICHZEITIG GUT AUFGESTELLT, UM DIESE ZU ERKENNEN UND ABZUWEHREN

Während 82 Prozent der Befragten zwar eine hohe bis sehr hohe Bedrohungslage durch mögliche Cyber-Angriffe wahrnehmen, sehen 94 Prozent ihre Unternehmen gut gegen entsprechende Angriffe geschützt und damit mit einer sehr hohen Kompetenz ausgestattet, Bedrohungen durch Hackerangriffe frühzeitig zu identifizieren und ihre Unternehmensnetzwerke zu schützen. Etwas geringer ist das Security-Level in den untersuchten Unternehmen aus dem Sektor Telekommunikation/Medien/Verlage: Von diesen sehen sich nur 85 Prozent gut gegen Cyber-Angriffe gerüstet.

Vergleicht man Konzerne mit mehr als 1 Milliarde Euro Umsatz und mittelständische Unternehmen mit Umsätzen zwischen 250 Millionen und 1 Milliarde Euro, wird deutlich, dass der Mittelstand sich etwas schlechter gegen Cyber-Risiken aufgestellt sieht als die größeren Konzerne. Während 51 Prozent der Befragten aus Konzernen mit über 1 Milliarde

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Euro Umsatz ihren Unternehmen eine sehr hohe Security-Kompetenz zusprechen, sind es bei den mittelständischen Unternehmen nur 37 Prozent.

Eine mögliche Erklärung für die positive Einschätzung zur Kompetenz, Cyber-Angriffe zu erkennen und abzuwehren, ist, dass sich diese Kompetenzwahrnehmung auf diejenigen Cyber-Vorfälle bezieht, die auch tatsächlich entdeckt werden. Die Frage ist jedoch vielmehr, wie schnell die Reaktion auf entdeckte Angriffe erfolgt. Tatsächlich sind Angreifenden oft lange Zeit unbemerkt in den IT-Systemen, spähen diese nach lukrativen Schwachstellen und geeigneten Angriffszeitpunkten aus und installieren beispielsweise Ransomware, um Lösegeld für blockierte Systeme zu erpressen. Wenn der eigentliche Angriff erkannt wird, ist der Schaden in der Regel längst entstanden. So hat die Zahl an Ransomware-Attacken 2021 laut BSI stark zugenommen, was auf verwundbare IT-Systeme schließen lässt Möglicherweise wiegen sich hier viele der in der Studie untersuchten Unternehmen in einer trügerischen Sicherheit bis zum nächsten (unbemerkten) Angriff.

### TRÜGERISCHE SICHERHEIT ENTGEGEN DEM BEDROHUNGSPOTENZIAL: DIE CYBER-RESILIENZ WIRD HOCH EINGESCHÄTZT UND UNTERNEHMEN SEHEN SICH POTENZIELLEN ANGRIFFEN GEGENÜBER GUT AUFGESTELLT

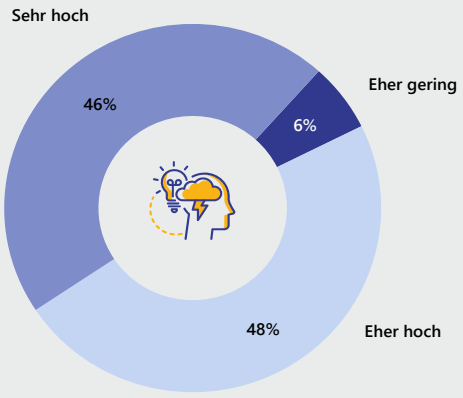


Abb. 7: Frage: Wie schätzen Sie die Fähigkeit Ihres Unternehmens ein, Bedrohungen durch Hackerangriffe zu identifizieren und somit eine Früherkennung von Cyberangriffen zu gewährleisten?; Alle Teilnehmer; Häufigkeitsverteilung; n = 140

# Mehr Innovation durch Cloud-Nutzung – und auch mehr Sicherheit?

Immer mehr Unternehmen entscheiden sich für eine Modernisierung ihrer IT-Landschaft und den Umbau zu einer Cloud-Infrastruktur. Ein wesentlicher Treiber dafür sind die veränderten Anforderungen an die IT bei der Umsetzung von Digitalisierungsstrategien – insbesondere von digitalen und datenbasierten Geschäftsmodellen, aber auch bei der intelligenten Automatisierung und Steuerung von Geschäftsprozessen. Vor allem die Zusammenführung und Auswertung von Daten ist eine zentrale Voraussetzung für die nachhaltige Umsetzung von Digitalstrategien, weshalb Themen wie Skalierbarkeit, Verfügbarkeit, Flexibilität und Interoperabilität besonders im Fokus stehen. Traditionelle Legacy-Anwendungen stoßen allerdings bei diesen Anforderungen an ihre Grenzen, weshalb Unternehmen immer häufiger auf Cloud-Dienste setzen.

**70 %**

wollen im Jahr 2022 ihre Budgets für die Cloud-Transformation erhöhen.

### EXKURS: CYBER SECURITY IST EIN ZENTRALES DIGITALISIERUNGSTHEMA

Die Lünendonk®-Studie 2021 „Der Markt für Digital Experience Services in Deutschland“ zeigt, dass für 49 Prozent der Unternehmen 2022–2023 die Cloud-Transformation, also der Umbau von Teilen der IT-Landschaft zu einer Cloud-native-IT-Architektur, eines der wichtigsten Investitionsthemen ist. 70 Prozent der Unternehmen planen sogar, ihre Budgets für die Cloud-Transformation im Jahr 2022 zu erhöhen – rund jedes zehnte sogar um mehr als 10 Prozent.

Mit Blick auf die kommenden Jahre erwarten laut dieser Studie 53 Prozent der befragten CIOs, dass Software überwiegend als Software as a Service (SaaS) bereitgestellt wird. Da SaaS-Modelle darauf basieren, dass die zugehörige IT-Infrastruktur durch die Softwareanbieter betrieben wird, handelt es sich bei SaaS in der Regel um Public-Cloud-Services. Während 37 Prozent der CIOs davon ausgehen, dass in Zukunft der überwiegende Teil der IT-Services in einer Cloud-Umgebung bereitgestellt wird, sind sich weitere 31 Prozent der CIOs diesbezüglich noch unschlüssig und stimmen dieser Aussage nur teilweise zu.

### ZWEI VON DREI UNTERNEHMEN HABEN EINE CLOUD-STRATEGIE

Auch in der vorliegenden Studie zeichnet sich ein klarer Trend zur verstärkten Cloud-Nutzung ab. 32 Prozent der untersuchten Unternehmen verfolgen eine Cloud-first-Strategie, prüfen also bei jedem Projekt, ob es sich mithilfe von Cloud-Services umsetzen lässt. Einen besonders hohen Anteil an Unternehmen mit Cloud-first-Strategien lässt sich in den Branchen Automotive (50 %), Chemie/Pharma (45 %) und Manufacturing (40 %) beobachten, was unter anderem mit dem Trend zur Digitalisierung der Produktionsketten im Zuge der Industrie 4.0 und Themen wie digitaler Zwilling und Digital Engineering zusammenhängt.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Da sich aus ganz unterschiedlichen Gründen nicht alle traditionellen IT-Kernsysteme in die Cloud migrieren (Lift & Shift) oder zu Cloud-native-Services umbauen lassen, zeigt sich in der Praxis meist eine hybride IT-Architektur aus den traditionellen IT-Kernsystemen und Cloud-Anwendungen. Eine sogenannte Cloud-too-Strategie, also die Verlagerung einzelner Anwendungen in die Cloud beziehungsweise den Bezug einzelner Anwendungen als Software as a Service, verfolgen 37 Prozent der befragten Unternehmen. Insbesondere im Handel ist dieser Anteil mit 60 Prozent überdurchschnittlich hoch. Weitere 27 Prozent wollen bis zum Jahr 2024 eine Cloud-Strategie entwickelt haben und nur für 4 Prozent ist eine Cloud-Strategie auch in Zukunft keine Option.

### NAHEZU ALLE UNTERNEHMEN VERFOLGEN EINE CLOUD-STRATEGIE

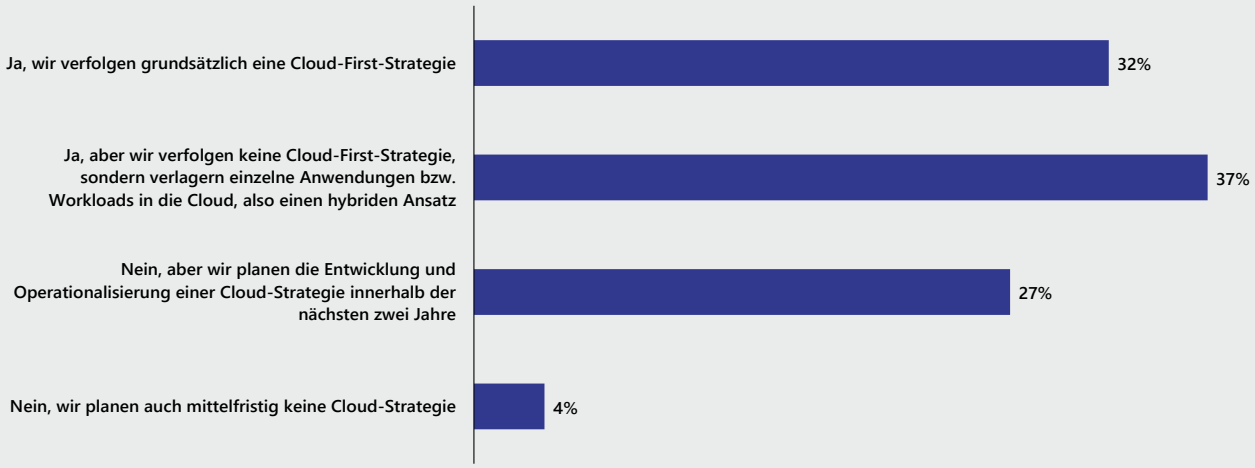


Abb. 8: Frage: Hat Ihr Unternehmen eine Cloud-Strategie?; Alle Teilnehmer; Häufigkeitsverteilung; n = 140

### DER TREND GEHT ZUR PUBLIC CLOUD – ABER GENAU DORT SIND DIE DATEN AUS SICHT EINIGER UNTERNEHMEN NOCH NICHT GUT GENUG GESCHÜTZT

Diejenigen Unternehmen, die bereits über eine Cloud-Strategie verfügen, wurden gefragt, für wie sicher sie ihre Daten in den unterschiedlichen Cloud-Varianten halten. Am sichersten ist aus Sicht der Befragten – wenig überraschend – die Private Cloud. 67 Prozent sehen in der Private Cloud ein sehr hohes Schutzniveau vor Cyber-Angriffen. Nur 9 Prozent erachten ihre Daten in der Private Cloud als nicht sicher.

Ein hohes Schutzniveau ihrer Daten verorten die befragten IT-Entscheiderinnen und –Entscheider auch in der Hybrid Cloud. Allerdings ist der Anteil derer, für die die Hybrid Cloud ein „sehr hohes Schutzniveau" bietet, mit 39 Prozent deutlich geringer als bei der Private Cloud. Dennoch bieten hybride Umgebungen aus Sicht von 51 Prozent

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

der Befragten noch ein „eher hohes Schutzniveau". Allerdings gilt es bei hybriden Umgebungen darauf zu achten, dass keine Tool-Lösungen für die Cloud-Sicherheit zum Einsatz kommen, die sich von denen für lokale Systeme unterscheiden, um die Komplexität im Security Monitoring der hybriden Umgebungen nicht zu stark zu erhöhen.

Hinsichtlich der Datensicherheit in der Public Cloud bestehen in jedem dritten Unternehmen noch Vorbehalte – obwohl vor allem die Cloud-Anbieter in den letzten Jahren enorme Investitionen in die Absicherung ihrer Rechenzentren gegen Cyber-Angriffe getätigt haben. Vor allem die Hyperscaler (AWS, Azure und Google Cloud) investieren laut eigenen Angaben pro Jahr Milliardensummen in die technologische Absicherung ihrer Cloud-Rechenzentren und vor allem in die KI-gestützte Früherkennung und Cyber-Abwehr – Investitionen, die einzelne Kunden in dieser Höhe nicht tätigen können, sodass diese auch Schwierigkeiten haben, mit den Methoden der Hackerinnen und Hacker Schritt zu halten. So hat beispielsweise Google im März 2022 die IT-Sicherheitsfirma Mandiant für 5 Milliarden Euro übernommen. Auch Microsoft hatte Interesse an Mandiant. Im Juli 2021 hat Microsoft aber den IT-Security-Spezialisten RiskIQ für 500 Millionen Dollar gekauft.

**39 %**

stufen hybride Cloud-Umgebungen mit einem sehr hohen Schutzniveau ein.

Aus einer anderen Perspektive betrachtet, vertrauen jedoch sieben von zehn Unternehmen der Public Cloud ihre Daten an – ein Wert, der vor einigen Jahren noch deutlich geringer war. So waren laut der Lünendonk®-Studie „IT-Strategien und Cloud-Sourcing im Zuge des digitalen Wandels" aus dem Jahr 2019 nur 37 Prozent der Unternehmen bereit, Teile ihrer Anwendungen in die Public Cloud zu migrieren. Grundsätzlich spielen hier Narrative bei der Frage nach der Bewertung der Cloud-Sicherheit eine große Rolle und die Öffentlichkeit war in der Vergangenheit – zumindest in Europa – vor allem aus Datenschutzaspekten kritisch gegenüber der Public Cloud eingestellt. Damit kann es sich auch erklären, dass ein so großer Teil der befragten IT-Managerinnen und Manager hybride Umgebungen (also mit einem On-Premise-Anteil) immer noch als sicherer einschätzt als reine Public-Cloud-Angebote.

Zwei Branchen stechen allerdings mit einer überdurchschnittlich hohen wahrgenommenen Datensicherheit in der Public Cloud hervor: 86 Prozent der Befragten aus den Branchen Automotive und Chemie/Pharma bewerten die Datensicherheit in der Public Cloud als hoch.

Die überwiegende Zustimmung der Befragten hinsichtlich der Sicherheit von Unternehmensdaten in der Cloud spiegelt sich auch in der Tatsache wider, dass 61 Prozent der Ansicht sind, dass die Cloud zu einem höheren Sicherheitsniveau führt (Abbildung 10). Unter denjenigen Unternehmen, die eine Cloud-first-Strategie verfolgen, machen sogar 84 Prozent diese Beobachtung, während immerhin noch 48 Prozent der Unternehmen mit einer Cloud-too-Strategie feststellen, dass sich das Security-Level durch einen zunehmenden Cloud-Bezug erhöht.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Unter den untersuchten mittelständischen Unternehmen ist der Anteil derjenigen, die einen Zusammenhang zwischen zunehmender Cloud-Nutzung und höherer Datensicherheit sehen, mit 56 Prozent nicht viel geringer als unter den Befragten aus Konzernen mit mehr als 1 Milliarde Euro Umsatz (64 %).

### IN DER PUBLIC CLOUD SEHEN SIEBEN VON ZEHN BEFRAGTEN IHRE DATEN BEREITS SICHER AUFGEHOBEN

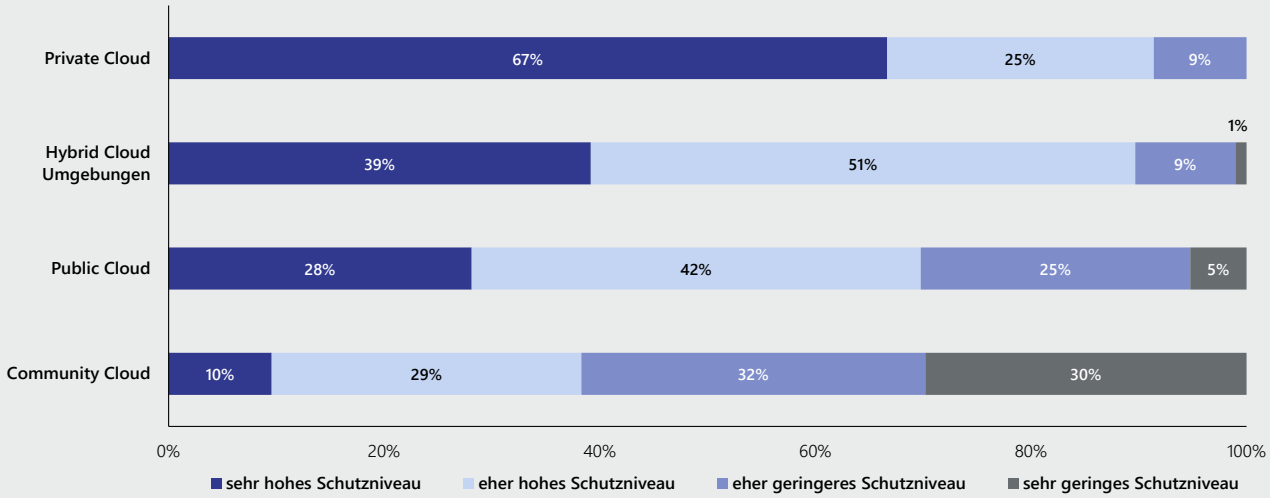


Abb. 9: Frage: Wie schätzen Sie den derzeitigen Schutz Ihrer Daten in den einzelnen Cloud-Deployments ein?; Alle Teilnehmer; Häufigkeitsverteilung: n = 93

### CLOUD-NUTZUNG ERHÖHT DAS SECURITY-NIVEAU – FÜHRT ABER AUCH ZU HÖHEREN INVESTITIONEN IN DIE IT-SICHERHEIT

Welche Folgen hat – über das Thema der Datensicherheit hinaus – der stärkere Bezug von Cloud-Services, zumindest aus Sicht derjenigen Unternehmen, die bereits über eine Cloud-Strategie verfügen? Neben einem Umbau der IT-Architektur zur Nutzung hybrider und multipler Cloud-Services (70 %) sehen 62 Prozent der Befragten die Notwendigkeit, mehr in die IT-Sicherheit zu investieren. Auch laut der "Lünendonk®-Studie 2021: Der Markt für IT-Beratung und IT-Service in Deutschland" planen 86 Prozent der Unternehmen, die Ausgaben für IT-Security im Jahr 2022 zu erhöhen – jedes zweite Unternehmen sogar um mehr als 5 Prozent. Allerdings ist es mehr als fraglich, ob die Unternehmen mit ihren häufig doch begrenzten finanziellen Mitteln in der Lage sind, technologisch so aufzurüsten, dass sie großflächigen, automatisierten Cyber-Angriffen – beispielsweise durch Bot-Netzwerke – etwas entgegensetzen können. So investiert allein Microsoft laut seinem Geschäftsbericht 2021 in den kommenden fünf Jahren etwa 20 Milliarden Dollar in die Sicherheit seiner Cloud-Umgebungen.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

### DIE DURCHDRINGUNG DER CLOUD ERFORDERT EINE UMFASSENDE NEUAUSRICHTUNG DER SECURITY-PROZESSE

Auch wenn sich eine Mehrheit der befragten Unternehmen durch mehr Cloud-Nutzung besser gegen Cyber-Angriffe geschützt sieht als in On-Premise-Umgebungen, hat der Bezug von immer mehr Cloud-Services und Cloud-Architekturen einen hohen Einfluss auf die künftige Security-Architektur. Mit zunehmender Digitalisierungsgeschwindigkeit müssen sich IT-Security-Verantwortliche nun nicht mehr nur auf die Absicherung der IT-Infrastruktur fokussieren, sondern – und das ist tatsächlich ein Game Changer für CIOs und CISOs – sämtliche Geschäftsprozesse betrachten und absichern.

### DIE CLOUD ERHÖHT AUS SICHT VON KNAPP ZWEI DRITTELN DER UNTERNEHMEN DAS SECURITY-NIVEAU

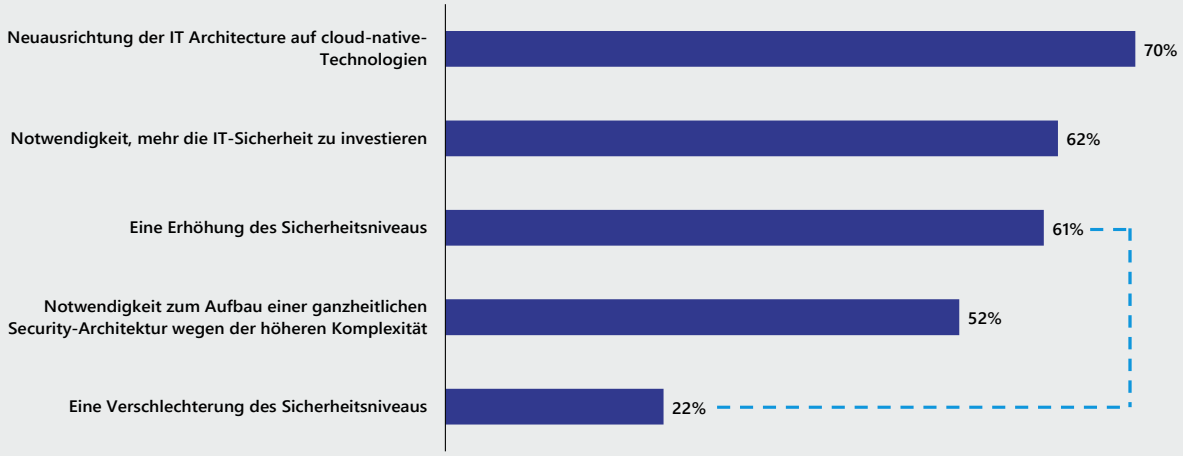


Abb. 10: Frage: Welche Folgen hat Ihrer Ansicht der stärkere Bezug von Cloud-Services für die IT-Sicherheit? Alle Teilnehmer; Häufigkeitsverteilung; n = 140

Neue potenzielle Einfallstore für Hackerinnen und Hacker ergeben sich unter anderem durch schlecht abgesicherte Homeoffice-Netzwerke oder Online-Geschäftsmodelle. Neben der zunehmenden Komplexität, die sich aus hybriden Umgebungen ergeben, und dem stärkeren Bezug von Software as a Service sehen 90 Prozent der Befragten in der Entwicklung digitaler Produkte auf der Basis von Cloud-native-Technologien ein weiteres Security-Risiko. Für ebenso viele führen steigende Sicherheitsanforderungen der Kunden durch die Nutzung digitaler Produkte dazu, dass das Thema „Security by Design“ an Relevanz gewinnt.

Ein weiterer wesentlicher Einflussfaktor für IT-Security ist die aufkommende digitale Plattformökonomie. Für 81 Prozent führt die stärkere Nutzung von cloudbasierten Plattformökosystemen zu einer größeren Bedrohungslage. Unter den Befragten aus den (sehr stark kundenzentrisch ausgerichteten) Branchen Telekommunikation, Medien und

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Verlage sehen sogar 95 Prozent in digitalen Plattformökosystemen eine größere Cyber-Bedrohung. Aber auch in den untersuchten Unternehmen aus der Manufacturing-Industrie sehen 95 Prozent eine größere Bedrohungslage durch digitale Plattformen. Hierauf wird im folgenden Kapitel noch etwas näher eingegangen.

Die Ergebnisse zeigen, dass IT-Security-Verantwortliche eine ganze Reihe von Themen auf der Agenda haben, die alle hoch priorisiert und daher auch gleichzeitig angegangen werden müssen. So wird es einer modernen Sicherheitsarchitektur nicht mehr gerecht, sich nur auf den Schutz der eigenen Unternehmensnetzwerke zu beschränken und die Vernetzung mit anderen Unternehmen im Rahmen von digitalen Geschäftsmodellen nicht zu berücksichtigen. Es wird also mit Blick in die Zukunft darauf ankommen, der CIO- und der CISO-Funktion deutlich mehr Budget, aber auch den Rahmen für notwendige organisatorische, prozessuale und kulturelle Veränderungsmaßnahmen zu geben.

### AUSWIRKUNGEN DER ZUNEHMENDEN CLOUD-NUTZUNG AUF DIE IT-SECURITY

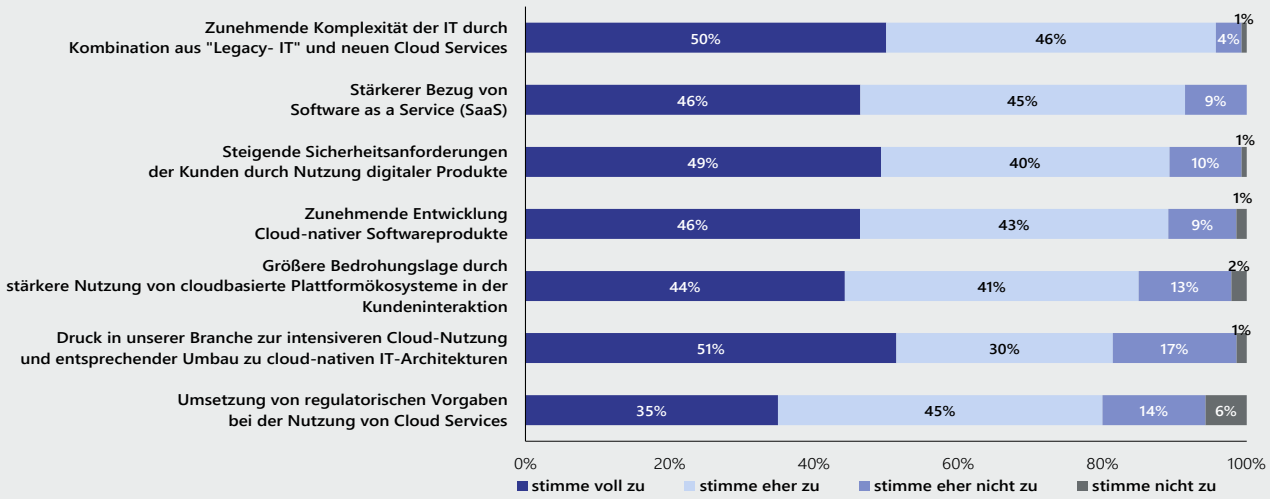


Abb. 11: Frage: Was sind die wesentlichen Einflussfaktoren für IT-Security in Ihrem Unternehmen?; Alle Teilnehmer; Häufigkeitsverteilung; Skala: 1 = kein Einfluss“ bis 4 = „sehr großer Einfluss“; n = 138

# Ausrichtung der Cyber-Security-Strategie auf eine veränderte digitale Welt

Der Schutz vor Cyber-Angriffen ist fester Bestandteil der digitalen Transformation, gilt als wertschöpfend, erfordert aber auch kontinuierliche Attention und Investitionen – so lässt sich die Sichtweise auf Cyber Security in den untersuchten Unternehmen zusammenfassen.

Demnach gilt Cyber Security in 87 Prozent der Unternehmen als Wertschöpfungsfaktor und ist damit ein fester Bestandteil der meisten Digitalisierungs- und Cloud-Strategien. Da sich aus dieser Position heraus aber konsequenterweise auch Investitionen in die IT-Sicherheit ergeben müssen, betrachten 75 Prozent der Befragten Cyber Security gleichzeitig als Kostenfaktor. Besonders häufig wird IT-Security in den produzierenden Unternehmen aus der Automobil- und Manufacturing-Branche (jeweils 93 %) als Wertschöpfungsfaktor und fester Bestandteil der digitalen Transformation und Cloud-Strategie gesehen. In diesen Hochtechnologiebranchen werden die Produktionsanlagen zu einem großen Teil IT-gesteuert und die Vernetzung zu Produktionsverbünden ist stark ausgeprägt. Aber auch in den anderen untersuchten Branchen sehen mindestens 75 Prozent der Befragten IT-Security als wertschöpfendes Element im Rahmen ihrer Digitalprogramme.

**75 %**

der Unternehmen sehen Cyber Security auch als Kostenfaktor.

Ein weiterer interessanter Punkt ist, dass deutlich mehr Befragte aus den mittelständischen Unternehmen (85 %) IT-Security als Kostenfaktor wahrnehmen als aus den Konzernen mit mehr als 1 Milliarde Euro Umsatz (70 %). Diese Diskrepanz zwischen Mittelstand und Großunternehmen mag mit den vergleichsweise limitierten Budgetmöglichkeiten einiger der untersuchten mittelständischen Unternehmen im Vergleich zu großen Konzernen zusammenhängen.

Von denjenigen Unternehmen, die eine Cloud-first-Strategie verfolgen, sehen sogar alle Unternehmen IT-Security als wertschöpfenden Faktor an, gleichzeitig aber auch 87 Prozent als Kostenfaktor. Hieraus ergibt sich die Schlussfolgerung, dass die Cloud zwar grundsätzlich aus Sicht der Mehrheit der Befragten die Datensicherheit erhöht, aber gleichzeitig eben auch hohe Investitionen in die Absicherung der Netzwerke beziehungsweise Ökosysteme erforderlich sind. Unternehmen, die eine Cloud-first-Strategie verfolgen, setzen in der Regel auch auf digitale Geschäftsmodelle und somit auf digitale Kunden-Touchpoints. Wenn Kundinnen und Kunden jedoch ihre Daten in den Online-Systemen hinterlassen sollen, müssen diese sensiblen Kundenportale aber auch entsprechend sicher sein, um Akzeptanz zu gewinnen. Das gelingt durch Zero-Trust-Konzepte und Security by Design, also die Berücksichtigung von IT-Security bereits in der Produktentwicklung und entlang des gesamten Produktlebenszyklus.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

### SECURITY-KONZEPTE MACHEN NOCH OFT AN DEN EIGENEN UNTERNEHMENSGRENZEN HALT

Spätestens seit Ausbruch der Corona-Pandemie investieren Unternehmen in den Aus- oder Aufbau ihrer digitalen Kundenschnittstellen. Im Laufe der Corona-Krise wurde vielen Unternehmen sehr schnell deutlich, dass sie in zahlreichen Bereichen der Digitalisierung enorme Rückstände aufweisen und handeln müssen. Entsprechend hoch waren und sind Investitionen in die Digitalisierung der Marketing- und Vertriebskanäle, in den Aufbau einer digitalen Customer Journey und vor allem in digitale Geschäftsmodelle und Plattformökosysteme. Diese Beobachtung gilt nicht nur für klassische B2C-Branchen wie Handel, Telekommunikation, Medien und Verlage, sondern immer stärker auch für Unternehmen aus dem B2B-Sektor und traditionellen Industriezweigen wie Chemie, Pharma oder dem Maschinenbau, die immer stärker kundenzentrisch und digital agieren.

Aber auch die Umsetzung der Industrie 4.0 gewinnt seit der Corona-Krise an Geschwindigkeit – unter anderem, um an Prozesseffizienz zu gewinnen, Produktentwicklungszeiten zu verkürzen oder Innovationen wie Losgröße 1 und 3D-Druck umzusetzen. Einige Entwicklungen im Zuge der fortschreitenden Digitalisierungen wirken sich in diesem Zusammenhang besonders stark auf die IT-Sicherheit in produzierenden Unternehmen aus:

**58 %**

legen in ihrem gesamten Ökosystem den Fokus auf Cyber-Security.

- Die zunehmende Digitalisierung der Operational Technology (Steuerung von Produktions- und Logistikprozessen) im Zuge der Industrie 4.0 erfordert einen sicheren Zugang zu den Bedienoberflächen von Steuerungsgeräten, beispielsweise im Shop Floor und für Predictive-Maintenance-Anwendungsfälle.
- Der steigende Softwareanteil in Produkten (z. B. Medizintechnik, Automotive, Manufacturing) führt zu einem Anstieg der Entwicklung von Embedded Systems, in denen sich wiederum Security-by-Design-Konzepte wiederfinden müssen.
- IIoT-Plattformen (Industrial Internet of Things) gewinnen als technologische Plattformen für die Vernetzung von Maschinen und Anlagen sowie von Fahrzeugen oder Haushaltsgeräten mehr und mehr an Relevanz. Immer mehr Unternehmen vernetzen ihre Objekte mit Sensoren, um zunächst Daten zu sammeln und später aus historischen Daten Prognosemodelle auf KI-Basis zu entwickeln. Darüber hinaus vernetzen immer mehr Unternehmen ihre Produkte miteinander, um auf der Basis eines Plattformökosystems datenbasierte Geschäftsmodelle anzubieten (Predictive Maintenance, Predictive Monitoring etc.). Damit kann IT-Security nicht mehr nur unternehmensbezogen gedacht werden, sondern muss in einem Kontext von unternehmensübergreifenden Netzwerken betrachtet werden.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Die Befragungsergebnisse zeigen, dass immerhin 58 Prozent der befragten Unternehmen bereits ihr gesamtes Ökosystem in den Fokus der Cyber-Abwehr stellen. Unter den Unternehmen mit einer Cloud-first-Strategie sind es sogar 71 Prozent. Die Betrachtung nach Branchen zeigt, dass vor allem die Unternehmen aus den Sektoren Automotive (70 %), Manufacturing (65 %) und Handel (75 %) besonders häufig ihr gesamtes Ökosystem in die Cyber-Abwehr integrieren. Besonders selten bezieht sich IT-Security dagegen bei den untersuchten Konsumgüterherstellern (20 %) und bei Unternehmen aus den Sektoren Chemie/Pharma (55 %) und Telekommunikation/Medien/Verlage (60 %) auf das gesamte Ökosystem.

### IT-SECURITY HAT SICH ZWAR ZUM WERTSCHÖPFUNGSFAKTOR ENTWICKELT, FINDET ABER NOCH ZU OFT INNERHALB DER EIGENEN UNTERNEHMENSGRENZEN STATT

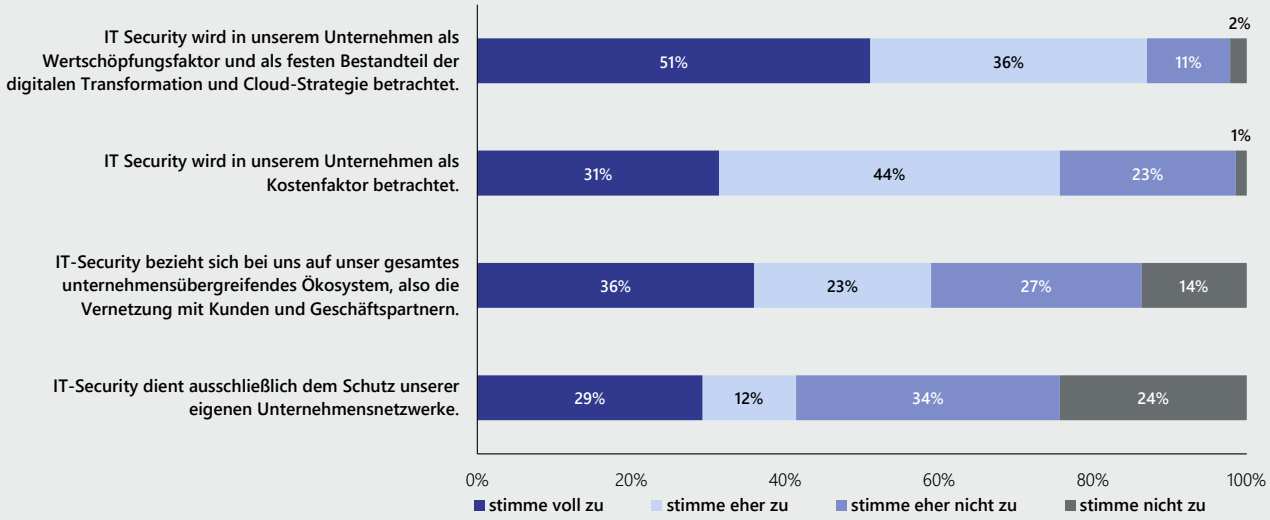


Abb. 12: Frage: Wie wird IT-Security Ihrem Unternehmen wahrgenommen? Alle Teilnehmer; Häufigkeitsverteilung; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll zu"; n = 139

### PLATTFORMÖKONOMIE ERFORDERT NEUE SECURITY-ARCHITEKTUREN

Diejenigen Unternehmen, die IT-Security noch ausschließlich in ihren eigenen Unternehmensgrenzen betrachten, sind zwar in der Minderheit, aber dennoch gefordert, sich den steigenden Security-Anforderungen an digitale und plattformbasierte Geschäftsmodelle zu stellen.

So zeigt die Lünendonk®-Studie „Der Markt für Digital Experience Services in Deutschland", dass acht von zehn Unternehmen auf eine stärkere Vermarktung ihrer Produkte und Dienstleistungen über digitale Absatzkanäle setzen. Ebenso viele Unternehmen planen für 2022, die Entwicklung softwarebasierter Produkte zu forcieren, was in den meisten Fällen mit einer Vernetzung mit externen IT-Systemen und Third-Party-Anwendungen einhergeht.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Ein wesentlicher Grund für die zunehmenden Digitalisierungsprogramme ist die wahrgenommene Bedrohungslage, von der Digitalisierung im Wettbewerb abgehängt zu werden. So fühlen sich 43 Prozent der Unternehmen bereits durch Wettbewerber bedroht, die durch den Einsatz digitaler Technologien (z. B. Cloud, Data Analytics, AI) Wettbewerbsvorteile aufgebaut haben.

### SECURITY BY DESIGN: DIGITALISIERUNG DER KUNDENSCHNITTSTELLEN FÜHRT ZU ERHÖHTEM SCHUTZ VON KUNDEN- UND UNTERNEHMENSDATEN

Zu diesem Zweck investieren Unternehmen intensiver in digitale Produkte wie Kunden-Apps, Online-Portale oder in plattformbasierte Ökosysteme – kurzum in die Digitalisierung der Customer Journey. Tatsächlich planen laut Lünendonk®-Studie „Der Markt für Digital Experience Services in Deutschland" 63 Prozent der Unternehmen den Aufbau neuer Geschäftsmodelle und den Eintritt in neue Märkte durch digitale Lösungen.

**63 %**
planen digitale Lösungen für den Aufbau neuer Geschäftsmodelle.

Immer mehr solcher digitalen Anwendungen (Portale, Apps, Embedded Systems etc.) werden in BizDevOps-Teams (Business, Development, Operations) und auf der Grundlage einer Cloud-native-Architektur entwickelt, woraus sich wiederum hohe Anforderungen an den Schutz der gesammelten personenbezogenen Daten ergeben. Dabei geht es sowohl um den Schutz von sensiblen Kundendaten als auch um die Absicherung digitaler Frontend-Schnittstellen gegen mögliche Hackerangriffe.

Security by Design, also die Berücksichtigung von Security-Elementen bereits während der Produktentwicklung, ist folglich eine wichtige Kernanforderung, die Unternehmen bereits bei der Entwicklung digitaler Produkte und Schnittstellen zu berücksichtigen haben. Dabei geht es unter anderem um eine Minimierung der Angriffsfläche, um den Einsatz von Verschlüsselungstechnologien und um ein wirkungsvolles Identity & Access Management, beispielsweise mithilfe einer 2-Faktor-Authentifizierung.

Aber nicht nur in klassischen Kunden-Frontends spielt Security by Design eine immer wichtigere Rolle. Auch in der Industrie gewinnt dieser Ansatz im Zuge von mehr unternehmensübergreifender Vernetzung, also dem Wandel von Wertschöpfungsketten zu Wertschöpfungsnetzwerken, wie wir sie im Kontext von Industrie 4.0 und IoT erleben, an Relevanz. Laut der Lünendonk®-Studie „Der Markt für Engineering Services in Deutschland" wird der Anteil derjenigen Unternehmen, deren Produkte zu einem überwiegenden Teil auf Software basieren, von 18 Prozent (2021) auf 40 Prozent (2022) ansteigen. Vor allem Unternehmen aus dem Anlagen- und Maschinenbau, der Elektrotechnik und dem Automotive-Sektor gehen von einem höheren Softwareanteil in ihren Produkten aus.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

### EXKURS: DER ANTEIL VON SOFTWAREBASIERTEN PRODUKTEN WIRD IN ZUKUNFT STARK STEIGEN

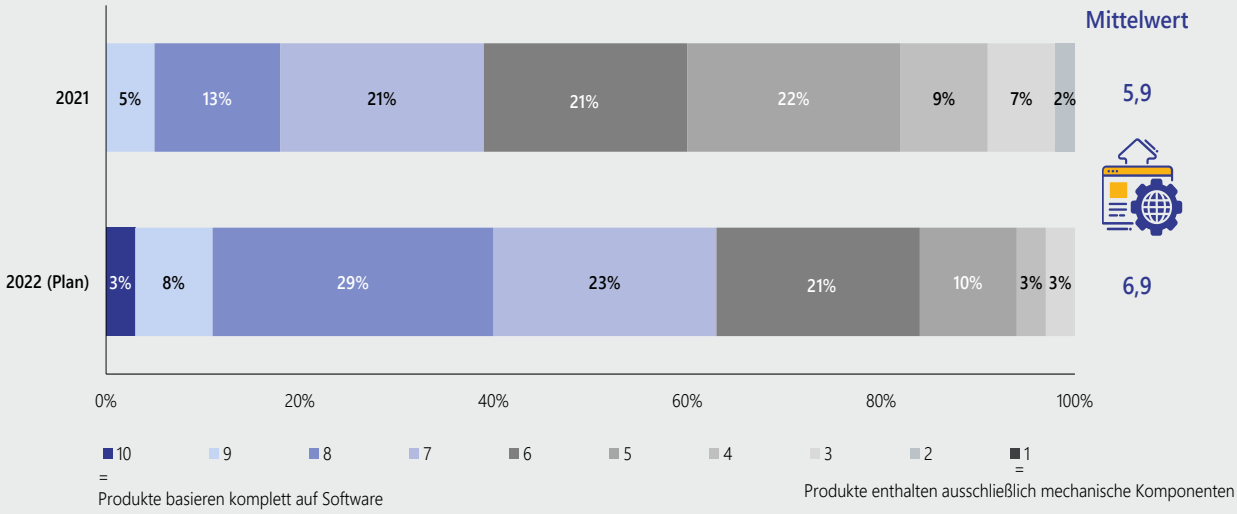


Abb. 13: Frage: Wie schätzen Sie das Verhältnis von Hardware zu Software in ihren Produkten ein?; Skala von 1 = „Unsere Produkte enthalten ausschließlich mechanische Komponenten" bis 10 = „Unsere Produkte basieren komplett auf Software"; Häufigkeitsverteilung; n = 100;
Quelle: Lünendonk®-Studie „Der Markt für Engineering Services in Deutschland".

Allerdings – und das spiegeln die Befragungsergebnisse im Rahmen dieser Studie gut wieder – finden IT-Security-Anforderungen bisher nur bei 43 Prozent der Unternehmen im Design digitaler Produkte Berücksichtigung. Jedoch planen nahezu alle anderen befragten Unternehmen, in Zukunft Security by Design in der Softwareentwicklung als integralen Bestandteil zu berücksichtigen.

Überdurchschnittlich hoch ist der Anteil der befragten Unternehmen, bei denen Security by Design bereits ein fester Bestandteil der Entwicklung digitaler Produkte und Softwarelösungen ist, in den Branchen Handel (53 %) und Telekommunikation/Medien/Verlage (63 %). Unternehmen mit einer Cloud-first-Strategie verfolgen ebenfalls häufiger Security-by-Design-Ansätze (56 %) als die übrigen untersuchten Unternehmen. Das hängt unter anderem damit zusammen, dass diese Unternehmen häufiger Cloud-Architekturen nutzen als solche mit einer eher opportunistischen Cloud-Strategie.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

### SECURITY BY DESIGN IST ALS FESTER BESTANDTEIL BEI DER ENTWICKLUNG VON PRODUKTEN UND SOFTWARELÖSUNGEN GEPLANT

**Ist IT-Security von Anfang an ein fester Bestandteil bei der Entwicklung von digitalen Produkten und Softwarelösungen im Sinne von Security by Design in Ihrem Unternehmen?**

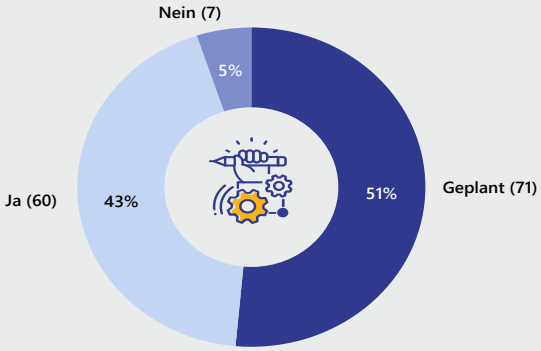


Abb. 14: Frage: Ist IT Security von Anfang an ein fester Bestandteil bei der Entwicklung von digitalen Produkten und Softwarelösungen im Sinne von Security by Design in Ihrem Unternehmen?; Alle Teilnehmer; Häufigkeitsverteilung; n = 138

### WIDERSPRUCH ZUR EIGENEN WAHRNEHMUNG HINSICHTLICH DES SECURITY-LEVELS: EIN DRITTEL DER UNTERNEHMEN ÜBERPRÜFT NICHT REGELMÄSSIG DEN IT-SECURITY-STATUS

Dieses Kapitel hat gezeigt, dass 87 Prozent der befragten Unternehmen IT-Security als Wertschöpfungsfaktor und damit als integralen Bestandteil der digitalen Transformation und der Cloud-Strategie betrachten. Ein Drittel verfolgt sogar eine Cloud-first-Strategie, weitere 37 Prozent einen Cloud-too-Ansatz und sogar 60 Prozent der Unternehmen betrachten den Schutz ihres gesamten unternehmensübergreifenden Ökosystemnetzwerks als integralen Bestandteil ihrer IT-Security-Strategie.

Zur Operationalisierung einer Cloud-Security-Strategie sowie zur Absicherung digitaler Geschäftsmodelle gehört es aber auch, die IT-Security-Strategie und -Prozesse kontinuierlich auf ihre Wirksamkeit hin zu überprüfen. Da es häufig vorkommt, dass sich Angreifende unbemerkt in die IT-Systemen hacken und auf den richtigen Zeitpunkt für einen Angriff warten, sind regelmäßige Security-Reports enorm wichtig. Aber nur sieben von zehn der befragten Unternehmen überprüfen regelmäßig die Wirksamkeit ihrer Cyber-Security-Strategie. Das bedeutet im Umkehrschluss, dass 30 Prozent der teilnehmenden Unternehmen zum Zeitpunkt der Studienerstellung (Frühjahr 2022) den Cyber-Security-Status nicht regelmäßig messen.

Sogar noch seltener werden Penetration-Tests, kurz Pentests, durchgeführt. Nur jedes zweite Unternehmen (54 %) überprüft seine IT-Systeme regelmäßig mithilfe von Pentesting.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Dabei werden die IT-Systeme einem empirischen Sicherheitscheck unter definierten Rahmenbedingungen unterzogen. Die Ergebnisse werden in einem Bericht zusammengefasst und die identifizierten Schwachstellen, Konfigurationsfehler und Best-Practice-Empfehlungen aufgelistet.

Laut den Studienergebnissen führen diejenigen Unternehmen mit einer Cloud-first-Strategie deutlich häufiger Security-Statusmessungen (76 %) und Pentestings (67 %) durch. Dieser höhere Anteil mag damit zusammenhängen, dass Unternehmen mit einer konsequenten Cloud-Strategie eine entsprechende Cloud Governance mit klaren Vorgaben für die Cyber-Security-Prozesse implementiert haben. Regelmäßige szenariobasierte Security-Tests führen sogar nur 38 Prozent und regelmäßige Gap-Analysen nur 39 Prozent der untersuchten Unternehmen durch. Auch hier sind die Cloud-first-Unternehmen deutlich weiter: Jedes zweite Unternehmen mit Cloud-first-Strategie nutzt Red Teaming Exercises und externe Security-Audits.

### FEHLENDE ÜBERPRÜFUNG: EIN TEIL DER UNTERNEHMEN HAT KEINEN ÜBERBLICK ÜBER SEINEN IT-SECURITY-STATUS

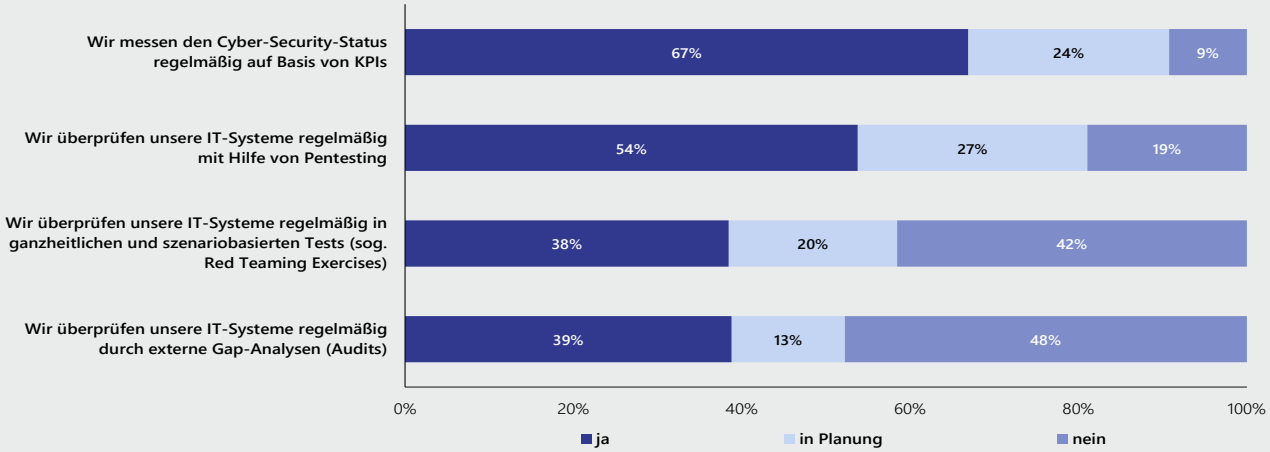


Abb. 15: Frage: Wie überprüfen Sie in Ihrem Unternehmen die Wirksamkeit/Resilienz Ihrer IT-Security?; Alle Teilnehmer; Häufigkeitsverteilung; Skala: 1 = kein Einfluss“ bis 4 = „sehr großer Einfluss“; n = 130

### WIDERSPRUCH ZWISCHEN ANSPRUCH UND WIRKLICHKEIT

Die Ergebnisse lassen den Schluss zu, dass ein signifikanter Teil der befragten Unternehmen derzeit nicht in der Lage ist, Auskunft über ihren jeweiligen Security-Status zu geben – einfach weil keine entsprechenden und regelmäßigen Überprüfungen stattfinden. Hier deutet sich ein klarer Widerspruch zur Wahrnehmung der eigenen Cyber-Resilienz an (siehe Abbildung 7 in Kapitel 2), denn neun von zehn Unternehmen schätzen die Fähigkeit ihres Unternehmens, Bedrohungen durch Hackerangriffe zu identifizieren und somit eine Früherkennung von Cyber-Angriffen zu gewährleisten, als hoch ein.

# Budget für Cyber Security

Die vorangegangenen Kapitel haben gezeigt, dass die untersuchten Unternehmen aus unterschiedlichen Gründen mehr in die IT-Sicherheit investieren wollen. Steigende Ausgaben für die IT-Sicherheit ergeben sich beispielsweise aus den veränderten Compliance- und Risk-Anforderungen im Zusammenhang mit der Cloud-Transformation und der damit verbundenen notwendigen Umsetzung einer wirkungsvollen Cloud Governance. Aber wie genau werden die Budgets für Cyber Security steigen und in welchen Bereichen entwickeln sie sich besonders dynamisch und wo eher nicht?

**76 %**
werden ihre Budgets im Bereich "Identify" erhöhen.

## KEIN UNTERNEHMEN REDUZIERT SEINE BUDGETS FÜR IT-SECURITY

Die wichtigste Nachricht für alle IT- und Security-Verantwortlichen, aber auch für die Kundinnen und Kunden: Bei keinem der untersuchten Unternehmen wird im Jahr 2022 weniger Geld für die IT-Sicherheit ausgegeben. Auch gibt es keine wesentlichen Unterschiede in der Höhe der Budgetzuwächse zwischen mittelständischen Unternehmen und Konzernen.

Die größten Zuwächse in den Budgets finden sich im Bereich Identifizieren von Schwachstellen (Identify): 76 Prozent der befragten Unternehmen werden ihre Budgets für die Früherkennung von potenziellen Cyber-Risiken und Angriffen um bis zu 10 Prozent erhöhen. Schwachstellen und somit Risiken finden sich beispielsweise in veralteten IT-Landschaften oder der Operational Technology (OT) in Form von Konfigurationsfehlern oder fehlerhaften Codes. Ebenso sind häufig Endgeräte wie Drucker oder Maschinen zwar mit dem Internet verbunden – und bieten so eine potenzielle Angriffsfläche –, aber eben nicht in eine Security-Architektur eingebunden.

Den zweiten großen Block für Budgeterhöhungen bildet die Antizipation und Abwehr von Cyber-Angriffen (Prevention). 61 Prozent der Studienteilnehmer wollen die Investitionen in diesem zentralen Bereich der Cyber-Abwehr um bis zu 10 Prozent erhöhen, 15 Prozent sogar um mehr als 10 Prozent. Damit ist die Prevention der Bereich, in dem die untersuchten Unternehmen die höchsten Investitionen tätigen werden. Hier mag ein Zusammenhang mit dem massiven Anstieg an Hackerangriffen im Jahr 2021 bestehen. Am häufigsten werden Unternehmen aus den Branchen Automotive (91 %), Manufacturing (85 %) und Telekommunikation/Medien/Verlage (84 %) ihre Prevention-Ausgaben erhöhen. Besonders hohe Budgetsprünge finden sich dagegen im Handel: 40 Prozent der befragten Handelsunternehmen wollen ihre Prevention-Budgets um mehr als 10 Prozent erhöhen.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Im Bereich der frühzeitigen Erkennung von Cyber-Angriffen und Unregelmäßigkeiten in den IT-Systemen (Detection) werden die Budgets hingegen laut den Planungen weniger stark steigen. Die vergleichsweise moderate Entwicklung mag unter anderem damit zusammenhängen, dass viele Unternehmen in den letzten Jahren ihre Rechenzentren technologisch modernisiert, technische Schulden abgebaut und in neue Security-Softwarelösungen zur Gefahrenabwehr investiert haben. Ebenso führt der steigende Cloud-Anteil in den IT-Landschaften tendenziell zu einem höheren Security-Level – unter anderem weil Cloud-Rechenzentren durch den Einsatz modernster Verschlüsselungstechnologien oder auch KI-basierter Abwehrverfahren und höhere Investitionsmittel der Cloud-Provider oft besser abgesichert sind als klassische On-Premise-Rechenzentren. Dass die Cloud grundsätzlich zu einem höheren Sicherheitsniveau führt, haben an anderer Stelle dieser Studie 61 Prozent der Befragten auch bestätigt (siehe Abbildung 10).

**44 %**
wollen die Budgets im Bereich "Response" konstant halten.

Bei der Detection geht es neben technologischen Aspekten aber auch sehr stark um organisatorische und prozessuale Maßnahmen, die es im Falle aufgedeckter Unregelmäßigkeiten zu treffen gilt. Denn gerade durch den digitalen Arbeitsplatz ergibt sich eine Vielzahl neuer Angriffspunkte und es gilt, die Endpoint Security entsprechend nachzuziehen und an die Heimarbeitsplätze anzupassen. In diesem Bereich fanden jedoch seit Ausbruch der Corona-Krise und der Verlagerung eines großen Teils der Arbeitsplätze in die Homeoffices bereits signifikante Investitionen statt. Daher überrascht es nicht, dass mit 59 Prozent vergleichsweise wenige Unternehmen ihre Ausgaben für die Erkennung von Angriffen und Unregelmäßigkeiten im Jahr 2022 noch mehr erhöhen werden. Besonders hoch ist der Anteil an Unternehmen mit steigenden Detection-Ausgaben in den Branchen Energie (60 %) und Manufacturing (75 %).

### MODERATE STEIGERUNGEN BEI RESPONSE UND RECOVERY

Vergleichsweise geringe Budgetsteigerungen finden sich auch im Bereich „Response“, bei dem es um das Ergreifen der richtigen Maßnahmen im Falle eines Cyber-Angriffs geht. 44 Prozent der Unternehmen planen, ihre Budgets in diesem Bereich konstant zu halten. Jedoch steht der Faktor „Mensch“ für die Wirksamkeit von Cyber-Security-Strategien besonders im Mittelpunkt, denn mit zunehmender Digitalisierung der internen und externen Kommunikation nehmen die potenziellen Angriffspunkte zu. Gleichzeitig werden die Methoden der Angreifenden – beispielsweise durch Social-Engineering-Kampagnen wie Phishing-Mails oder CEO-Fraud – immer professioneller und sind häufig nicht mehr als Fake erkennbar. Die Sensibilisierung der Mitarbeitenden, Fake-Mails zu erkennen und im Falle einer Falschhandlung unmittelbar die richtigen Schritte zu ergreifen, ist daher mindestens ebenso wichtig wie die technologische Absicherung der Netzwerke. Allerdings zeigt sich in den Budgetplanungen, dass genau für diesen sehr sensiblen Bereich die Ausgaben nur moderat steigen.

Gleiches gilt auch für Recovery-Maßnahmen, also das Wiederherstellen der Daten und IT-Systeme nach der Kompromittierung durch einen Cyber-Angriff: 60 Prozent der befragten

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Unternehmen werden ihre Budgets in diesem Bereich 2022 erhöhen. Interessanterweise sind es unter den Unternehmen, die eine Cloud-first-Strategie verfolgen, sogar 75 Prozent, was damit zusammenhängt, dass Recovery ein wesentlicher Bestandteil der Business Continuity und damit der Cloud Governance ist.

### ENTWICKLUNG DER BUDGETS FÜR CYBER SECURITY

| | um über 10% steigen | um bis zu 10% steigen | konstant |
|---|---|---|---|
| Identify: Identifizieren von Schwachstellen | 3% | 76% | 21% |
| Prevention: Antizipation und Abwehr von Cyberangriffen | 15% | 61% | 24% |
| Detection: Erkennung von stattfindenden Angriffen und Unregelmäßigkeiten/Anomalien | 7% | 52% | 41% |
| Response: Ergreifen der richtigen Maßnahmen bei erfolgten Cyberangriffen | 8% | 49% | 44% |
| Recovery: Wiederherstellen der Daten und IT-Systeme | 5% | 54% | 41% |

Abb. 16: Frage: Wie werden sich im kommenden Jahr die extern vergebenen Budgets in Ihrem Unternehmen voraussichtlich in den folgenden Bereichen verändern?; Alle Teilnehmer; Häufigkeitsverteilung; n = 135

### SECURITY SOLLTE DEZENTRALER UND CROSSFUNKTIONALER GESTEUERT WERDEN

Die Analyse der Budgetverantwortung für die Umsetzung von IT-Security-Strategien zeigt einige deutliche Unterschiede in den einzelnen Branchen und lässt auf unterschiedliche Reifegrade in der Digitalisierung und Agilität schließen. So zeigen die Ergebnisse, dass in 71 Prozent der Unternehmen, die eine Cloud-first-Strategie verfolgen, das Budget für IT-Security in dezentralen IT-Einheiten angesiedelt ist. Der Durchschnittswert über alle Unternehmen hinweg liegt mit 66 Prozent um 5 Prozentpunkte niedriger. Auch in den Branchen Automotive (84 %) und Energie (70 %) haben überdurchschnittlich viele der befragten Unternehmen ihre Security-Budgets in dezentralen IT-Einheiten organisiert.

Die zunehmende Digitalisierung von Geschäftsmodellen sowie ein immer weiter steigender Softwareanteil in Produkten (Embedded Software) wie in Haushaltsgeräten, Medizintechnik, Maschinen oder Fahrzeugen führen bereits während der Entwicklung digitaler Produkte zu einer stärkeren Berücksichtigung von Security by Design, um digitale Schnittstellen resilient gegenüber Cyber-Angriffen zu machen. Folglich erhalten Produkt-IT-Einheiten – vor allem in produzierenden Unternehmen – immer häufiger einen Teil des Security-Budgets.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Während in 27 Prozent der befragten Unternehmen dezentrale Produkt-IT-Einheiten über Security-Budget verfügen, liegt der Anteil im Sektor Chemie/Pharma schon bei 35 Prozent, in der Konsumgüterindustrie bei 32 Prozent und in Unternehmen aus dem Bereich Telekommunikation/Medien/Verlage sogar bei 45 Prozent.

Obwohl in dieser Studie überwiegend produzierende Unternehmen befragt wurden, für die Operational Technology eine zentrale Rolle in der Wertschöpfungskette spielt, haben nur 17 Prozent der betrachteten Unternehmen tatsächlich ihren OT-Einheiten bisher auch ein Cyber-Security-Budget gegeben. Dieses Ergebnis steht etwas im Widerspruch zu der zunehmenden Digitalisierung der Operational Technology, ihrer Vernetzung mit der Unternehmens-IT (OT/IT), aber auch zu der immer stärkeren Vernetzung von Produktionsanlagen zu Produktionsnetzwerken im Kontext von Industrie 4.0 und (I)IoT. Einzig unter den befragten Energieunternehmen haben 30 Prozent den OT-Einheiten ein dediziertes Security-Budget zugeteilt, was vor dem Hintergrund dessen, dass der Energiesektor zur kritischen Infrastruktur zählt, nicht überrascht. Eine Erklärung für den geringen Anteil von OT-Einheiten mit dediziertem Security-Budget ist, dass in vielen Unternehmen die OT/IT-Integration bereits so weit fortgeschritten ist, dass die IT im Rahmen einer integrierten OT/IT-Security-Strategie die gesamte Angriffsfläche überwacht.

**Bei 27 %**

verfügen dezentrale Produkt-IT-Einheiten über ein Security Budget.

### DIE VERANTWORTUNG FÜR CYBER-ABWEHR ERFOLGT DURCH DEZENTRALE ANSÄTZE UND IN VERANTWORTUNG MEHRERER FACHBEREICHE

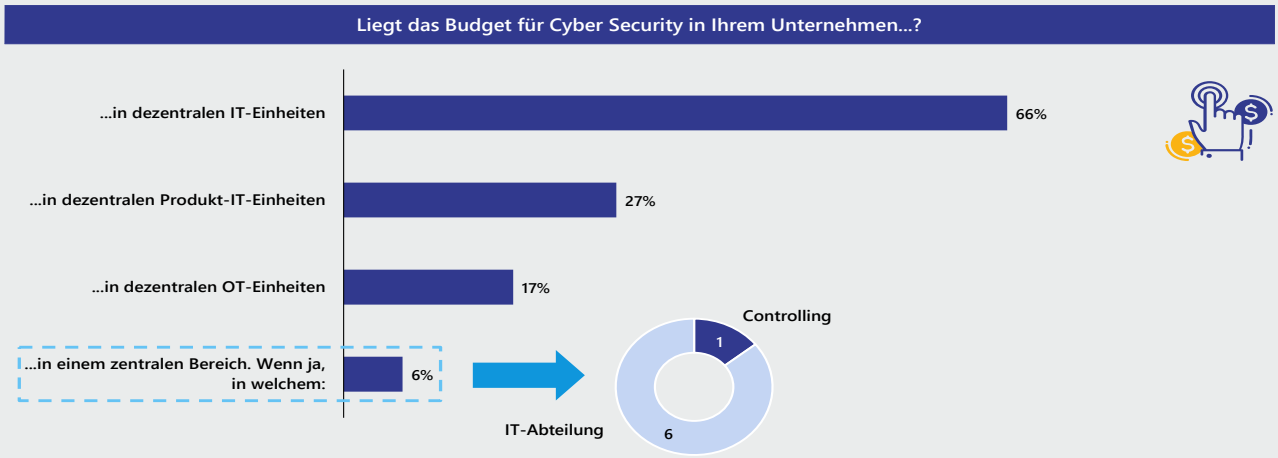


Abb. 17: Frage: Liegt das Budget für Cyber Security in Ihrem Unternehmen...?; Alle Teilnehmer; n = 137

# Geplante Security-Maßnahmen

Digitalisierte Kundenschnittstellen und Prozesse, mehr Cloud, neue Bedrohungsszenarien, veränderte Anforderungen an Daten- und IT-Sicherheit und steigende Budgets: Die befragten Unternehmen stellen sich in den kommenden Jahren der neuen Realität in der IT-Sicherheit und investieren in die bessere Absicherung ihrer IT-Infrastrukturen, Produkte und digitalen Geschäftsmodelle.

## SCHWACHSTELLEN ERKENNEN, BEVOR SCHÄDEN EINTRETEN: UNTERNEHMEN SETZEN FOKUS AUF FRÜHERKENNUNG

Wie bereits die Budgetplanungen im vorangegangenen Kapitel gezeigt haben, liegt ein sehr großer Fokus der befragten Unternehmen in den Jahren 2022/2023 auf Investitionen im Bereich „Identify", also dem Identifizieren von Schwachstellen und Sicherheitslücken, sowie dem Identity & Access Management als Security Gate.

**50 %**
der Unternehmen legen einen sehr starken Fokus auf das Vulnerability Management.

So legen 50 Prozent der Unternehmen einen sehr starken und weitere 34 Prozent einen eher starken Fokus auf das Vulnerability Management, also die präventive Erkennung und Behebung von Schwachstellen in der eigenen IT-Infrastruktur beziehungsweise im gesamten Ökosystem. Noch stärker im Fokus steht aber mit Blick auf die kommenden zwei Jahre das Identity & Access Management (IAM), also die Verwaltung der Benutzerkonten und Zugriffsberechtigungen. Hier wollen sogar 93 Prozent der befragten Unternehmen einen Fokus setzen.

Eine hohe Relevanz erlangt das IAM durch den Trend zu Multi-Cloud-Prozessen und zu digitalen Kunden-Touchpoints. Eine der Kernfunktionen ist die Authentifizierung und Autorisierung des Users, weshalb IAM auch eine zentrale Zugriffskontrolle für Webdienste darstellt (Stichwort: 2-Faktor-Authentifizierung). Eine weitere Kernfunktion moderner IAM-Softwarelösungen ist die zentrale Verwaltung der Zugriffsberechtigungen, also rollenbasierte Regelungen, auf welche Informationen Mitarbeitende Zugriff haben und auf welche nicht. Einen stets aktuellen Überblick über die Berechtigungen und Zugriffe zu haben ist vor allem infolge der zunehmenden Zahl von Public-Cloud-Diensten und entsprechend der potenziellen Angriffspunkte wichtiger denn je.

Der Blick auf diejenigen Unternehmen mit einer Cloud-first-Strategie zeigt, dass 96 Prozent dem Vulnerability Management mehr Aufmerksamkeit widmen. So zeigen Analysen erfolgter Cyber-Angriffe – unter anderem vom BSI oder den Security Operations Centers der großen Cloud-Hyperscaler – dass Angriffe vor allem dann geplant werden, wenn Unternehmen beispielsweise ankündigen, stärker in Cloud-Lösungen, digitale Geschäftsmodelle oder in

Cyber Security zu investieren. Beim Blick auf die einzelnen Branchen fällt auf, dass alle befragten Chemie- und Pharmaunternehmen einen stärkeren Fokus auf das Identity & Access Management legen wollen.

### UNTERNEHMEN WOLLEN SECURITY MONITORING WEITER AUSBAUEN

Analog zu den Budgetplanungen steht neben dem Identify-Bereich die Prevention potenzieller Cyber-Angriffe im Fokus der Maßnahmen für mehr Cyber-Resilienz.

**92 %**
wollen ihr Security-Monitoring verbessern bzw. ausbauen.

Besonders wichtig ist dabei den in der Studie untersuchten Unternehmen das Security Monitoring. 92 Prozent von ihnen wollen in den Jahren 2022–2023 ihr Security Monitoring verbessern beziehungsweise weiter ausbauen. Signifikante Branchenunterschiede gibt es bei diesem Thema keine, das bedeutet, dass hinsichtlich der Überwachung der zunehmenden Zahl digitaler Touchpoints und mit dem Internet verbundener Geräte und Produkte großer Nachholbedarf besteht. So hat Kapitel 4 gezeigt, dass nur sieben von zehn der befragten Unternehmen regelmäßig ihre IT-Systeme auf Security-Vorfälle (siehe Abbildung 15) überprüfen.

Infolge der laut BSI weiter stark steigenden Cyber-Bedrohungslage – unter anderem durch Zunahme von Ransomware-Angriffen und immer mehr und neuen Malware-Varianten, aber auch durch neue digitale Kundenschnittstellen und die zunehmende OT/IT-Vernetzung – ist ein kontinuierliches Tracking der Unternehmensnetzwerke ein wesentlicher Bestandteil der digitalen Transformation und des Risikomanagements.
Zum Bereich der Prevention gehören neben dem Security Monitoring auch die Cloud Security und die Data Center Security. Während 64 Prozent der Unternehmen einen Fokus auf die Cloud Security legen, wollen 73 Prozent ihre Aktivitäten zur Data Center Security weiter ausbauen. Unter den befragten mittelständischen Unternehmen wollen sich sogar 77 Prozent mehr auf die Data Center Security fokussieren.

Die Sicherheit von Industrieanlagen – die sogenannte OT/ICS Security – ist dagegen ein Thema, das nur produzierende Unternehmen betrifft. 83 Prozent planen in diesem Bereich in den kommenden zwei Jahren (2022/2023) einen eher starken bis starken Fokus zu legen. Unter den einzelnen Branchen finden sich in Automotive und Chemie/Pharma (jeweils 90 %) sowie Manufacturing (95 %) überdurchschnittlich viele Unternehmen, die in die OT/ICS-Sicherheit investieren werden. Von denjenigen Unternehmen mit einer Cloud-first-Strategie wollen 93 Prozent ihre Maßnahmen zur Absicherung der Operational Technology ausbauen.

### DETECTION: MEHR CLOUD-NUTZUNG FÜHRT ZU STÄRKEREM FOKUS AUF SIEM

Im Bereich der Detection wollen 84 Prozent der in der Studie untersuchten Unternehmen vor allem das Security Information and Event Management (SIEM) in den Fokus der Maßnahmen

rücken. Von den Unternehmen, die eine Cloud-first-Strategie verfolgen, werden sich mit 96 Prozent sogar fast alle Unternehmen in Zukunft mehr um ihre SIEM-Prozesse kümmern.

Tatsächlich besteht ein enger Zusammenhang zwischen dem SIEM und der zunehmenden Cloud-Nutzung. Je häufiger sich Unternehmen im Rahmen ihrer Cloud-Strategien für Multi-Clouds und hybride Umgebungen entscheiden oder komplett mit ihren Anwendungen und IT-Infrastruktur in die Cloud gehen, ist es im Sinne einer wirkungsvollen Security-Strategie ratsam, die Monitoring-Daten aus den einzelnen Cloud-Services an einer zentralen Stelle zusammenlaufen zu lassen. Organisatorisch und prozessual kommt es hierbei jedoch darauf an, ein zentrales SIEM aufzubauen, das die unterschiedlichen Cloud-Provider beziehungsweise Managed-Cloud-Service-Provider steuert und somit für eine integrierte Steuerung der Cloud-Prozesse im Sinne von End-to-End sorgt.

**55 %**

planen den Aufbau von SOCs, um mehr Cyber-Resilienz zu erreichen.

Dagegen ist Endpoint Security bereits seit Jahren ein Thema für Investitionen und daher bereits ein vergleichsweise reifes Marktsegment. Dennoch wird jedes zweite Unternehmen weiterhin einen Fokus auf die Endpoint Security legen.

Zur Detektion von Cyber-Angriffen und Security-Schwachstellen setzen immer mehr Unternehmen auf Security Operation Centers (SOCs). Dabei handelt es sich um Organisationseinheiten, die für die kontinuierliche Überwachung der IT-Systeme und für die Informationssicherheit verantwortlich sind. SOCs können sowohl intern als auch extern oder als hybride Formen – abhängig von der Verfügbarkeit von Inhouse-Security-Expertinnen und Experten – betrieben werden. Sie beschäftigen sich vor allem damit, Cyber-Angriffe zu verhindern, aktiv davor zu schützen, sie zu erkennen und entsprechende Maßnahmen einzuleiten. Dabei werden Ansätze und Technologien wie Schwachstellenmanagement, Gefährdungsbewertung und Endpoint Detection, Security Monitoring oder SIEM-Systeme in einem zentralen Center of Excellence gebündelt. Dieser Ansatz verspricht die bestmögliche Umsetzung eigener oder durch Regulatorik vorgegebener Sicherheitskonzepte durch Kombination aller relevanten Aufgaben in einer zentralen Organisation und in einem integrierten und ganzheitlichen Security-Ansatz. 55 Prozent der in der Studie befragten Unternehmen planen im Zeitraum 2022–2023 den Aufbau von SOCs als eine der Schwerpunktmaßnahmen, um mehr Cyber-Resilienz zu erreichen.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

### SCHWERPUNKTE IN DEN KOMMENDEN ZWEI JAHREN ZUR ERHÖHUNG DER CYBER-RESILIENZ LIEGEN VOR ALLEM IN DER FRÜHERKENNUNG VON CYBER-ANGRIFFEN

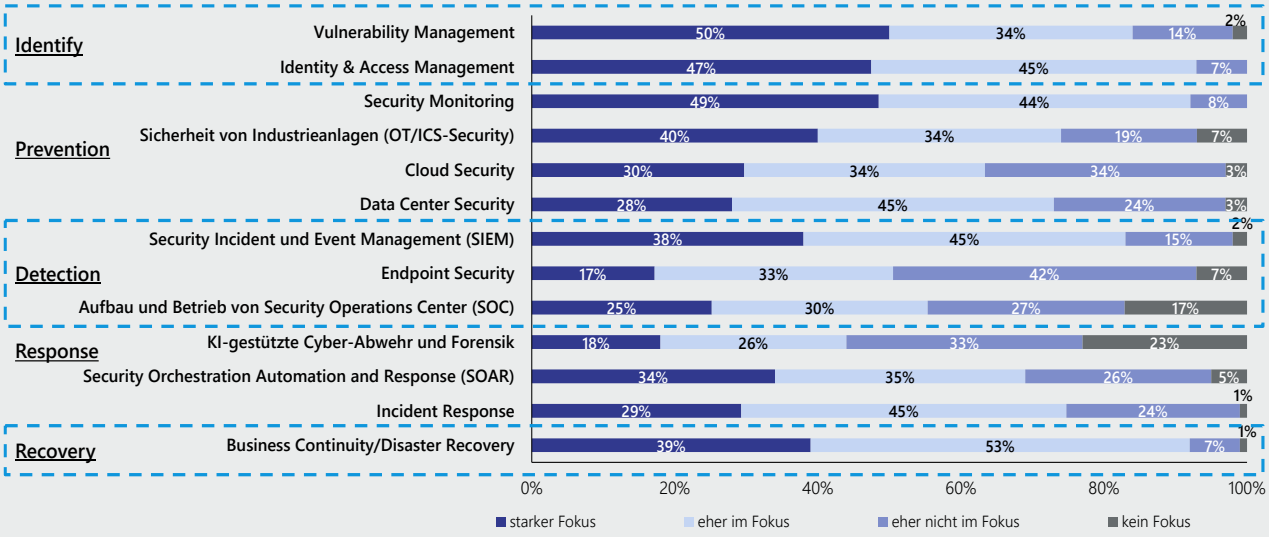


Abb. 18: Frage: Welche der folgenden Security-Aspekte stehen in Ihrem Unternehmen in den kommenden zwei Jahren im Fokus?; Alle Teilnehmer; Häufigkeitsverteilung; Skala von 1 = „kein Fokus" bis 4 = „starker Fokus"; n = 134

### WAS PASSIERT BEI EINEM ANGRIFF? NOCH GERINGER EINSATZ VON KÜNSTLICHER INTELLIGENZ, ABER DAFÜR FOKUSSIERUNG AUF DIE REAKTIONSGESCHWINDIGKEIT

Ist ein Cyber-Angriff erfolgt, kommt es darauf an, schnell zu handeln. Denn je effektiver die Reaktion – die Response – auf einen Security-Vorfall ist, desto höher ist die Chance, einen Datendiebstahl, das Verschlüsseln der Systeme oder den Ausfall produktiver Prozesse zu verhindern. Auch Meldungen an Behörden – beispielsweise beim Diebstahl personenbezogener Daten – müssen sehr zeitnah erfolgen. Für eine möglichst effektive und effiziente Reaktion auf Cyber-Angriffe kommt es vor allem auf Kommunikation, Organisation, Prozesse und Ressourcen an.

Dass drei Viertel der an der Studie teilnehmenden Unternehmen einen Fokus auf Incident Response legen wollen, zeigt, dass bei der Reaktionsfähigkeit noch häufig Handlungsbedarf besteht.

Die Aufgaben für den Schutz vor Cyber-Angriffen werden im Zuge der Digitalisierung immer vielfältiger und komplexer. Die steigende Datenmenge und die Komplexität im Cyber-Security-Tracking stellen viele Security-Abteilungen vor große Herausforderungen, die Flut an Gefahren zu erkennen und abzuwehren. Um die steigende Datenflut im Security Monitoring besser zu beherrschen, aber auch um die Security-Expertinnen und Experten von aufwendigen Routineaufgaben zu entlasten, denken Unternehmen immer häufiger über den Einsatz Künstlicher Intelligenz (KI) beziehungsweise Machine Learning bei der

Cyber Security nach. Die kontinuierliche und automatisierte Analyse von Daten und Ereignissen kann signifikant dazu beitragen, potenzielle Bedrohungen frühzeitig zu erkennen, zu klassifizieren und auf mögliche Angriffe schneller zu reagieren sowie großflächige Schäden vom Unternehmen abzuwenden.

Auf den Einsatz von KI zur Cyber-Abwehr setzen bereits 44 Prozent der in der Studie untersuchten Unternehmen. Unter denen, die eine Cloud-first-Strategie verfolgen, ist der Anteil mit 54 Prozent noch deutlich höher. Einen ebenfalls überdurchschnittlich hohen Fokus auf die KI-gestützte Cyber-Abwehr legen die befragten Unternehmen aus den Branchen Chemie/Pharma und Manufacturing (jeweils 55 %).

**44 %**

der Unternehmen setzen bereits auf den Einsatz von KI zur Cyber-Abwehr.

Beim Einsatz von KI – vor allem von Machine Learning – geht es darum, Angriffsmuster besser und vor allem frühzeitiger zu erkennen und somit eine deutlich bessere Prävention sicherzustellen. So haben Machine-Learning-basierte Algorithmen den Vorteil, kontinuierlich und automatisiert Millionen von Ereignissen zu überwachen und Muster (Anomalien) schneller und zuverlässiger zu erkennen. Vor allem um der steigenden Zahl von Bot-Angriffen und immer neuen Schadsoftwareprogrammen etwas entgegenzusetzen, lohnt es sich, sich mit Machine Learning zu befassen und auch KI-betriebene Bots einzuführen, die die Netzwerke nach Gefahren tracken. Die Notwendigkeit für Unternehmen, sich mehr mit KI in der Cyber-Abwehr zu beschäftigen, wird auch vom BSI bestätigt: So hat im Jahr 2021 die Zahl neuer Schadprogrammvarianten um rund 144 Millionen (+22 %) zugenommen und auch die Angriffe durch Bot-Netzwerke werden immer professioneller. Ein weiterer Vorteil vom Einsatz KI-basierter Security Services ist, dass KI-Technologien die IT-Netzwerke in einem 24/7-Modus tracken können und damit eine Reihe von Angriffspunkten schließen können.

### RECOVERY: BUSINESS CONTINUITY STEHT BEI NEUN VON ZEHN UNTERNEHMEN IM FOKUS

Nach einem erfolgten Cyber-Angriff oder Datendiebstahl ist es essenziell, sehr schnell wieder die Kontrolle über die Prozesse und die Daten zu erlangen. Dabei kommt es im Rahmen von Business-Continuity-Strategien sehr stark darauf an, die Prozesse und Daten wiederherzustellen. Disaster-Recovery-Konzepte sind beispielsweise in regulierten Branchen wie dem Energiesektor schon längere Zeit zwingend erforderlich. Im Zuge der Digitalisierung und der damit veränderten Cyber-Bedrohungslage ist Business Continuity ein wesentlicher Bestandteil einer Cloud Governance – beziehungsweise sollte es sein. Für fast alle der befragten Unternehmen (92 %) ist Business Continuity mit Blick auf die kommenden zwei Jahre eines der wichtigen Fokusthemen.

# Security Operations Centers

Das vorangegangene Kapitel hat gezeigt, dass 55 Prozent der untersuchten Unternehmen einen Fokus auf den Aufbau von SOCs legen werden. Diese Maßnahmen sind auch mit Blick auf die bereits im Betrieb befindlichen SOCs notwendig, denn hier besteht in Bezug auf die Bedrohungslage noch großer Nachholbedarf. So haben bisher (Stand Frühjahr 2022) nur 16 Prozent der befragten Unternehmen ein SOC etabliert, also bereits in Betrieb genommen. In Unternehmen mit einer Cloud-first-Strategie sind es jedoch bereits 25 Prozent. Höhere Anteile von Unternehmen mit einem SOC finden sich in den Branchen Automotive (33 %), Chemie/Pharma (26 %) und Telekommunikation/Medien/Verlage (26 %).

**Nur 16 %**
der Unternehmen haben bereits ein SOC etabliert.

46 Prozent der analysierten Unternehmen befanden sich zum Zeitpunkt der Studienerstellung inmitten des Rollouts, also der Operationalisierung, von SOCs. Weitere 22 Prozent planen in den kommenden Jahren den Aufbau von SOCs. Bemerkenswert ist, dass 16 Prozent der befragten Unternehmen nicht planen, ein SOC einzuführen – vor allem im Energiesektor (21 %) und in der Manufacturing-Industrie (35 %) ist der Anteil besonders hoch.

SOCs übernehmen für die Umsetzung der Cyber-Security-Strategie eine zentrale Aufgabe: Nicht selten werden Cyber-Angriffe und Datendiebstahl überhaupt nicht erkannt – unter anderem weil die Monitoring-Systeme bestimmte Schadprogramme nicht erkennen und entsprechend nicht melden.

Ein kontinuierliches Monitoring des gesamten Unternehmensökosystems (Unternehmensinfrastruktur, mobile Endgeräte, Third-Party-Anwendungen) ist daher essenziell, um die gesetzlichen und regulatorischen Anforderungen zu erfüllen, die bei der Cloud-Nutzung gelten. Zur effizienten Erfüllung der eigenen oder der externen Compliance-Vorgaben empfiehlt es sich daher, Know-how zur Cyber-Abwehr zentral in einem SOC zu bündeln.

Im SOC sollten Security-Spezialistinnen und Spezialisten organisatorisch angesiedelt sein; sie sollen eine eigene Einheit bilden und sich komplett auf die Cyber-Abwehr konzentrieren können. SOCs sind oft losgelöst von anderen IT-Teams, um unabhängiger von der IT zu agieren.

## REIFEGRAD DER SOCS: NAHEZU ALLE ZENTRALEN AUFGABEN WERDEN ERBRACHT

Die zahlreichen Aufgaben, die in einem SOC gebündelt werden, müssen und werden in der Regel nicht komplett innerhalb eines Unternehmens angesiedelt sein. Vielmehr werden einige im Rahmen von Managed Security Services an Dienstleister übertragen, auch Beratungs- und Transformationsaufgaben werden oft ausgelagert. Das hängt damit zu-

sammen, dass in vielen Unternehmen einerseits Security-Expertinnen und Experten fehlen und sich andererseits bestimmte Aufgaben aufgrund von Effizienzvorteilen für die Vergabe an externe Dienstleister eignen.

## SECURITY OPERATION CENTER NEHMEN IMMER HÄUFIGER IHRE ARBEIT AUF

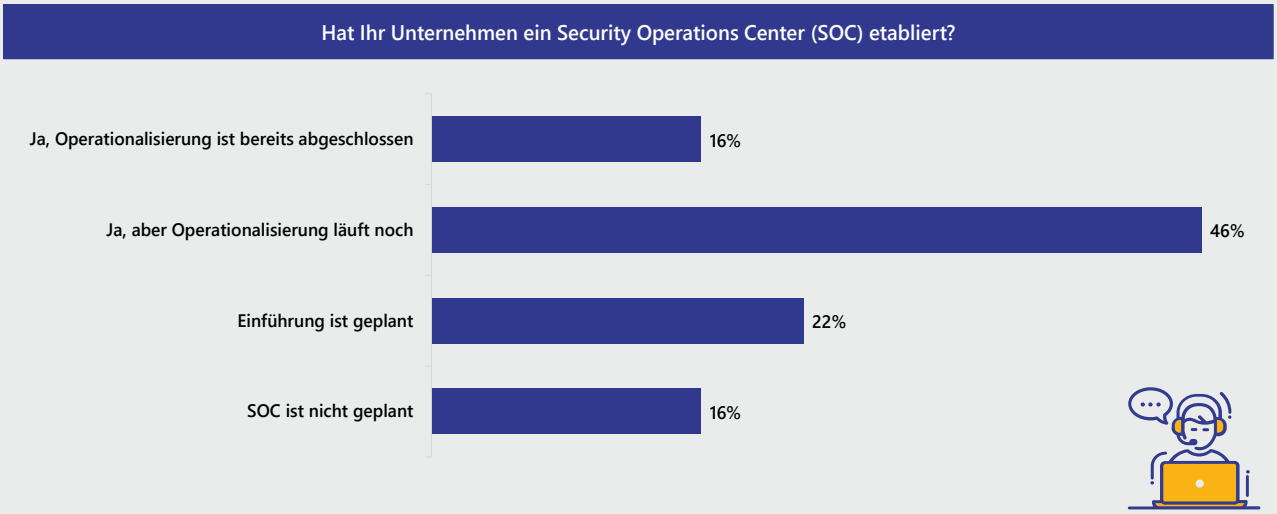


Abb. 19: Frage: Hat Ihr Unternehmen ein Security Operations Center (SOC) etabliert?; Alle Teilnehmer; Häufigkeitsverteilung; n = 131

Diejenigen Unternehmen, die bereits ein SOC in Betrieb haben oder gerade dabei sind, eines einzuführen, wurden gefragt, welche Aufgaben das SOC erfüllt. Im überwiegenden Teil der untersuchten Unternehmen übernehmen die SOCs alle relevanten Aufgaben im Rahmen einer IT-Security-Strategie.

Auffällig ist, dass in 35 Prozent der Unternehmen die Beratung zu Enterprise-Architektur und Security by Design keine Aufgabe eines SOC ist, sondern vermutlich in anderen Bereichen umgesetzt wird. Ebenso gaben 30 Prozent der Befragten an, dass Pentestings nicht zu den Aufgaben eines SOC in ihrem Unternehmen gehören, was gleichermaßen für die Definition und das Reporting von KPIs (in 22 Prozent der Unternehmen) gilt.

Die SOCs in den untersuchten Unternehmen übernehmen mehrheitlich vor allem Aufgaben, die sehr nah an der IT-Infrastruktur respektive den IT-Systemen sind und sich vergleichsweise gut standardisieren lassen. So wird das Configuration Management in 65 Prozent der Unternehmen intern erbracht, das Update- und Patch-Management in 68 Prozent und das SIEM sogar in 75 Prozent der Unternehmen.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Dagegen werden weniger technologische, sondern eher strategische, organisatorische und kulturelle Themen wie Change Management, Entwicklung von Use Cases, die Beratung zu Enterprise Architecture und Security by Design sowie das IT-Risikomanagement stärker extern vergeben.

### AUFGABEN EINES SOC UND DER MAKE-OR-BUY-MIX

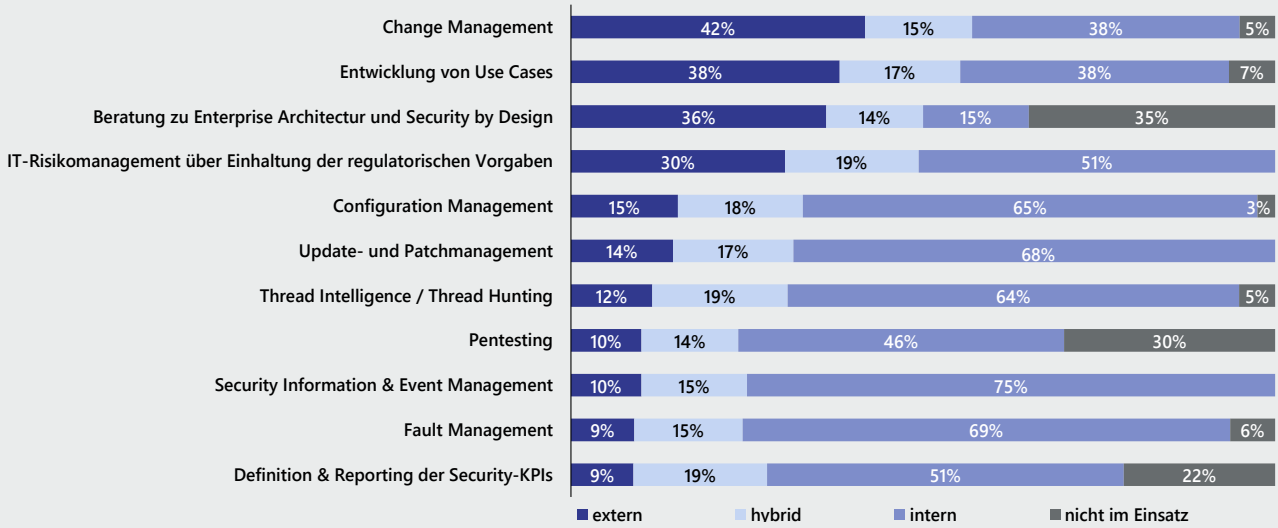


Abb. 20: Frage: Wie erfolgt die Leistungserbringung der folgenden Aufgaben eines SOCs?; Alle Unternehmen; Häufigkeitsverteilung; n = 78

.

# Externe Unterstützung und Managed Security Services

Für eine erfolgreiche Umsetzung von IT-Security-Strategien kommt es – neben den technologischen und organisatorischen Voraussetzungen – vor allem auf die Verfügbarkeit von Security-Expertinnen und Experten an, um die Konzepte auch wirksam umzusetzen. Allerdings mangelt es genau an dieser Stelle an Fachkräften. Die Vielzahl von Aufgaben zum Schutz vor der wachsenden Bedrohungslage rund um Cyber-Kriminalität und Cloud werden die Unternehmen daher nicht aus eigener Kraft bewältigen können.

## BEDARF AN EXTERNER UNTERSTÜTZUNG IST IN EINIGEN BEREICHEN SEHR HOCH

So werden in den untersuchten Unternehmen vermehrt externe Dienstleister zur Reduktion von Cyber-Risiken und zur Cyber-Abwehr eingesetzt.

**40 %**

sehen bei den Security-Feldern Response und Recovery eine hohe Nachfrage nach externen Dienstleistungen.

Die Mehrheit der Unternehmen hat im Bereich der Prevention einen hohen Bedarf an externen Dienstleistungen – vor allem bei den Themen „Sicherheit von Industrieanlagen“ (54 %), „Cloud Security“ (50 %) und „Product Security“ (49 %). In den Security-Feldern Response und Recovery besteht ebenfalls in mehr als 40 Prozent der Unternehmen eine hohe Nachfrage nach externen Dienstleistungen. Beim Blick auf die einzelnen Branchen fällt auf, dass in den Sektoren Automotive und Manufacturing der Bedarf an externen Dienstleistungen signifikant höher ist als im Durchschnitt aller Branchen.

Die Ergebnisse zeigen ebenfalls, dass die Unternehmen, die eine Cloud-first-Strategie verfolgen, deutlich häufiger mit externen Dienstleistern zusammenarbeiten – unter anderem weil sie höhere Anforderungen an die Cloud Security stellen. So arbeiten beispielsweise 58 Prozent der Unternehmen mit einer Cloud-first-Strategie im Bereich der Cloud Security und sogar 64 Prozent bei der KI-gestützten Cyber-Abwehr und Forensik mit externen Dienstleistern zusammen. Einen noch höheren Anteil an Unternehmen mit hohem Bedarf an externem Know-how findet sich in den Aufgabenfeldern „Product Security“ (71 %) und „Security Orchestration Automation and Response“ (69 %).

Tatsächlich bestätigt das Nachfragebarometer von Lünendonk für den deutschen IT-Dienstleistungsmarkt (siehe Lünendonk®-Studie „Der Markt für IT-Dienstleistungen in Deutschland“): Während Cyber Security 2020 noch bei 59 Prozent der durch Lünendonk in der genannten Studie befragten IT-Dienstleister einen großen Teil der Nachfrage ausmachte, erwarten mit Blick auf 2021 und 2022 nun 78 Prozent eine hohe Nachfrage nach Dienstleistungen rund um Cyber Security.

## FACHKRÄFTEMANGEL UND BEDARF AN EXTERNEM KNOW-HOW: DIE ZUSAMMENARBEIT MIT EXTERNEN DIENSTLEISTERN IST STARK AUSGEPRÄGT

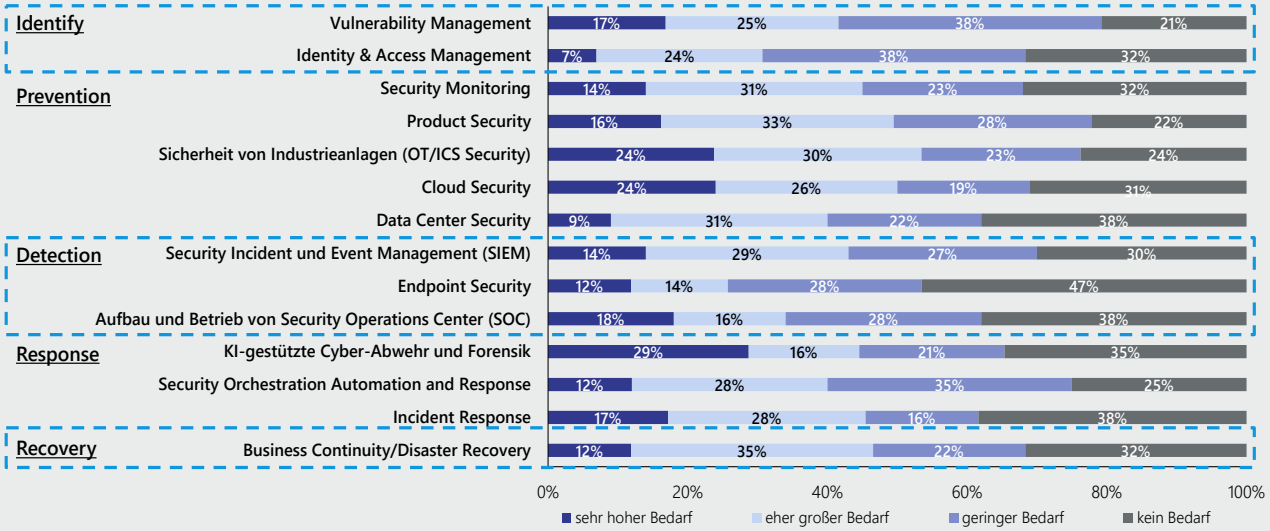


Abb. 21: Frage: Bei welchen der folgenden Themenfelder greift Ihr Unternehmen in Zukunft vermehrt auf externe Dienstleistungen zurück?; Alle Teilnehmer; Häufigkeitsverteilung; Skala von 1 = „kein Bedarf" bis 4 = „sehr hoher Bedarf"; n = 127

Tatsächlich berichten viele Kundenunternehmen von massiven Problemen, Security-Expertinnen und -Experten zu rekrutieren. Demnach ist es auch nur konsequent, dass Cyber Security für 86 Prozent der Unternehmen einen Investitionsschwerpunkt für die Jahre 2022–2023 bildet. 17 Prozent der Unternehmen werden ihre Budgets für Cyber Security sogar um mehr als 10 Prozent erhöhen, was auch durch diese Studie (siehe Kapitel 5, Abbildung 16) bestätigt wird.

### HOHER BEDARF AN MANAGED SECURITY SERVICES

Da immer größere Teile der IT-Landschaft von klassischen Rechenzentren in die Cloud geschoben werden, nimmt die Nachfrage nach Managed Cloud Services enorm zu. In diesem Zusammenhang steigt infolge der immer größeren Aufgabenfülle, zunehmender Komplexität und eines gleichzeitigen Mangels an Inhouse-Expertise auch der Bedarf an so-genannten Managed-Security-Service-Providern.

Den steigenden Bedarf an Managed Security Services bestätigen auch die in dieser Lünendonk®-Studie untersuchten Unternehmen: 84 Prozent nutzen bereits solche Dienstleistungen oder planen, mittelfristig auf sie zurückzugreifen. Signifikante Unterschiede zwischen mittelständischen Unternehmen und Konzernen mit mehr als 1 Milliarde Euro Umsatz bestehen nicht, sodass ersichtlich ist, dass die IT-Sicherheit auch im Mittelstand immer stärker professionalisiert wird.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Bei vielen Hackerangriffen spielt der Mensch als Angriffsfläche eine besondere Rolle. Durch CEO-Fraud oder Phishing-Kampagnen sollen Mitarbeitende dazu gebracht werden, auf täuschend echte Mails und Webseiten zu reagieren und somit die Angreifenden in die IT-Systeme zu lassen. Die Absicherung der Kommunikationskanäle ist daher von enormer Bedeutung – wichtiger noch als die reinen Security-Prozesse. Da sich die Methoden der Hackerinnen und Hacker sehr schnell ändern, der technologische Fortschritt im Feld der IT-Security rasant ist und gleichzeitig häufig internes Know-how und Investitionsmittel fehlen, bieten sich gerade Aufgaben rund um den Schutz der Kommunikationskanäle für Managed Services an. So arbeitet bei Aufgaben wie E-Mail-Security, Identity & Access Management und Endpoint Security mehr als jedes zweite Unternehmen mit Managed-Security-Service-Providern oder plant, dies zu tun. SOCs, Datensicherheit und Recovery und Ähnliches werden dagegen selten als Managed Services ausgelagert.

### 84 PROZENT DER UNTERNEHMEN SETZEN MITTELFRISTIG AUF MANAGED SECURITY SERVICES

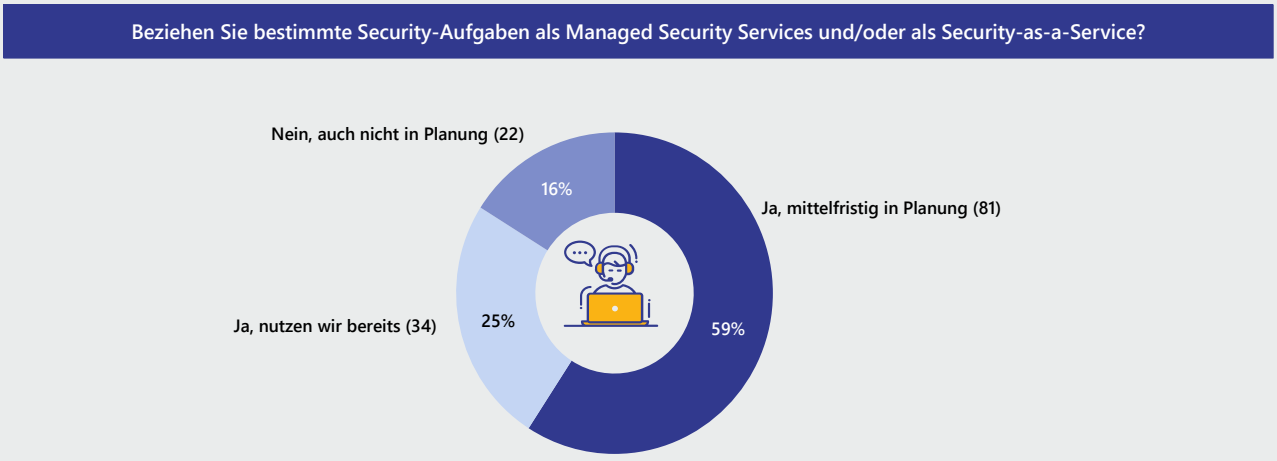


Abb. 22: Frage: Beziehen Sie bestimmte Security-Aufgaben als Managed Security Services und/oder als Security-as-a-Service?; Alle Teilnehmer; Häufigkeitsverteilung; n = 137

### ABRECHNUNG NACH AUFWAND IST DERZEIT DIE PRÄFERIERTE VERTRAGSFORM BEI MANAGED SECURITY SERVICES

Das gängige Vertragsmodell für Managed Security Services oder Security as a Service ist derzeit die Abrechnung nach Aufwand. 65 Prozent der befragten Unternehmen setzen auf die aufwandsbasierte Abrechnung, wohingegen 44 Prozent zusätzlich auch Festpreise und weitere 25 Prozent KPI-basierte Vergütungsmodelle bevorzugen.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

### BEREICHE, DIE UNTERNEHMEN AN MANAGED-SERVICE-PROVIDER VERGEBEN ODER ALS SECURITY AS A SERVICE BEZIEHEN

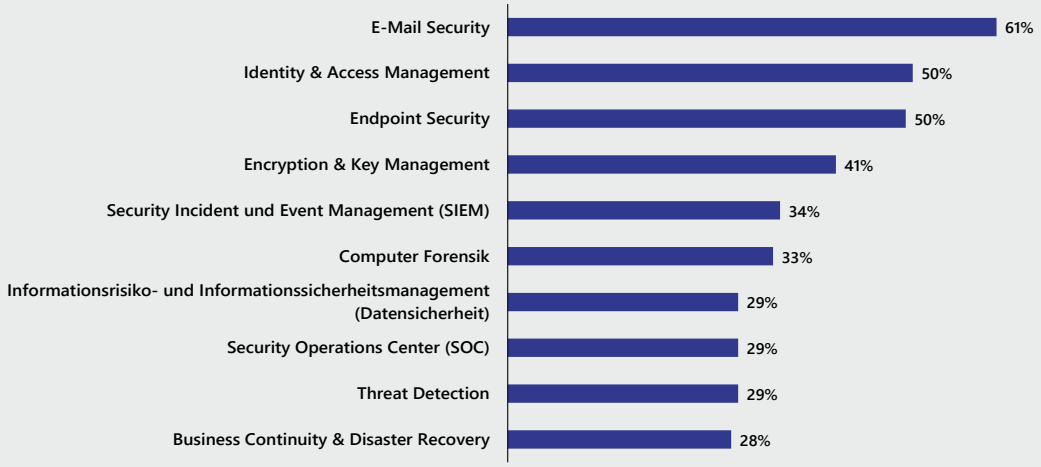


Abb. 23: Frage: Für welche Aufgabenfelder nutzen Sie als Managed Security Services oder Security-as-a-Service-Leistungen?; Alle Teilnehmer; Häufigkeitsverteilung; n = 115

### END-TO-END-SECURITY-SERVICES WERDEN BELIEBTER

Eine Erkenntnis aus den vergangenen Cyber-Angriffen lautet: Mit isolierten Security-Ansätzen ist es aufgrund der komplexen Bedrohungslage und der vielschichtigen Herausforderungen rund um die Nutzung von Cloud-Services nicht getan. Auch das BSI empfiehlt, Cyber Security mehr ganzheitlich zu sehen und IT-Security-Strategien zum einen stärker mit den Business-Strategien zu verzahnen und zum anderen die Schnittkanten zwischen den einzelnen Security-Services deutlich zu reduzieren.

### TIME & MATERIAL IST BEI SECURITY-AS-A-SERVICE DAS BEVORZUGTE ABRECHNUNGSMODELL

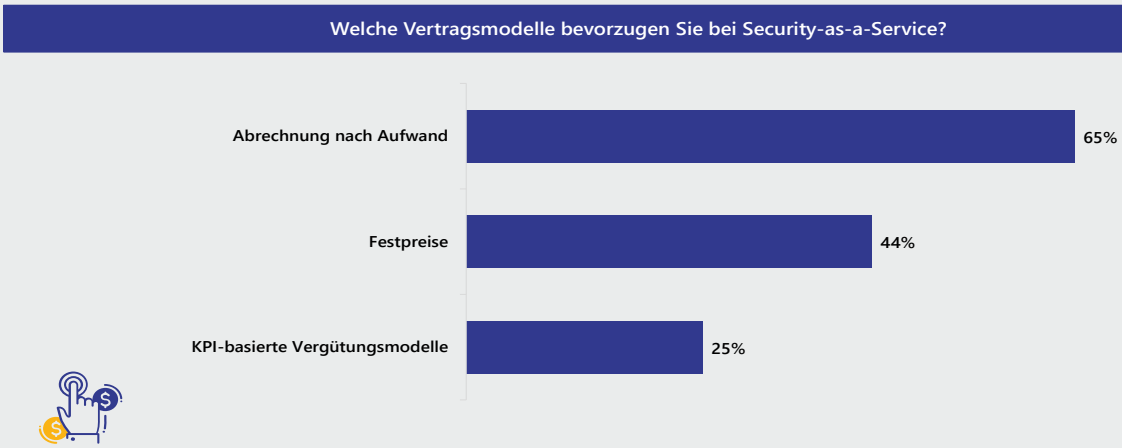


Abb. 24: Frage: Welche Vertragsmodelle bevorzugen Sie bei Security-as-a-Service?; Alle Teilnehmer; Häufigkeitsverteilung; n =110

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Gerade wenn Cloud-Dienste von mehreren Providern bezogen werden und immer mehr Workloads auf mehreren Cloud-Services aufsetzen (Multi-Cloud), kommt es darauf an, diese komplexeren Umgebungen möglichst effizient und regelkonform zu managen. Integrierte End-to-End-Lösungen, die alle Bereiche der Security-Strategie abdecken, gewinnen daher an Relevanz. Jedes zweite befragte Unternehmen (48 %) bevorzugt einen solchen ganzheitlichen und integrierten Ansatz im Rahmen seiner Cyber-Security-Strategie. Unter den untersuchten mittelständischen Unternehmen mit Umsätzen zwischen 250 Millionen und 1 Milliarde Euro Umsatz präferieren sogar 53 Prozent grundsätzlich einen integrierten Ansatz.

Darüber hinaus ergeben sich auch einige Branchenunterschiede: Während 58 Prozent der Energieunternehmen den integrierten Ansatz bevorzugen, setzen nur 26 Prozent der Handelsunternehmen auf End-to-End-Security-Konzepte.

### 50:50-VERTEILUNG: KEINE TENDENZ ZU INTEGRIERTEN ODER VERSCHIEDENEN SECURITY-SERVICES

**Bevorzugen Sie in Multi-/Hybrid-Cloud-Umgebungen eher mehrere einzelne Security-Services und -Anbieter für jeden Einzelbereich oder suchen Sie nach einer integrierten End-to-End-Lösung, welche alle Bereiche der Security-Strategie abdeckt?**

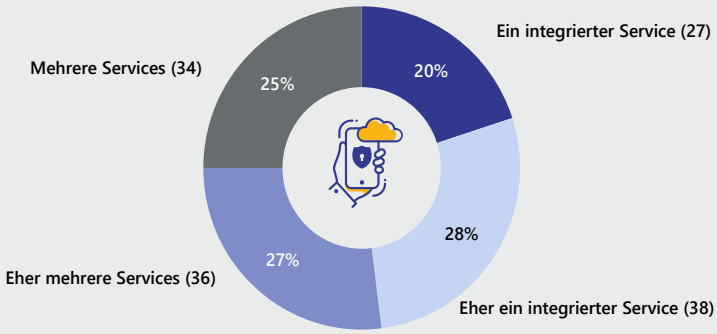


Abb. 25: Frage: Bevorzugen Sie in Multi-/Hybrid-Cloud-Umgebungen eher mehrere einzelne Security-Services und -Anbieter für jeden Einzelbereich oder suchen Sie nach einer integrierten End-to-End-Lösung, welche alle Bereiche der Security-Strategie abdeckt?; Alle Teilnehmer; Häufigkeitsverteilung; n = 135

# Fazit und Ausblick

Für die Lünendonk®-Studie „Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?" wurde auf der Basis von 140 Gesprächen – überwiegend mit IT- und Security-Verantwortlichen – analysiert, wie große mittelständische Unternehmen und Konzerne aus unterschiedlichen Branchen hinsichtlich der steigenden Bedrohungslage rund um Cyber-Kriminalität und Datendiebstahl aufgestellt sind.

Die Studienergebnisse veranschaulichen sehr deutlich, dass eine große Gefahr von immer professionelleren Cyber-Angriffen ausgeht und sich die IT-Security daher zu einem strategischen Wertschöpfungsfaktor entwickelt. Dabei spielt es eine Rolle, dass sich IT-Security längst nicht mehr nur auf die IT-Infrastruktur, also die Unternehmensnetzwerke, bezieht, sondern mit zunehmender Digitalisierung der Geschäftsmodelle auch auf die Produkt-IT im Sinne von Security by Design und die Absicherung von Industrieanlagen im Kontext einer Industrie 4.0.

Die zunehmende Cyber-Kriminalität, vor der das BSI regelmäßig warnt, wird auch von 82 Prozent der in der Studie Befragten als sehr hoch eingestuft. Vor allem die steigende Zahl von Angriffen durch Ransomware, Phishing-Kampagnen und DDoS-Attacken wird von zwei Dritteln der Unternehmen mit großer Sorge beobachtet. Daneben wächst – im Zusammenhang mit dem massiven Ausbau von Remote Working – die Gefahr, dass sich durch die Einbindung unautorisierter Endgeräte in die Unternehmensnetzwerke neue Sicherheitsrisiken ergeben.

### DIE CLOUD ERHÖHT DIE IT-SICHERHEIT, ERFORDERT ABER AUCH EINE ANGEPASSTE SICHERHEITSARCHITEKTUR

Hinzu kommt als weiteres Security-Risiko die seit der Corona-Krise beschleunigte Cloud-Transformation. 70 Prozent der befragten Unternehmen verfolgen bereits eine Cloud-Strategie und weitere 27 Prozent planen, innerhalb der nächsten zwei Jahre eine solche umzusetzen. Aus der zunehmenden Cloud-Nutzung versprechen sich 61 Prozent der Unternehmen zwar grundsätzlich eine Erhöhung ihres Security-Levels, unter anderem weil Cloud-Rechenzentren unter Einsatz modernster Technologien besser gegen Cyber-Angriffe geschützt sind und die Cloud-Provider massiv in ihre Absicherung investieren. Allerdings verlassen sich die befragten Unternehmen nicht ausschließlich auf die Cloud-Provider, sondern sehen darüber hinaus die Notwendigkeit, mehr in die IT-Sicherheit zu investieren.

Tatsächlich zeigen die Studienergebnisse, dass ein Teil der untersuchten Unternehmen noch nicht optimal auf die Anforderungen und Veränderungen, die sich durch die Digitalisierung ergeben, aufgestellt ist. Trotz der starken Zunahme von Ransomware-Angriffen und

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Phishing-Kampagnen gerade in den Jahren seit der Corona-Krise führt nur jedes zweite Unternehmen regelmäßiges Pentesting durch. Noch auffälliger an den Aussagen vieler Befragter ist, dass für jedes dritte Unternehmen der Cyber-Security-Status nicht transparent ist, weil er nicht regelmäßig überprüft und entsprechende Kennzahlen erstellt werden. Solche Aufgaben werden immer häufiger durch SOCs übernommen, in denen an zentraler Stelle verschiedene Aufgaben rund um die IT-Sicherheit gebündelt werden. Allerdings haben bisher nur 16 Prozent der untersuchten Unternehmen ein solches SOC in Betrieb genommen, wobei sich weitere 46 Prozent zum Zeitpunkt der Studienerstellung inmitten des Rollouts befanden.

Infolge des rasanten technologischen Fortschritts bei IT-Security-Technologien und der immer höheren Professionalität von Hackerorganisationen gewinnt eine Bündelung relevanter Sicherheitsaufgaben in einem zentralen Competence Center an Bedeutung. Gleichzeitig entscheiden sich immer mehr Unternehmen, Teile eines SOC durch spezialisierte externe Dienstleister – häufig im Rahmen von Managed Security Services – übernehmen zu lassen. Gerade bei Security-Themen, die direkt die Schnittstelle zu den Unternehmensnetzwerken betreffen und bei denen der Faktor Mensch einen hohen Einfluss hat, wie Endpoint- und E-Mail-Sicherheit, setzt mehr als jedes zweite befragte Unternehmen auf Managed Services.

### MEHR UND RICHTIGE INVESTITIONEN IN CYBER SECURITY

Es gibt also noch viel zu tun auf dem Weg zu einer wirksamen und systematischen Cyber Resilienz, und entsprechend hoch sind die geplanten Investitionen der Unternehmen. Einen besonders großen Fokus legen die Unternehmen dabei auf die Schwachstellenanalyse und die frühzeitige Abwehr von Cyber-Angriffen – also genau das Zeitfenster vor einem tatsächlichen Angriff. Vor allem die Analyse von Schwachstellen, das sogenannte Vulnerability Management, ist laut den Befragten enorm wichtig. Denn was nutzen die modernsten Security-Technologien und Prozesse, wenn die IT-Systeme veraltet und durch Konfigurationsfehler leichtes Ziel für Hackerangriffe sind? So legen 84 Prozent der befragten Unternehmen in den kommenden Jahren einen Fokus auf das Vulnerability Management.

Noch häufiger (in 92 Prozent der Unternehmen) stehen aber Security Monitoring, Identity & Access Management und Business Continuity & Recovery im Fokus der künftigen Maßnahmen. Da sich mit steigender Cloud-Nutzung die Zahl der IT-Systeme und der Anwendungen, die mit dem Internet verbunden sind, massiv erhöht, gewinnt die maximale Transparenz bezüglich sämtlicher Aktivitäten im gesamten IT-Netzwerk enorm an Bedeutung. Folglich legen 82 Prozent der Unternehmen auch einen Fokus auf das Security Incident & Event Management (SIEM). Vor allem durch die zunehmende Nutzung von Multi-Cloud-Umgebungen – also die Abbildung eines Geschäftsprozesses über mehrere Clouds hinweg – wird ein professionelles SIEM zum festen Bestandteil der Cloud Governance.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

In Zahlen ausgedrückt, steigen die Budgets im Bereich „Identify" im Zeitraum 2022/2023 in 76 Prozent der befragten Unternehmen um bis zu 10 Prozent. Deutlich aufwendiger als das Identifizieren von Schwachstellen ist die Prävention, also das Schließen von Sicherheitslücken. Dabei geht es beispielsweise um die Tilgung technischer Schulden – also um die IT-Modernisierung. Während 61 Prozent der Unternehmen ihre Budgets für die Prävention um bis zu 10 Prozent steigern wollen, erhöhen 15 Prozent ihre Ausgaben sogar um mehr als 10 Prozent. Auch die Lünendonk®-Studie „Der Markt für IT-Beratung und IT-Service in Deutschland" bestätigt, dass die IT-Modernisierung zu den Top-5-Investitionsthemen für CIOs gehört. In den Feldern Detection, Response und Recovery steigen die Budgets dagegen langsamer – wobei auch hier unter den Befragten niemand von sinkenden Budgets berichtete.

### IT-SECURITY MUSS ÜBER DIE TECHNOLOGISCHE PERSPEKTIVE HINAUS GESTEUERT WERDEN

Die geplanten Maßnahmen der untersuchten Unternehmen lassen den Schluss zu, dass es für einen wirksamen Schutz vor Cyber-Bedrohungen nicht mehr genügt, den Fokus nur auf die Absicherung der eigenen IT-Infrastruktur zu legen. Tatsächlich bezieht sich die Absicherung der Unternehmensnetzwerke in 60 Prozent der Unternehmen bereits auf das gesamte Ökosystem, also inklusive Lieferanten, Kundenkreis und Partnerunternehmen.

Auch die Verantwortung für IT-Security nur in der IT und bei den externen IT-Dienstleistern zu sehen, wird der Bedrohungslage im digitalen Zeitalter nicht mehr gerecht. Aus den Gesprächen im Rahmen dieser Studie wird deutlich, dass eine ganze Reihe neuer interner Kompetenzen und Rollen notwendig ist, um die digitalen Geschäftsmodelle der Zukunft, aber auch den digitalen Arbeitsplatz der Zukunft abzusichern. Der Erfolg digitaler Geschäftsmodelle und damit die Wettbewerbsstärke wird sich künftig viel stärker danach bemessen, wie sicher die Kundinnen und Kunden ihre Daten bei der Nutzung eines Online-Service aufgehoben sehen. Security dabei als Teil der Unternehmensstrategie und als integralen Bestandteil der Produktentwicklung im Sinne von Security by Design zu begreifen, wird hier die entscheidende Rolle spielen. Cyber-Security wird infolgedessen künftig viel stärker ganzheitlich gedacht und rückt aus der „IT-Ecke" heraus mehr in das Business sowie direkt an die Schnittstelle zu den Kunden und Kundinnen. Dazu muss die IT-Security in den Unternehmen aber auch den Stellenwert erhalten, den sie benötigt, um ihren Teil zu einem resilienten Unternehmen beizutragen.

# Lünendonk im Interview mit KPMG zu den Studienergebnissen

Wilhelm Dolle
Partner, Consulting - Head of Cyber Security

KPMG AG Wirtschaftsprüfungsgesellschaft

Dr. Michael Falk
Partner, Consulting, Cyber Security

KPMG AG Wirtschaftsprüfungsgesellschaft

Markus Limbach
Director, Consulting, Cyber Security

KPMG AG Wirtschaftsprüfungsgesellschaft

**LÜNENDONK:** Die Studie zeigt, dass die Bedrohungslage, Opfer eines Hackerangriffs zu werden, von der Mehrheit der Unternehmen als hoch eingeschätzt wird. Welche Auffälligkeiten zur Bedrohungslage sehen Sie, und gibt es Branchen- sowie sektorale Unterschiede?

**WILHELM DOLLE:** Bereits im letzten Jahr haben erfolgreiche Cyber-Angriffe zu schwerwiegenden Betriebsunterbrechungen bei Unternehmen und Behörden geführt. Diese verursachten zum Teil erhebliche wirtschaftliche Schäden. Mit Beginn des Russland-Ukraine-Kriegs im Februar 2022 haben die Cyber-Bedrohungen weiter zugenommen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sprach im April von einer „abstrakt erhöhten Bedrohungslage". Phishing-Kampagnen und Ransomware-Attacken zählen dabei zu den häufigsten Vorfällen, die wir aktuell sehen.

Die erhöhte Bedrohungslage gilt besonders für Unternehmen, die Teil der kritischen Infrastruktur sind, also beispielsweise Energie-, Telekommunikations-, Medien-, Gesundheits- und Finanzdienstleistungsunternehmen. Für sie gilt aus meiner Sicht eine erhöhte Alarmbereitschaft. Und zwar unabhängig davon, ob die Unternehmen in Russland, der Ukraine, den Nachbarländern oder im Westen tätig sind.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

**LÜNENDONK:** Die Unternehmen sind sich allem Anschein nach immer noch unsicher: Ist IT-Security aus Ihrer Sicht eher ein Wertschöpfungs- oder Kostenfaktor?

**MICHAEL FALK:** Das Thema Sicherheit ist für fast alle Unternehmen bereits eine wichtige Grundlage der Geschäftstätigkeit. Das Bewusstsein dafür nimmt erfreulicherweise zu. Denn schlecht aufgestellte Unternehmen erhalten keine Cyber-Versicherung, die wiederum die Produktionsausfälle in Folge eines Cyber-Angriffs abdecken würde. Und wenn wir bei unseren Kunden anfangen, Cyber-Risiken auf Basis von Szenario-Betrachtungen monetär zu quantifizieren, stehen häufig potenzielle Schäden im Raum, die den Fortbestand des Unternehmens gefährden.

Wir müssen grundsätzlich das Bewusstsein dafür schaffen, dass wir Angriffe nie vollständig verhindern können und gleichzeitig die Bereitschaft bei den Unternehmen erhöhen, in die Reaktion auf Cyber-Bedrohungen zu investieren. Sie glauben gar nicht, wie glücklich der Vorstand bzw. die Geschäftsführung ist, wenn sie sehen, dass mit dem Backup tatsächlich die Wiederherstellung kritischer Systeme gelingt.

"Sie glauben gar nicht, wie glücklich der Vorstand bzw. die Geschäftsführung ist, wenn sie sehen, dass mit dem Backup tatsächlich die Wiederherstellung kritischer Systeme gelingt."

Dr. Michael Falk
KPMG

**LÜNENDONK:** Manche Unternehmen sehen in der Nutzung von Cloud gleichzeitig einen Gewinn für ihre eigene Sicherheit – andere sind wiederum skeptisch demgegenüber eingestellt. Was sehen Sie bei Ihren Kunden?

**MARKUS LIMBACH:** Die Nutzung von Cloud-Services ist aus dem Unternehmensalltag mittlerweile nicht mehr wegzudenken. Der Reifegrad der aus der Cloud und für die Cloud angebotenen Sicherheitsfunktionalitäten steigt kontinuierlich an. Durch den hohen Grad an Standardisierung und Automatisierung bieten Cloud Services bei richtiger Anwendung ein sehr hohes Maß an Sicherheit.

Ich sehe bei unseren Kunden, dass der kulturelle Wandel weiterhin in vollem Gange ist. Die Sicherheitsparadigmen ändern sich, und auch die Verantwortlichen im Bereich der IT- und Informationssicherheit müssen lernen, mit der hohen Geschwindigkeit und der Funktionalitätsvielfalt auf dem Cloud-Markt Schritt zu halten. Die Möglichkeiten zur Prävention, Detektion und auch automatisierten Reaktionen auf Cyber-Angriffe werden immer ausgefeilter. Konkret bedeutet das, sich im Rahmen der Cloud-Strategie auch intensiv mit den durch die großen Cloud-Provider angebotenen Sicherheitsfeatures zu beschäftigen. Diese Features werden viel dynamischer weiterentwickelt, als das klassische Anbieter von Sicherheitstechnologien historisch getan haben. In vielen Fällen überwiegen aus unserer Sicht die Vorteile der hoch integrierten Lösungen in der Cloud.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

Dennoch gibt es weiterhin sensible Bereiche, in denen die Nutzung von Cloud-Services wohl überdacht werden muss. Wir unterstützen unsere Mandanten regelmäßig dabei, solche risikobasierten Abwägungen vorzunehmen und eine nachhaltige Informationssicherheitsstrategie umzusetzen.

**LÜNENDONK:** Die Studie zeigt, dass Vorsorge, Krisenreaktion oder auch Cyber Resilience wichtige Trendthemen im Bereich Security sind. Wie kann KPMG Kunden hierbei konkret unterstützen? Wie hebt sich KPMG von den Wettbewerbern ab?

**MARKUS LIMBACH:** Cybervorfälle und Betriebsunterbrechungen sind mitunter die größten Sorgen für Unternehmen – sowohl international als auch in Deutschland. Diese Wahrnehmung wird insbesondere durch die steigende Anzahl von Cyberangriffen, fortschreitender Regulatorik (z.B. IT-Sicherheitsgesetz, Digital-Operational-Resilience-Act), geopolitische Konflikte und die Coronapandemie verstärkt.

"Cybervorfälle und Betriebsunterbrechungen sind mitunter die größten Sorgen für Unternehmen – sowohl international als auch in Deutschland. "

Markus Limbach
KPMG

Aus unserer Sicht ist diese Sorge auch durchaus berechtigt. Allein in den letzten Monaten haben wir mehreren Mandanten dabei geholfen, ihre IT-Systemlandschaft nach großflächigen Ransomware-Angriffen wiederherzustellen. Solche Krisensituationen wie der aktuelle Russland-Ukraine-Krieg bringen Unternehmen an den Rand ihrer Belastbarkeit und sind existenzgefährdend.

Mit unseren Cyber Resilience Services bereiten wir Unternehmen frühzeitig auf solche Situationen vor und entwickeln passgenaue Notfallpläne. Ich lege allen Unternehmenslenkern ans Herz, diese Krisenszenarien im Rahmen einer Simulation durchzuspielen, um im Ernstfall auf trainierte und erprobte Abläufe zurückgreifen zu können. Wir achten bei unseren Kunden darauf, diese Ernstfälle realitätsnah und szenariobasiert regelmäßig zu proben und die Organisation und einzelne Akteure bewusst unter Stress zu setzen.

**LÜNENDONK:** Enthält die Studie Ergebnisse bzw. Aussagen Ihrer Mandanten, die überraschend für Sie waren?

**MICHAEL FALK:** Ich würde sagen, weniger überraschend, sondern eher durchaus bemerkenswert. Wie wir anhand der Studienergebnisse sehen können, werden die Gefahren nach wie vor als hoch eingeschätzt. Allerdings sind die Unternehmen weder bezogen auf ein regelmäßiges KPI-Reporting noch in der Bereitschaft, realistisch und szenariobasiert die eigenen Fähigkeiten zu testen, aktuell gut aufgestellt.

Auch wenn Unternehmen auf uns zukommen, um im Bereich des Patch- und Vulnerability-managements gesteuerte Prozesse aufzusetzen oder sogenannte Red Teaming Exercises

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

durchzuführen, dauert es erfahrungsgemäß eine Weile, bis aus den gewonnenen Erkenntnissen Verbesserungen konsequent umgesetzt werden. Wir sprechen hier gerne von kontinuierlicher Verbesserung oder einer lernenden Organisationskultur – aber in der Praxis geht zu viel Zeit für die Suche eines Schuldigen verloren.

**LÜNENDONK:** Welche Schlüsse zieht KPMG als führendes Beratungsunternehmen für Cyber Security aus dieser Studie und welche ableitenden Empfehlungen würden Sie Ihren Mandanten mit auf den Weg geben?

**WILHELM DOLLE:** Viele Rückmeldungen aus der Studie bestätigen den bei KPMG strategisch eingeschlagenen Weg. Unternehmen investieren verstärkt in Cyber Security, die Bedrohungslage wird zunehmend differenzierter betrachtet und Risiken in Produktionsprozessen, Liefer- und Logistikprozessen sowie in Produkten – Stichwort Internet of Things (IoT) – haben einen direkten Einfluss auf die Geschäftsentwicklung.

"Unternehmen sollten ihre eigene Bedrohungslage überprüfen und sich im Klaren darüber sein, welchem Risiko sie im Falle eines Cyberangriffs ausgesetzt sind. "

Wilhelm Dolle
KPMG

Grundsätzlich sollten alle Organisationen ihre Cyber-Security-Maßnahmen umfangreich überprüfen und hierbei die folgenden vier Schwerpunkte berücksichtigen:

- **WIDERSTANDSFÄHIGKEIT:** Unternehmen sollten ihre eigene Bedrohungslage überprüfen und sich im Klaren darüber sein, welchem Risiko sie im Falle eines Cyberangriffs ausgesetzt sind. Hierbei sollten sie ihre Reaktionspläne auf folgende Fragen überprüfen: Wie oft haben Sie Ihre Pläne getestet? Wie relevant sind die Testszenarien für aktuelle Bedrohungen?

  Unternehmen sollten dabei alle vorgeschriebenen Meldepflichten für digitale Sicherheitsvorfälle kontrollieren und bei Bedarf Gespräche mit Strafverfolgungsbehörden, die im Falle eines größeren Cyberangriffs involviert wären, in Erwägung ziehen.

- **CYBER-SICHERHEIT:** Es ist wichtig, bei der Behebung von Schwachstellen die Prioritäten in die IT-Infrastruktur zu setzen. Unternehmen sollten ihre IT regelmäßig auf Lücken scannen sowie die Zugangskontrollen zu den wichtigsten Systemen und Cloud-Diensten überprüfen. Ungenutzte oder abgelaufene Konten sollten entfernt werden.

  Zudem sollte sichergestellt sein, dass eine Anti-Malware-Software installiert ist, die Lizenzen auf dem neuesten Stand sind und die Software regelmäßig aktualisiert wird. Für kritische Anwendungen sollten Backup-Prozesse vorhanden sein und regelmäßige Offline-Kopien erstellt werden.

## Von Cyber Security zur Cyber Resilience – mehr Digitalisierung, mehr Cyber-Bedrohung?

- MITARBEITENDE: Unternehmen sollten dafür Sorge tragen, dass die eigenen Mitarbeiterinnen und Mitarbeiter Zugang zu verlässlichen Informationen über die aktuelle Krise haben und sie über die neusten Phishing-Mails, gefälschte Websites und andere Formen von Cyberattacken im Bilde sind. Mitarbeitende, die an besonders gefährdeten Standorten oder in exponierten Rollen arbeiten, sollten gesondert und regelmäßig über mögliche Bedrohungsszenarien geschult werden.

- LIEFERANTEN UND LIEFERKETTEN: Unternehmen sollten ihre Abhängigkeiten von Anbietern aus der Ukraine, Russland und den Nachbarländern identifizieren und einen Notfallplan für den Fall erstellen, dass sie von der Lieferkette abgeschnitten werden. Zudem sollte verstärkt der digitale Verkehr aus Ländern, die in den Konflikt verwickelt sind, überwacht werden.

  Viele Hackergruppen, besonders in Russland, haben in der derzeitigen Situation freie Hand. Einige Hackerangriffe werden sogar direkt der russischen Regierung zugeschrieben. Unternehmen sollten grundsätzlich nachvollziehen können, welche Folgen eine Cyberattacke auf die eigenen Lieferketten hat und daraufhin entsprechende Schutzmaßnahmen einleiten.

Da unklar ist, wie sich die Cyber-Bedrohungslage entwickeln wird, empfehlen wir unseren Mandanten, verschiedene Szenarien zu entwickeln, um kurzfristig die Sicherheitsstrategie anpassen zu können. Dabei sollte für jedes Szenario konkret untersucht werden, was eine potenzielle Cyberattacke für das eigene Unternehmen in Bezug auf Mitarbeitende, Lieferketten und digitale Risiken bedeutet. Es ist wichtig, auf alle Eventualitäten vorbereitet zu sein.

"Für jedes Szenario sollte konkret untersucht werden, was eine potenzielle Cyberattacke für das eigene Unternehmen in Bezug auf Mitarbeitende, Lieferketten und digitale Risiken bedeutet. "

Wilhelm Dolle
KPMG

# Die Interviewpartner im Profil

Wilhelm Dolle
**Partner, Consulting - Head of Cyber Security**
KPMG AG
Wirtschaftsprüfungsgesellschaft

Telefon: +49 (0)30 20682323
E-Mail: wdolle@kpmg.com

Wilhelm Dolle leitet als Partner bei der KPMG den Bereich Cyber Security und ist Geschäftsführer der KPMG CERT GmbH. Er ist Experte für technische und organisatorische Aspekte der Informationssicherheit. Dazu gehören Risiko- und Sicherheitsanalysen, der Aufbau von Informationssicherheitsmanagementsystemen sowie Themen wie Penetrationstests und Sicherheit von Industrieanlagen. Zudem beschäftigt er sich intensiv mit den regulatorischen Anforderungen an die Informationssicherheit und das IT-Risikomanagement. Er hat bereits diverse Studien zum IT-Sicherheitsgesetz und zur Sicherheit in kritischen Infrastrukturen verfasst.

Dr. Michael Falk
**Partner, Consulting, Cyber Security**
KPMG AG
Wirtschaftsprüfungsgesellschaft

Telefon: +49 (0)152 09087862
E-Mail: mfalk@kpmg.com

Dr. Michael Falk ist Partner im Bereich Security Consulting von KPMG. Seine Tätigkeitsschwerpunkte liegen im Aufbau von Managementsystemen zu Cyber Security und Privacy (Datenschutz) sowie in der strategischen Beratung von Security Transformationen. Er verantwortet diverse Projekte für große und mittelständische Mandanten und hat dabei u.a. Schwerpunkte auf die Risikobewertung neuer Technologien und auf Risikoquantifizierung gesetzt.

Markus Limbach
**Director, Consulting, Cyber Security**
KPMG AG
Wirtschaftsprüfungsgesellschaft

Telefon: +49 (0)174 3001998
E-Mail: mlimbach@kpmg.com

Markus Limbach verfügt über mehr als 15 Jahre Erfahrung in den Bereichen Cyber Security, Cloud Security und Business Continuity & Resilience Management. Zum Schutz vor Cyber-Bedrohungen und zur Herstellung eines angemessenen Sicherheitsniveaus unterstützt er seine nationalen und internationalen Kunden entlang des gesamten Lebenszyklus auf dem Weg zu einer cyber-resilienten Organisation – von der Definition der Security-Strategie bis zu deren organisatorischer und technischer Operationalisierung.

# KPMG AG Wirtschaftsprüfungsgesellschaft

KPMG ist ein weltweites Netzwerk rechtlich selbstständiger Firmen mit rund 236.000 Mitarbeitenden in 145 Ländern. Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist hier mit rund 12.200 Mitarbeitenden an 26 Standorten präsent. Die Leistungen gliedern sich in die Geschäftsbereiche Audit, Tax, Consulting und Deal Advisory.

KPMG berät Unternehmen zu allen Fragestellungen entlang der gesamten Wertschöpfungskette, beispielsweise bei der Entwicklung neuer Geschäftsmodelle, der Optimierung der Supply Chain ebenso wie zu Steuerungskonzepten und zu Fragen rund um Digital Labour und Cyber Security. Für wesentliche Wirtschaftsbranchen hat KPMG eine bereichsübergreifende Spezialisierung vorgenommen, mit der insbesondere Familienunternehmen und Mittelstand, Staat und öffentliche Hand sowie das Finanzwesen praxisnah beraten werden.

Die Begleitung von Transformationsprojekten ist ein Kernthema der Beratung. Dabei setzt die Beratungsgesellschaft auf eine multidisziplinäre Ausrichtung der Geschäftsbereiche Audit, Tax, Transactions & Restructuring sowie Consulting. Dadurch werden Kunden in betriebswirtschaftlichen, prozessualen, steuerlichen und rechtlichen Einzelfragen beraten.

KPMG betreut Mandanten jeder Größe und aus allen Branchen – vom mittelständischen Autozulieferer über die Regionalbank bis hin zu internationalen Pharma- und Medienunternehmen.

KONTAKT

KPMG AG
Wirtschaftsprüfungsgesellschaft

Dr. Michael Falk
Partner, Consulting, Cyber Security
Telefon: +49 (0)152 09087862
E-Mail: mfalk@kpmg.com
Website: www.kpmg.de

# Lünendonk & Hossenfelder GmbH

LÜNENDONK

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Management- und IT-Beratung, Wirtschaftsprüfung, Steuer- und Rechtsberatung, Facility Management und Instandhaltung sowie Personaldienstleistung (Zeitarbeit, Staffing).

Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk®-Listen und -Studien" heraus.

Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Unternehmer mit den Lünendonk-Service-Awards aus.

KONTAKT

Lünendonk & Hossenfelder GmbH

Mario Zillmann
Partner
Maximilianstraße 40, 87719 Mindelheim
Telefon: +49 8261-73140-0
E-Mail: zillmann@luenendonk.de
Website: www.luenendonk.de

# Studieninformation

www.luenendonk.de/agbs

Die hier dargestellte Studie wurde exklusiv für die KPMG Wirtschaftsprüfungsgesellschaft AG erstellt. Eine Zweitverwertung der Studienergebnisse ist nur unter Quellenangabe erlaubt. Eine Nutzung der Studie zu eigenen Marketing- oder Vertriebszwecken ist nicht gestattet.

Die Marke Lünendonk® ist geschützt und ist Eigentum des Unternehmens Lünendonk & Hossenfelder GmbH. Bei Fragen zur Studienlizenz steht Ihnen das Team von Lünendonk & Hossenfelder gerne zur Verfügung (Sekretariat@luenendonk.de).

Alle Informationen dieses Dokuments entsprechen dem Stand zum Veröffentlichungsdatum. Alle Berichte, Auskünfte und Informationen dieses Dokuments entstammen aus Quellen, die aus Sicht der Lünendonk & Hossenfelder GmbH verlässlich erscheinen. Die Richtigkeit dieser Quellen wird vom Herausgeber jedoch nicht garantiert. Enthaltene Meinungen reflektieren eine angemessene Beurteilung zum Zeitpunkt der Veröffentlichung, die ohne Vermerk verändert werden können.

Um weitere Vorteile eines Dokuments im PDF Format kennenzulernen, klicken Sie bitte auf den Hilfe-Leitfaden des Acrobat Reader, den Sie im aktuellen Dokument finden.

Acrobat Reader Leitfaden

LÜNENDONK

# ÜBER LÜNENDONK & HOSSENFELDER

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Management- und IT-Beratung, Wirtschaftsprüfung, Steuer- und Rechtsberatung, Facility Management und Instandhaltung sowie Personaldienstleistung (Zeitarbeit, Staffing). Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk®-Listen und -Studien" heraus. Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalisten.

Wirtschaftsprüfung & Steuerberatung

Managementberatung

Engineering Services

Informationstechnologie

Facility Management & Instandhaltung

Zeitarbeit & Personaldienstleistung


IMPRESSUM

Herausgeber:
Lünendonk & Hossenfelder GmbH
Maximilianstraße 40
87719 Mindelheim

Telefon: +49 8261 73140-0
Telefax: +49 8261 73140-66
E-Mail: info@luenendonk.de

Erfahren Sie mehr unter www.luenendonk.de

Autor:
Mario Zillmann, Partner

Bilderquellen:
Titel, © Adobe Stock / Gorodenkoff