LÜNENDONK



Lünendonk®-Studie 2022

IT im Wandel – wie die Cloud, der Fachkräftemangel und Cyber-Attacken die IT herausfordern

Eine Studie der Lünendonk & Hossenfelder GmbH in Zusammenarbeit mit

business factors



Inhaltsverzeichnis

VORWORT 3

METHODIK 4

DIGITALE TECHNOLOGIEN VERÄNDERN DAS BUSINESS 6

FAZIT UND AUSBLICK 15

UNTERNEHMENSPROFILE 17

Vorwort

Liebe Leserinnen, liebe Leser,

die IT-Welt dreht sich schneller denn je. Technologien wie Data Analytics, Künstliche Intelligenz oder Industrial Internet of Things (IIoT) werden für Unternehmen immer relevanter, um Wettbewerbsvorteile aufzubauen. Der Wertschöpfungsbeitrag der IT steigt infolgedessen. Doch es geht dabei längst nicht nur um die technische Implementierung einzelner Softwarelösungen und die Anpassung von Prozessen. Wer die Digitalisierung ernst nimmt, sollte diese als ganzheitliche Aufgabe betrachten, welche die gesamte Unternehmensorganisation, die Kultur und Geschäftsmodelle selbst betrifft. Es gilt also, keine Einzellösungen in wenigen Abteilungen zu entwickeln, sondern Silostrukturen aufzubrechen, Prozesse „end to end" zu betrachten, neue Messmetriken und Incentivierungsinstrumente zu nutzen und die Digitalisierung als Kern des Geschäftswesens zu betrachten.

Anhand dieser Anforderungen und Herausforderungen zeigt sich: Digitalisierung gehört in die Führungsebene. Die Zeit von Führungskräften ist jedoch knapp bemessen. Die StategieTage IT und IT-Security von business factors dienen daher seit jeher als effiziente Informationsquelle für IT-Strategien und als Plattform zum Austausch unter Gleichgesinnten. Den Teilnehmerinnen und Teilnehmern der StrategieTage wurde als Vorbereitung und Einstimmung auf die Events eine Onlinebefragung bereitgestellt, deren Ergebnisse in diesem Paper zusammengefasst wurden. Neben dem allgemeinen Digitalisierungsstatus widmete sich ein Schwerpunkt der IT-Security, welche nicht erst seit der Java-Sicherheitslücke Log4j besondere Aufmerksamkeit geschenkt wird, sondern bereits seit Jahren immer wichtiger für IT-Entscheider wird.

Weitere Marktanalysen, Trendentwicklungen und Studien zu den verschiedensten IT-Themen finden Sie auf der Website von Lünendonk & Hossenfelder.

Wir wünschen Ihnen eine nützliche Lektüre und freuen uns, Sie bald wieder auf einem StrategieTag begrüßen zu dürfen!

Herzliche Grüße

Tobias Ganowski & Atil Ural



Tobias Ganowski
Junior Consultant
Lünendonk & Hossenfelder GmbH



Atil Ural
Geschäftsführer
business factors Deutschland GmbH



Methodik

Lünendonk als führendes Marktforschungs- und Analystenunternehmen in Deutschland für die B2B-Dienstleistungsmärkte hat gemeinsam mit der Netzwerkplattform business factors zwei Befragungen unter IT-Verantwortlichen im Jahr 2021 durchgeführt. Die Ergebnisse beider Befragungen wurden für dieses Whitepaper zusammengeführt.

Themenschwerpunkte der ersten Befragung waren die Cloud sowie die IT-Modernisierung und die damit einhergehenden Business- und Technologieänderungen. 56 Personen, vornehmlich Security-Spezialistinnen und Spezialisten und Chief Information Officers (CIOs), diverser Branchen wurden befragt, wobei Finanzdienstleister einen Schwerpunkt darstellten. Die Unternehmen stammen zu 45 Prozent aus dem (gehobenen) Mittelstand, 55 Prozent weisen einen Umsatz von mehr als 1 Milliarde Euro auf.

Fokus der zweiten Befragung war das Themengebiet Cyber Security. Hieran beteiligten sich ebenfalls 56 Mittelständler und Großkonzerne, vornehmlich aus der Industrie und dem Financial-Services-Bereich. In beiden Fällen stammen die Unternehmen aus der DACH-Region (Deutschland, Österreich, Schweiz).

SAMPLE DER ERSTEN BEFRAGUNG

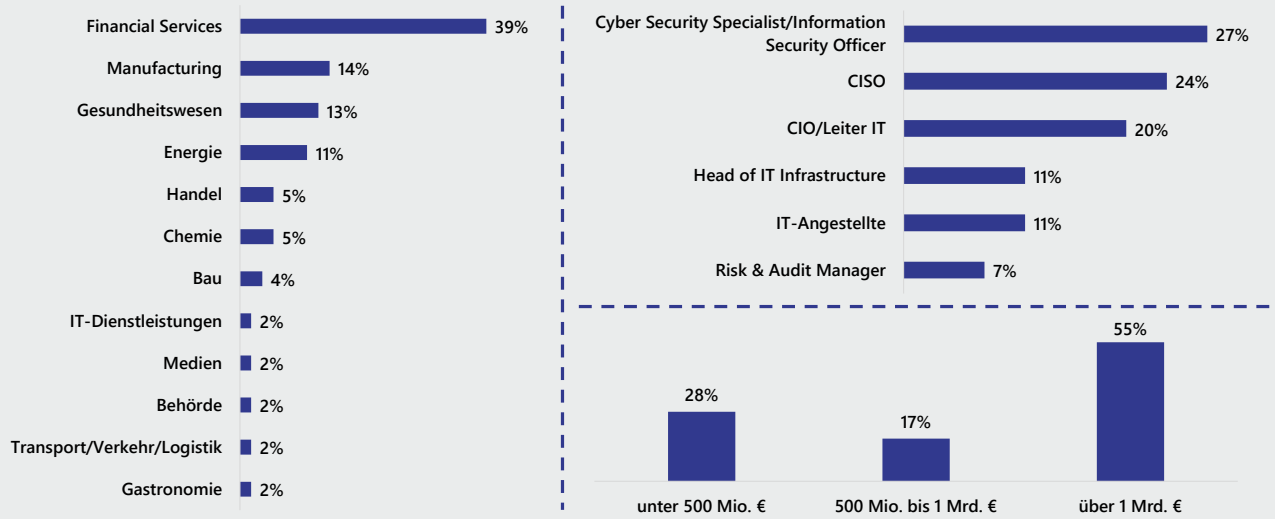


Abb. 1: Demografie der ersten Befragungszielgruppe; n = 56

SAMPLE DER ZWEITEN BEFRAGUNG

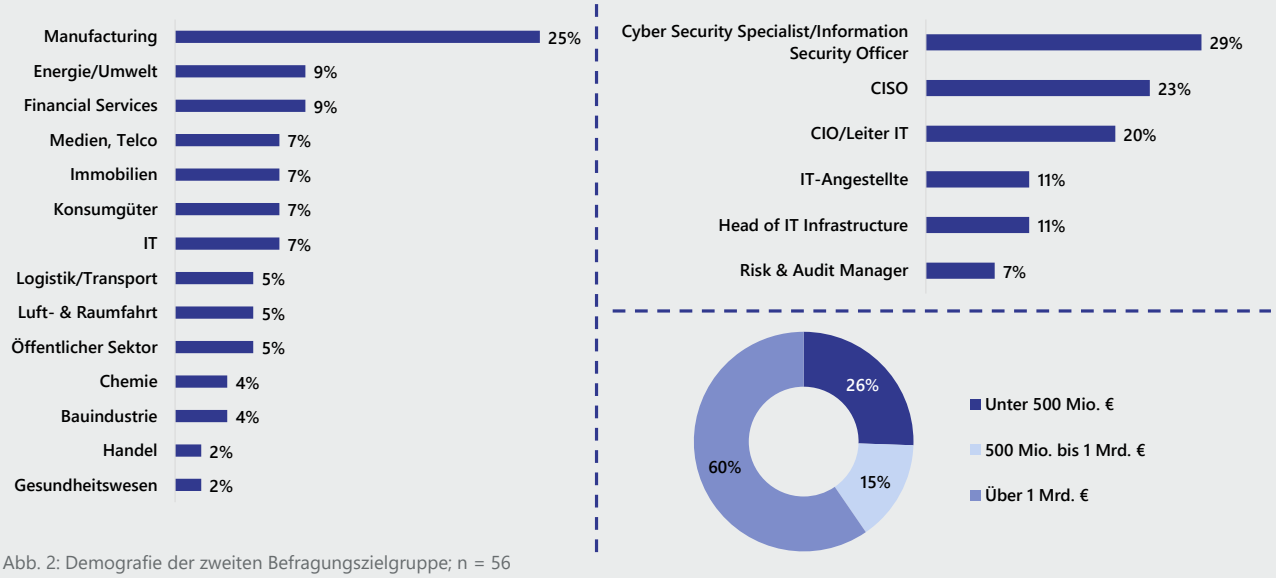


Abb. 2: Demografie der zweiten Befragungszielgruppe; n = 56



Digitale Technologien verändern das Business

Der Wertschöpfungsbeitrag der Digitalisierung in Unternehmen nimmt weiter zu. Digitale Technologien wie die Cloud, Data Analytics, Customer Experience Management oder Künstliche Intelligenz werden schon lange von Unternehmen genutzt, jedoch nicht mehr nur von einzelnen Abteilungen und Usern, sondern vermehrt unternehmensübergreifend. In der Produktion werden etwa Daten aus der Nutzung von Maschinen erhoben und in der Cloud ausgewertet, um die Produktqualität und Durchlaufzeiten zu optimieren. In Marketing und Vertrieb lassen sich mit moderner Softwareaufgaben automatisieren und mittels Customer Analytics Kundendaten auswerten, um individuelle und maßgeschneiderte Ansprachen und Angebote zu erstellen. Und auch die IT selbst wandelt sich, da sich das Verständnis der IT von einem Cost Center hin zum Innovationstreiber verschiebt.

Die IT wird für das Business damit immer wichtiger und eine enge Zusammenarbeit zwischen IT und den Fachbereichen somit unerlässlich. Um dem Business optimal helfen und Innovationen proaktiv in Fachbereiche hineintragen zu können, war es zunächst interessant zu erfahren, ob die IT auf dem Stand der aktuellen Technologien ist (State of the Art) und Kunden- und Marktanforderungen kennt.

38 Prozent der befragten Unternehmen bejahrten diese Frage voll und ganz, weitere 46 Prozent stimmen zumindest überwiegend zu. 12 Prozent sehen die eigene IT aber nur zu einem geringen Maß an den aktuellen Marktanforderungen ausgerichtet, sodass Gegenmaßnahmen dringend eingeleitet werden sollten.

DIE IT DER UNTERNEHMEN IST MEHRHEITLICH AUF DIE AKTUELLEN MARKTANFORDERUNGEN EINGESTELLT

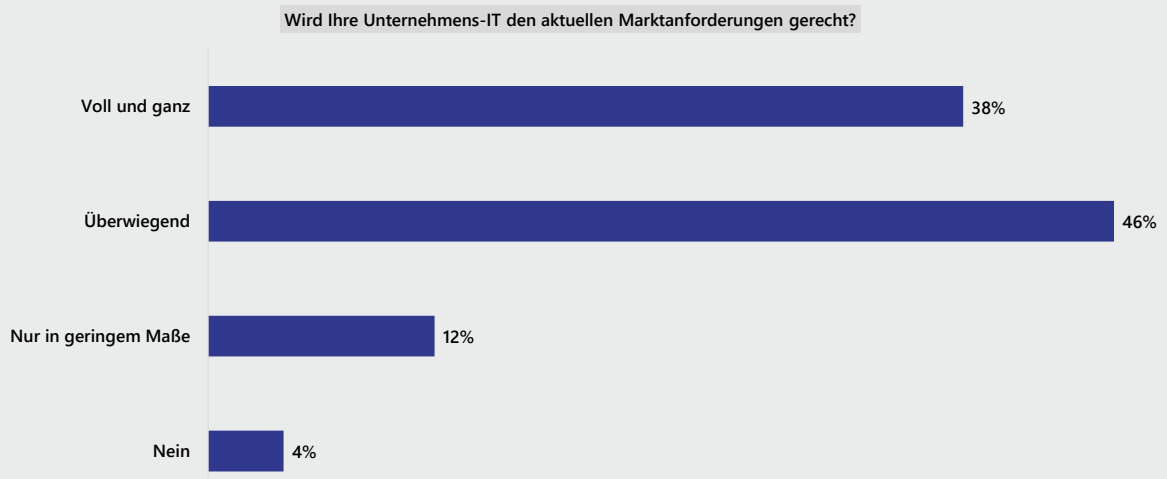


Abb. 3: Frage: Wird Ihre Unternehmens-IT den aktuellen Marktanforderungen gerecht?; n = 26

PERSONALMANGEL: EXTERNE DIENSTLEISTER STÄRKER GEFRAGT

Um von den Chancen der Digitalisierung profitieren zu können, müssen entsprechende Skills und Kompetenzen in den Unternehmen vorhanden sein. Seit Jahren herrscht jedoch ein Fachkräftemangel in der IT. Expertentum in der Softwareentwicklung, Information Um von den Chancen der Digitalisierung profitieren zu können, müssen entsprechende Skills und Kompetenzen in den Unternehmen vorhanden sein. Seit Jahren herrscht jedoch ein Fachkräftemangel in der IT. Expertentum in der Softwareentwicklung, Information Security oder Cloud-Architektur zählt zu den gefragtesten Skills und ausgeschriebene Stellen können oft monatelang nicht besetzt werden.

Externe Dienstleister wie IT-Beratungen, Systemhäuser oder Managed Services Provider (MSP) sind daher wichtige und gefragte Partner zur Bewältigung der digitalen Transformation: 31 Prozent der Befragten gehen davon aus, dass sie im Jahr 2025 deutlich mehr Managed Services, also externe IT-Dienstleistungen auf der Basis von Service Level Agreements (SLAs), von Dienstleistern in Anspruch nehmen werden als heute. Vor allem im Zuge der zunehmenden Cloud-Nutzung werden Managed Services immer wichtiger, beispielsweise um die multiplen und hybriden Cloud-Deployments zu orchestrieren – auch im Sinne von Cyber Security und Provider-Management.

Durch den Einkauf von Managed Services sollen Leistungen eingekauft werden, die intern nicht in der erforderlichen Qualität erbracht werden können oder bei denen der Einkauf durch die Nutzung von Skaleneffekten kostengünstiger ist als bei einer eigenen Leistungserbringung (Make or Buy).

55 Prozent der Befragten erwarten, dass in einem geringen Maße mehr Managed Services hinzukommen werden. Eine Minderheit von 14 Prozent geht davon aus, dass Managed Services im gleichen oder einem geringeren Umfang genutzt werden als heute. Der überwiegende Teil der Unternehmen möchte die Zusammenarbeit mit IT-Dienstleistern somit intensivieren.

MANAGED SERVICES NEHMEN AN BEDEUTUNG ZU

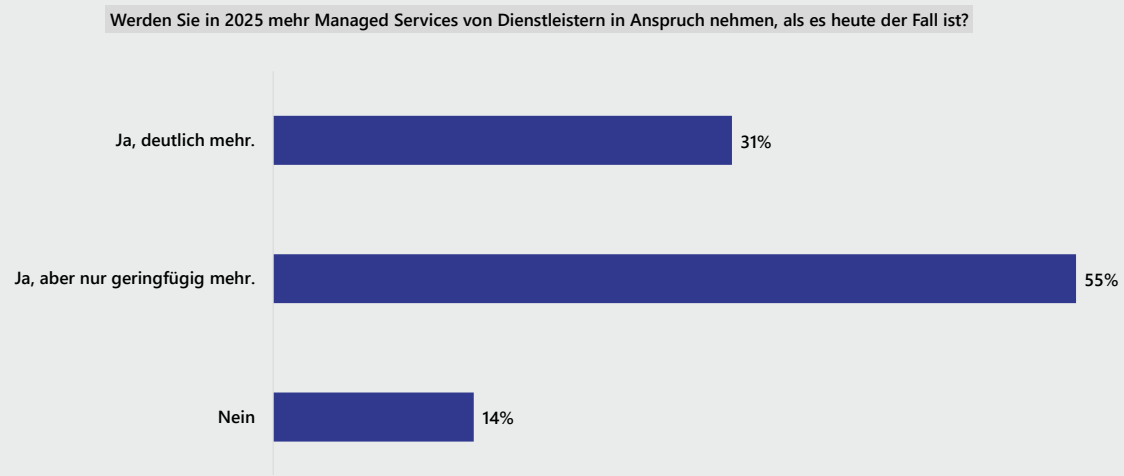


Abb. 4: Frage: Werden Sie in 2025 mehr Managed Services von Dienstleistern in Anspruch nehmen, als es heute der Fall ist?; n = 51

CLOUD: GEKOMMEN, UM ZU BLEIBEN

Der vermutlich wichtigste digitale Trend, sei es für Kundenunternehmen oder auch die IT-Dienstleister selbst, dürfte die Verlagerung von Infrastruktur, Plattformen und Anwendungen in die Cloud sein. Insbesondere Großunternehmen und Konzerne beschäftigen sich seit Jahren mit der Cloud. Mittelständische Unternehmen ziehen nun seit einigen Jahren – spätestens aber seit Ausbruch der Corona-Pandemie – nach. Dies betrifft etwa den digitalen Arbeitsplatz oder die Digitalisierung von Kundenschnittstellen, vor allem aber erhofft man sich von der IT-Modernisierung und dem Umbau zu einer Cloud-native-IT-Landschaft dringend notwendige Effizienzsteigerungen. Da die Hyperscaler um AWS, Microsoft Azure und Google Cloud jedoch alle aus den USA stammen und somit den dortigen Rechten – und nicht der DSGVO – unterliegen, zweifelt ein nicht unwesentlicher Anteil der Unternehmen an der Cloud. Auch fehlt es einigen Unternehmen schlicht und ergreifend an Erfahrung, wie durch die Cloud Mehrwerte geschaffen werden können, welche Auswirkungen Cloud-Sourcing auf die IT hat und welche Prozessanpassungen erforderlich sind.

14 Prozent der Befragten wollen in den nächsten drei Jahren einen Cloud-only-Ansatz verfolgen und somit IT-Applikationen ausschließlich aus der Cloud beziehen respektive in der Cloud hosten und nicht on premise. Einen großen Teil ihrer Applikationen in die Cloud verlagern möchten 48 Prozent der befragten Unternehmen. Einige wenige Anwendungen, etwa besonders unternehmenskritische Daten und Anwendungen, sollen bei diesen Unternehmen weiterhin on premise betrieben werden. Eine gegenteilige Strategie, dass nur ein kleiner Teil in die Cloud verlagert werden soll, beabsichtigen 36 Prozent der Befragten. Weitere Lünendonk®-Studien wie die Studie "Cloud-native Software Development" bestätigen den Trend hin zur Cloud und hybriden Cloud- und On-premise-Umgebungen.

DIE CLOUD-TRANSFORMATION IST IM GANGE

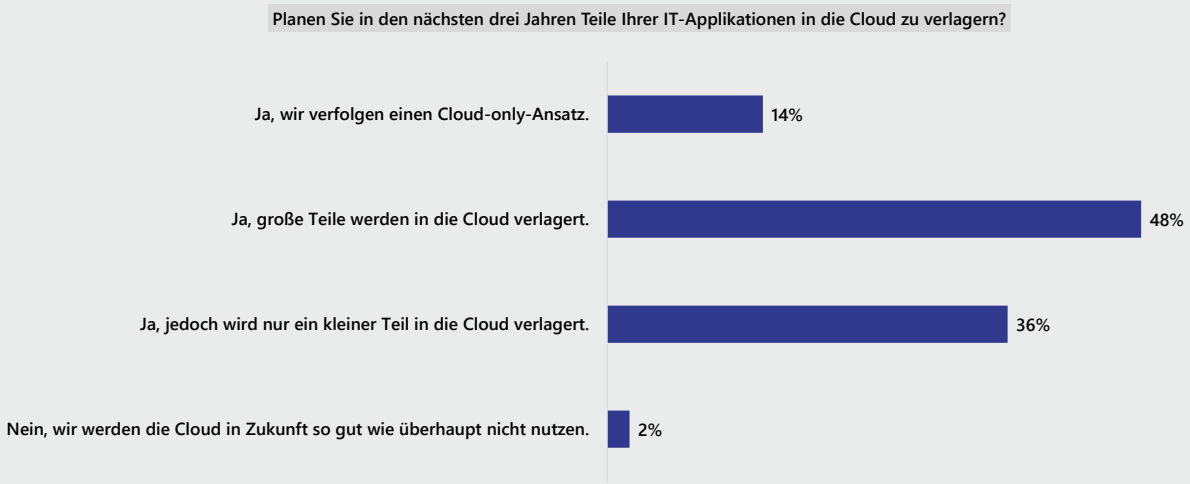


Abb. 5: Frage: Planen Sie in den nächsten drei Jahren Teile Ihrer IT-Applikationen in die Cloud zu verlagern?; n = 50

CYBER SECURITY: NICHT NUR IN DER CLOUD VON ZENTRALER BEDEUTUNG

Nicht nur der Cloud-Trend, sondern auch der allgemein ansteigende Digitalisierungsgrad führt dazu, dass die IT-Systeme und Anwendungen sicher aufgesetzt werden müssen und infolgedessen steigende Budgets für Cyber Security notwendig sind.

Nicht erst seit der Java-Schwachstelle Log4j, welche Ende 2021 aufgedeckt wurde, und der damit einhergehenden Warnung des Bundesamtes für Sicherheit und Informationstechnik (BSI), sondern bereits seit einigen Jahren hat sich die Wahrnehmung von Cyber-Angriffen und Datensicherheit spürbar verändert. Der IT-Branchenverband bitkom berechnet etwa den jährlichen Schaden durch Cyber-Attacken auf etwa 223 Milliarden Euro für die deutsche Wirtschaft für 2020/2021. 2018/2018 lag der Wert noch bei 103 Milliarden Euro, die Schadensumme stieg damit auf mehr als das Doppelte an. 86 Prozent der befragten

Unternehmen wurden demnach bereits Opfer eines Cyberangriffs, 2019 lag der Anteil noch bei 70 Prozent. Die Wahrscheinlichkeit eines Angriffs steigt somit – Unternehmen sollten dafür gewappnet sein. Doch wie schätzen sie ihre aktuellen Schutz- und Sicherheitsmaßnahmen in der IT ein?

Im Großen und Ganzen sehen sich die Unternehmen hinsichtlich ihrer IT-Security gut aufgestellt: 33 Prozent sehen keine Notwendigkeit, Maßnahmen zur Verbesserung der IT Security einzuleiten. Die Hälfte der Unternehmen (50 %) plant geringfügige Verbesserungen, um sich besser vor Cyber-Attacken zu schützen. Einen großen Handlungsbedarf, etwa aufgrund fehlender Verantwortlichkeiten oder veralteter Sicherheitslösungen, sehen 8 Prozent der Befragten. Ebenfalls 8 Prozent können ihr Cyber-Security-Niveau nicht beurteilen. Diesen Unternehmen ist zu raten, etwa durch einen externen Provider oder einen internen Kontrollmechanismus eine Validierung der Cyber-Resilienz vornehmen zu lassen, um mögliche Schwachstellen aufzuzeigen. Bei den positiven Ergebnissen der Befragung gilt es jedoch zu beachten, dass Schwachstellen häufig erst entdeckt werden, wenn es zu spät ist und Angreifende bereits erfolgreich in Systeme eingedrungen sind und Teile oder komplette Systeme lahmgelegt haben.

DAS IT-SECURITY-NIVEAU WIRD GRÖSSTENTEILS ALS HOCH EINGESCHÄTZT

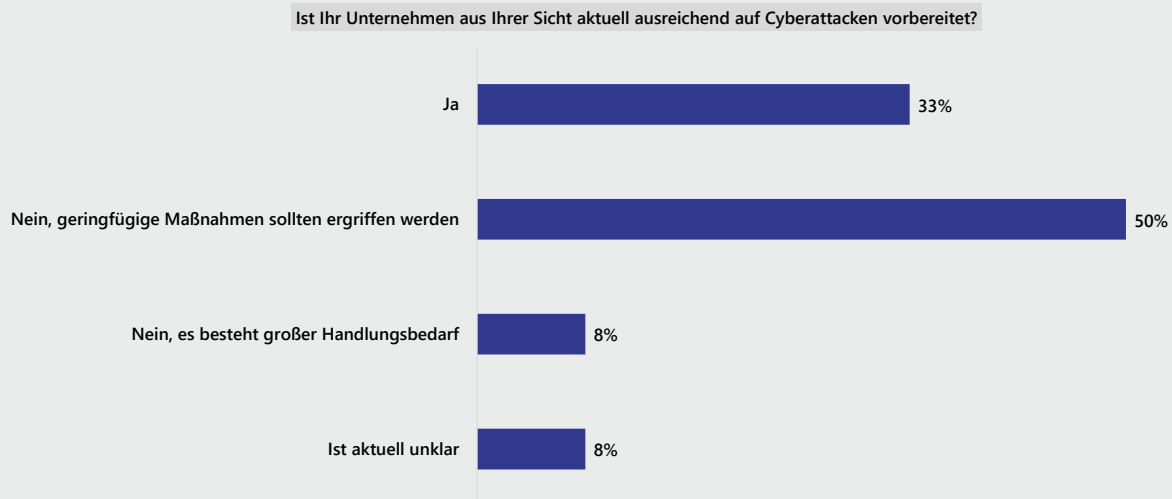


Abb. 6: Frage: Ist Ihr Unternehmen aus Ihrer Sicht aktuell ausreichend auf Cyberattacken vorbereitet?; n = 48

CLOUD-SECURITY WIRD KONTROVERS DISKUTIERT

Welche Auswirkungen hat jedoch die Cloud auf die IT-Security? Sowohl Cloud-only- als auch hybride Konzepte erfordern neue Sicherheitsmechanismen und eine veränderte IT-Security-Architektur. Viele der befragten Unternehmen sind sich bislang noch nicht einig,

ES BESTEHT UNEINIGKEIT DARÜBER, OB DIE CLOUD DAS IT-SECURITY-NIVEAU ERHÖHT

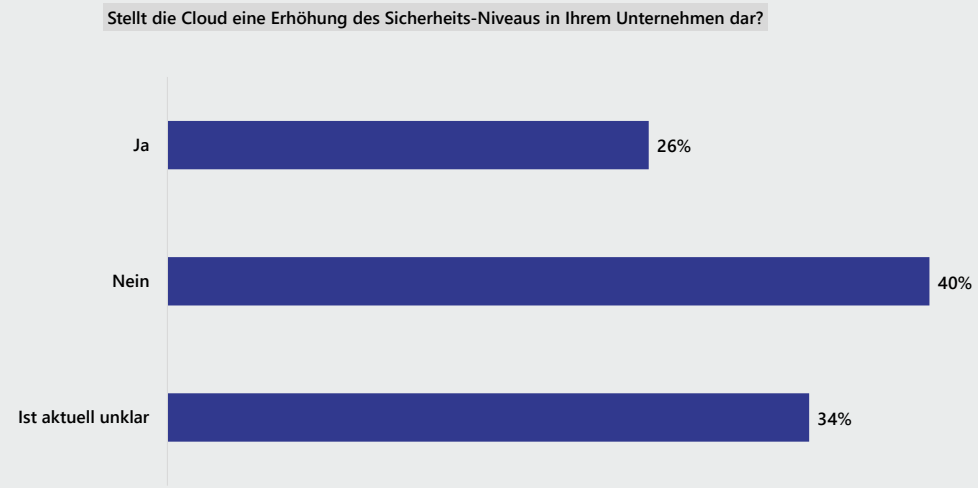


Abb. 7: Frage: Ist Ihr Unternehmen aus Ihrer Sicht aktuell ausreichend auf Cyberattacken vorbereitet?; n = 48

ob die Cloud eine Erhöhung oder eine Verschlechterung des Sicherheitsniveaus bewirkt: 26 Prozent erwarten mehr IT-Sicherheit durch Cloud-Sourcing, 40 Prozent stimmen dieser Aussage nicht zu. Ein Drittel (34 %) der Befragten kann derzeit keine valide Einschätzung abgeben, etwa aufgrund fehlender Erfahrung oder da mögliche Konzepte und Lösungen erst noch diskutiert werden.

Objektiv betrachtet wird das Sicherheitsniveau in der Cloud im Gegensatz zum Eigenbetrieb im Rechenzentrum aber höher, da die Cloud-Anbieter massiv in die IT-Security investieren und modernste Technologien im Bereich der Künstlichen Intelligenz einsetzen. Das alles hat zu einem erhöhten Vertrauen in das Sicherheitsniveau in der Cloud geführt.

Unterschiedliche Studien von Lünendonk zeigen, dass sich hinsichtlich des Vertrauens einiges verändert hat und die Sicherheitsstandards in der Cloud von immer mehr CIOs mittlerweile als besser eingeschätzt werden als diejenigen in klassischen Rechenzentrumsumgebungen. Vertrauen in die Cloud wird mittlerweile beispielsweise durch regelmäßige IT-Security-Audits aufgebaut oder durch die Übertragung des Managements der Cloud-Umgebungen an einen Managed Service Provider.

MANAGED SECURITY SERVICES SORGEN FÜR MEHR SICHERHEIT

Wie bereits erwähnt zählen IT-Security-Expertinnen und Experten zu den am stärksten nachgefragten IT-Fachkräften und sind daher schwer zu rekrutieren. Zur Einhaltung eines hohen IT-Sicherheitsniveaus werden daher standardisierte Managed Security Services eingesetzt, indem Sicherheitsanforderungen einer Organisation durch einen externen

Dienstleister verwaltet werden. Häufig genutzte Leistungen sind die E-Mail-Sicherheit, die Absicherung der Netzwerke und das Monitoring von Vorfällen – sogenannten Incidents. Über die Hälfte der Unternehmen (57 %) nutzen derartige Services bereits heute, weitere 30 Prozent planen, in den kommenden zwei Jahren Managed Security Services zu beziehen. 11 Prozent der Befragten nutzen keine externen Services, da ausreichend eigene Lösungen vorhanden sind.

MANAGED SECURITY SERVICES SIND FESTER BESTANDTEIL DER SECURITY-STRATEGIE

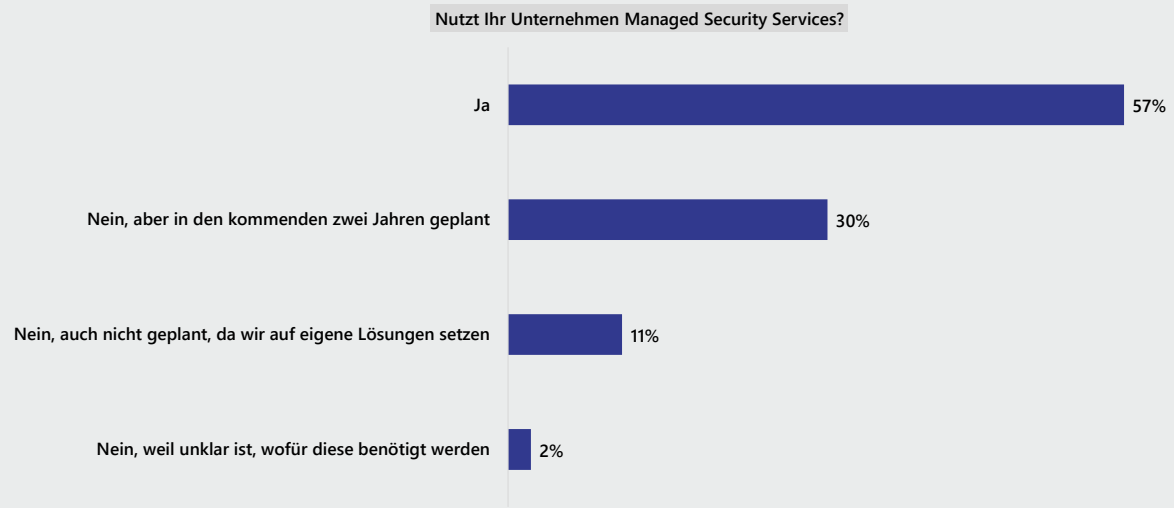


Abb. 8: Frage: Nutzt Ihr Unternehmen Managed Security Services?; n = 47

Der Markt für Security-Lösungen ist dabei nicht wirklich transparent. So gibt es diverse Hersteller und Softwarenanbieter, die wiederum unterschiedliche Lösungen für unterschiedliche Kundenbedürfnisse haben. Microsoft bietet nicht nur das führende Betriebssystem für Computer an und zählt zu den Top 3 führenden Public-Cloud-Anbietern, sondern hat auch eigene Security-Lösungen im Portfolio und verfügt damit über ein ganzheitliches Software-Ökosystem.

Auch in den kommenden Jahren soll massiv in die Cyber Security investiert werden: Microsoft-CEO Satya Nadella verkündete 2021 nach einem Meeting mit US-Präsident Biden, dass Microsoft in den kommenden fünf Jahren 20 Milliarden Dollar in die Weiterentwicklung seiner Sicherheitslösungen stecken werde und Cyber Security auf der Strategie-Agenda somit weit oben verankert werde. Dieses Commitment von Microsoft zu einer modernen Cyber Security hat jedoch nicht automatisch zur Folge, dass die IT-Security-Strategien von Unternehmen auf den Microsoft-Lösungen basieren. Schließlich gibt es eine Vielzahl weiterer Security-Provider, die ebenfalls entsprechende Lösungen

MICROSOFT-LÖSUNGEN WIRD ÄHNLICH HÄUFIG GENUTZT WIE INDEPENDENT SECURITY SOFTWARE VENDORS

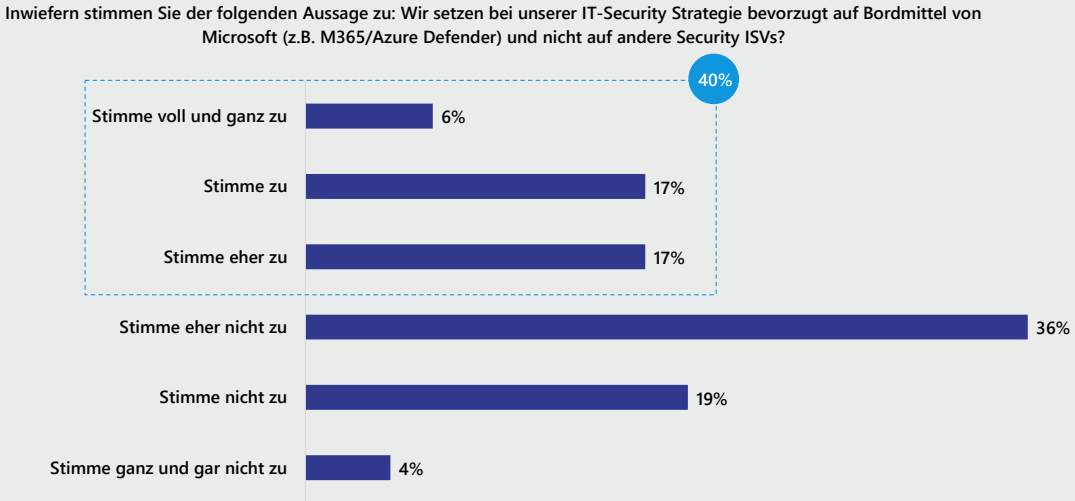


Abb. 9: Frage: Nutzt Ihr Unternehmen Managed Security Services?; n = 47

anbieten. Auch kann es vorkommen, dass sich Unternehmen ganz bewusst nicht für Microsoft, sondern für Independent Software Vendors (ISVs) entscheiden – etwa um einen Vendor-Lock-in zu vermeiden. Unter den befragten IT-Führungskräften bevorzugen in jedem Fall 40 Prozent Microsoft-Lösungen im Security-Umfeld, während 60 Prozent anderweitige Security-Produkte nutzen.

SOC: SECURITY OPERATIONS CENTERS SIND IM KOMMEN

Infolge der immer häufigeren und komplexeren Cyber-Attacken auf Unternehmen stellt sich für IT-Abteilungen die Frage, wie man in Zukunft diese Welle brechen kann. Im Trend liegen hierbei die sogenannten Security Operations Centers (SOCs). Ein SOC zentralisiert die Kompetenzen von Security-Fachleuten, um eine eigene Einheit zu schaffen, die sich vollständig auf die Cyber-Abwehr konzentriert und losgelöst von anderen IT-Teams agiert. Ein SOC muss nicht zwangsläufig intern betrieben werden, sondern kann auch ausgelagert und als Managed Security Service oder SOC as a Service (SOCaaS) bezogen werden. Schwerpunkt des SOC ist in der Regel die Prävention, sodass Gefahren proaktiv mittels Technologien wie Endpoint Detection oder Security Information and Event Management (SIEM) vorgebeugt werden. Sofern ein Sicherheitsvorfall eingetreten ist, reagiert das SOC mit entsprechenden Maßnahmen. SOCs überwachen daher die gesamte IT-Security und alle Vorfälle – 24 Stunden am Tag, 7 Tage die Woche. Aufgrund des bereits angesprochenen Mangels an Security-Fachleuten oder aus Kostengründen lagern 38 Prozent der befragten Unternehmen das SOC an einen externen Dienstleister aus. 31 Prozent verfügen über ein internes SOC, weitere 31 Prozent nutzen eine hybride Form, in der einige Leistungen intern durch eigenes Personal erbracht und einige extern bezogen werden.

40 Prozent der befragten Unternehmen verfügen heute bereits über ein SOC, 30 Prozent planen dessen Einführung. Lediglich jedes vierte Unternehmen sieht keine Notwendigkeit für die Nutzung eines SOC.

SECURITY OPERATIONS CENTER ETABLIEREN SICH

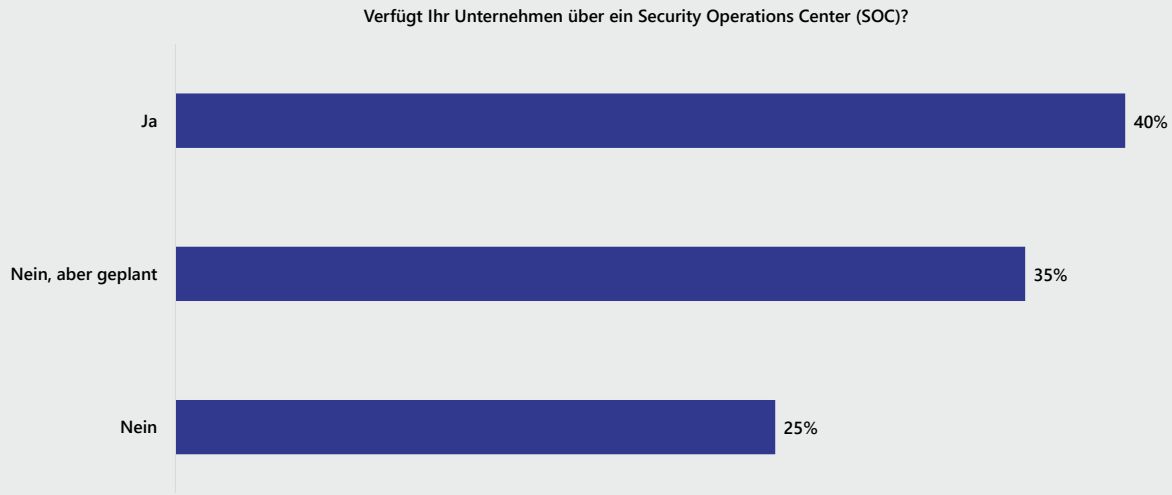


Abb. 10: Frage: Verfügt Ihr Unternehmen über ein Security Operations Center (SOC)?; n = 48

SOCS WERDEN REIN EXTERN, INTERN ALS AUCH HYBRID BETRIEBEN

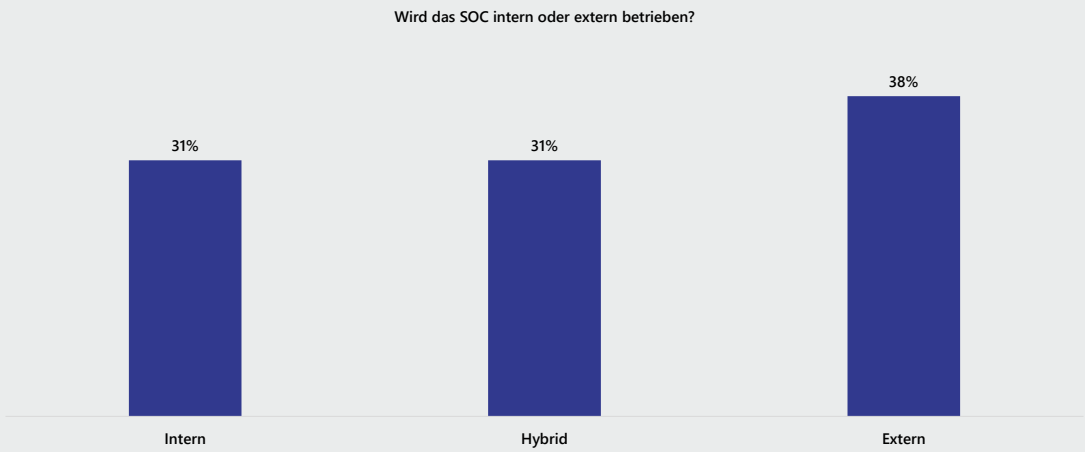


Abb. 11: Frage: Wie wird Ihr SOC betrieben?; n = 39



Fazit und Ausblick

Die Digitalisierung bietet Unternehmen völlig neue Chancen und Geschäftsmöglichkeiten, fordert Entscheiderinnen und Entscheider aber auch sehr stark heraus und verlangt eine Business-Transformation. Die große Mehrheit der befragten IT-Verantwortlichen sieht ihre IT adäquat für die aktuellen Marktanforderungen aufgestellt. Die IT sollte dabei verstärkt mit dem Business zusammenarbeiten, etwa in Form von crossfunktionalen Produktteams, sodass gemeinsam digitale Produkte und Services entwickelt werden und Security-Aspekte direkt in die Produktentwicklung miteinfließen (Security by Design). Die Cloud ist fester Bestandteil dieser Entwicklung: Vor allem hybride Ansätze, in denen On-premise-Betrieb, Private und Public Cloud kombiniert werden, kommen zum Einsatz. Einen Cloud-only-Ansatz können sich aufgrund von Altlasten und Legacy-Systemen nur die wenigsten Unternehmen vorstellen – ebenso wie die vollständige Vermeidung einer Cloud-Nutzung.

Eine der größten Herausforderungen der digitalen Transformation ist weiterhin der IT-Fachkräftemangel. Managed Services externer IT-Dienstleister dürften daher zukünftig noch stärker als heute nachgefragt werden, um den IT-Betrieb aufrechtzuerhalten. Auch für die Entwicklung digitaler Lösungen oder zur Unterstützung bei der Entwicklung einer Digitalisierungsstrategie werden IT-Dienstleister als wichtige Partner angesehen.

Infolge des zunehmenden Digitalisierungsgrades gilt es, auch die IT-Security auf ein höheres Niveau zu heben. Es geht längst nicht mehr nur darum, den Schutz eigener Daten zu gewährleisten, sondern es müssen auch sensible Kundendaten geschützt werden, die bei der Nutzung digitaler Geschäftsmodelle gesammelt werden. Das eigene

IT im Wandel – wie die Cloud, der Fachkräftemangel und Cyber-Attacken die IT herausfordern

IT-Sicherheitsniveau empfinden die meisten Unternehmen als gut, jedoch zeigen sich Schwachstellen oftmals erst dann, wenn es bereits zu spät ist und ein Cyber-Angriff erfolgt ist. Ein externer Blick kann dabei helfen, Sicherheitsrisiken zu reduzieren. Ob die Cloud eine Erhöhung oder eine Verminderung des IT-Sicherheitsniveaus darstellt, darüber sind sich die Unternehmen uneinig – zu Teilen auch überfragt. Managed Security Services werden stark nachgefragt, da sich die Bedrohungslage permanent verändert und eine stets aktuelle Security essenziell ist. Auch setzen IT-Entscheiderinnen und Entscheider zunehmend auf Security Operations Centers, um Cyber-Security-Kompetenzen zu bündeln. Diese werden sowohl rein intern, rein extern als auch hybrid betrieben. IT-Security wird somit nicht mehr nur als reiner Kosten-, sondern auch als Wertschöpfungsfaktor betrachtet, um digitale Innovationen zu ermöglichen und abzusichern.

UNTERNEHMENSPROFIL

business factors Deutschland GmbH



KONTAKT

business factors Deutschland GmbH

Atil Ural
Geschäftsführer
Tauentzienstraße 15, 10789 Berlin
Telefon: +49 8261 73140-0
Mobil: +49 160 750 12 12
E-Mail: atil.ural@businessfactors.de
Website: https://www.businessfactors.de

Als Kongressveranstalter schafft business factors exklusive Kommunikationsräume für hochrangige Führungskräfte deutscher und internationaler Unternehmen. Unser umfangreiches Leistungsspektrum umfasst die Konzeption sowie die Ansprache und Betreuung der persönlich geladenen Führungskräfte; unterstützt durch unsere Organisation füreine optimale Durchführung unserer Wirtschaftskongresse. Das strikte Augenmerk liegt dabei stets auf der Gleichrangigkeit unserer Teilnehmer sowie der individualisierten Vor- und Nachbereitung von Kontakten zur wegweisenden Ausweitung und Vertiefung des Netzwerks jedes Einzelnen.

Als unabhängiger Kongressveranstalter zeichnet sich business factors verantwortlich für maßgebende Kongresse für Führungskräfte u. a. in den Bereichen IT, HR, Vertrieb, Marketing, Energie, Industrie und Finance. Diese bieten den Teilnehmern erstklassige Möglichkeiten, sich umfassend zu informieren, auszutauschen und in den entscheidenden Themen zu vernetzen.

Als Anbieter von Managed Events konzipiert und organisiert business factors maßgeschneiderte Veranstaltungen für Ihr Unternehmen. Von exklusiven Business-Soiréen im kleinen Kreis bis hin zu mehrtägigen Konferenzforen zur Präsentation Ihrer Themen: Nutzen Sie unsere Erfahrung, Expertise und Netzwerke im Bereich hochklassiger Wirtschaftskongresse, um eigene Veranstaltungen entsprechend Ihrer Marketingstrategie fokussiert umzusetzen und den für Sie relevanten Teilnehmerkreis vor Ort begrüßen zu können.

Mit langjähriger Erfahrung und begeisterten Mitarbeitern setzt business factors als unabhängiges Veranstaltungsforum Standards für progressive Wirtschaftskongresse und schafft so exklusive Kommunikationsräume für hochrangige Führungskräfte deutscher und internationaler Unternehmen. business factors greift die entscheidenden, aktuellen Themenschwerpunkte des Arbeitsalltags auf und bietet das zielgenaue Format zur Entwicklung von Lösungsstrategien, im fokussierten Dialog von Entscheidern, Wissensmultiplikatoren und Kompetenzpartnern.

UNTERNEHMENSPROFIL

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

Tobias Ganowski
Junior Consultant
Maximilianstraße 40, 87719 Mindelheim
Telefon: +49 8261 73140-0
E-Mail: ganowski@luenendonk.de
Website: www.luenendonk.de

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

Autoren:
Tobias Ganowski, Junior Consultant
Mario Zillmann, Partner

Bilderquellen:
Titel, S.4, 6 und 15 © Adobe Stock / greenfutterfly

Copyright © 2022 Lünendonk & Hossenfelder GmbH, Mindelheim. Alle Rechte vorbehalten.