CIO CSO COMPUTERWOCHE VOICE OF DIGITAL

IT-SECURITY. IM ZEICHEN EUROPÄISCHER DATENSOUVERÄNITÄT.

In Zusammenarbeit mit unserem exklusiven Studienpartner

mimecast

INHALT

IMPRESSUM

Fragebogenentwicklung:
Bernd Hohlweg (Mimecast),
Halime-Merve Ersan (Mimecast),
Matthias Teichmann (Foundry)

Endredaktion /
CvD Studienberichtsband:
Matthias Teichmann

Analysen / Kommentierungen:
Oliver Schonschek, Bad Ems

Hosting / Koordination
Feldarbeit:
Armin Rozsa
(Foundry)

Studienpartner:
Mimecast Germany GmbH
Kistlerhofstraße 172
81379 München
Telefon: +49 89 904 200 800
www.mimecast.com/de

Grafik:
Patrick Birnbreier, München

Umschlaggestaltung unter
Verwendung einer Illustration
von © shutterstock / pancha.me

Lektorat:
Elke Reinhold, München

Ansprechpartner:
Matthias Teichmann
matthias.teichmann@foundryco.com

Foundry
(formerly IDG Communications)

Anschrift:
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086 0
Fax: +49 89 36086 118
E-Mail: info@idg.de

Vertretungsberechtigter:
Maria Savvidou

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com

EINLEITUNG

Die Rolle von IT-Security-Dienstleistern hat sich stark gewandelt. Ging es früher rein um die Abwehr technischer Angriffe, fungieren IT-Sicherheitsanbieter vor dem Hintergrund wachsender globaler Cyberbedrohungen, zunehmender Digitalisierung und hybrider Arbeitsmodelle als strategische Partner für ganzheitliche Sicherheits- und Compliance-Konzepte. Sie helfen Unternehmen dabei, resiliente IT-Infrastrukturen aufzubauen und regulatorische Anforderungen – wie etwa DSGVO oder NIS2 – technisch und organisatorisch umzusetzen.

Ein vertrauenswürdiger IT-Security-Partner sollte Transparenz, Nachvollziehbarkeit und Rechtssicherheit bei der Datenverarbeitung gewährleisten. Aufgrund der geopolitischen Unsicherheiten steht dies in Frage, weswegen der Wahl eines solchen Dienstleisters immer stärkere Bedeutung zukommt. Kann Datenhoheit und Compliance mit europäischen Datenschutzstandards gewährleistet bleiben, wenn z. B. US-Gesetze wie der CLOUD Act US-amerikanischen Behörden unter bestimmten Umständen den Zugriff auf Daten erlauben, selbst wenn diese in Europa gespeichert sind?

Ändern sich unter diesen Vorzeichen aktuell die Kriterien der Unternehmen bei der Auswahl eines geeigneten IT-Sicherheitsdienstleisters? Welche sind ausschlaggebend: technologische Expertise oder Datenhoheit und Compliance?

MANAGEMENT SUMMARY

Die Key Findings im Überblick

Kontrolle über die Dateninfrastruktur ist von größter Bedeutung

Während ein Drittel der Unternehmen die Fachkompetenz des eigenen Personals für die digitale Souveränität als sehr wichtig einstuft, sagen zwei von drei Unternehmen, die Dateninfrastruktur müsse unter Kontrolle sein. Datenschutz und Compliance ist in größeren Unternehmen zweitwichtigstes Kriterium.

Expertise und Datenschutz sind entscheidend, auch ohne Zertifizierung

68 Prozent suchen nach IT-Sicherheitsanbietern mit Expertise, 64 Prozent der Unternehmen achten auf Compliance. Aber nur 10 Prozent wollen Zertifizierungen von den IT-Sicherheitsanbietern sehen.

Größere Unternehmen achten besonders auf Geopolitik und Datenhoheit

Mehr als neun von zehn der Unternehmen mit über 1.000 Beschäftigen bestätigen, dass ihre Entscheidung für IT-Sicherheitsanbieter von Fragen zur Datenhoheit und Geopolitik beeinflusst wird.

1

Sichere Dateninfrastruktur ist entscheidender als Fachkompetenz

Für die befragten Unternehmen in Deutschland sind die Kontrolle über die Dateninfrastruktur, die technische Unabhängigkeit sowie Compliance und Datenschutz die drei wichtigsten Kriterien zur Bewertung und Aufrechterhaltung der digitalen Souveränität in ihrer Organisation. Deutlich dahinter liegen die Geschäftskontiunität, die Fachkompetenz des eigenen Personals und die Qualität der Partnerschaften.

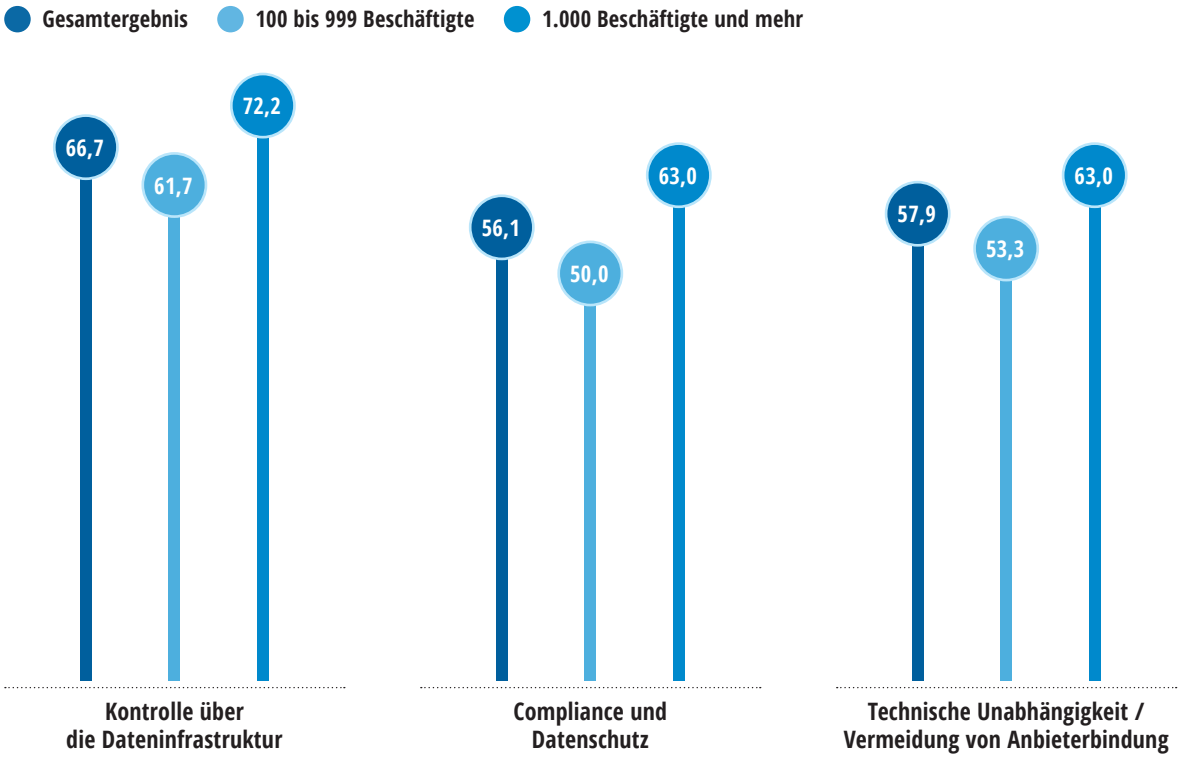
Größere Unternehmen mit mindestens 1.000 Beschäftigten nennen mit 72 Prozent der Antworten noch häufiger die Kontrolle über die Dateninfrastruktur als wichtigstes Kriterium einer digitalen Souveränität. Kleinere Unternehmen mit unter 1.000 Mitarbeitenden sagen dies zu 62 Prozent. Auch die Plätze 2 und 3 unter den wichtigsten Kriterien für digitale Souveränität erhalten bei den größeren Unternehmen einen jeweils höheren Zuspruch.

Die kleineren Unternehmen mit unter 1.000 Beschäftigten sagen zu 53 Prozent, dass sie die Vermeidung einer Anbieterabhängigkeit als wichtiges Kriterium für digitale Souveränität erachten, bei den größeren sind es sogar 63 Prozent.

Datenschutz und Compliance gewinnen immer mehr an Bedeutung: Bei den kleineren Unternehmen entfallen 50 Prozent der Antworten auf dieses Kriterium, was Platz 3 entspricht.

Bitte nennen Sie die drei wichtigsten Kriterien zur Bewertung und Aufrechterhaltung der digitalen Souveränität in Ihrer Organisation.

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 114



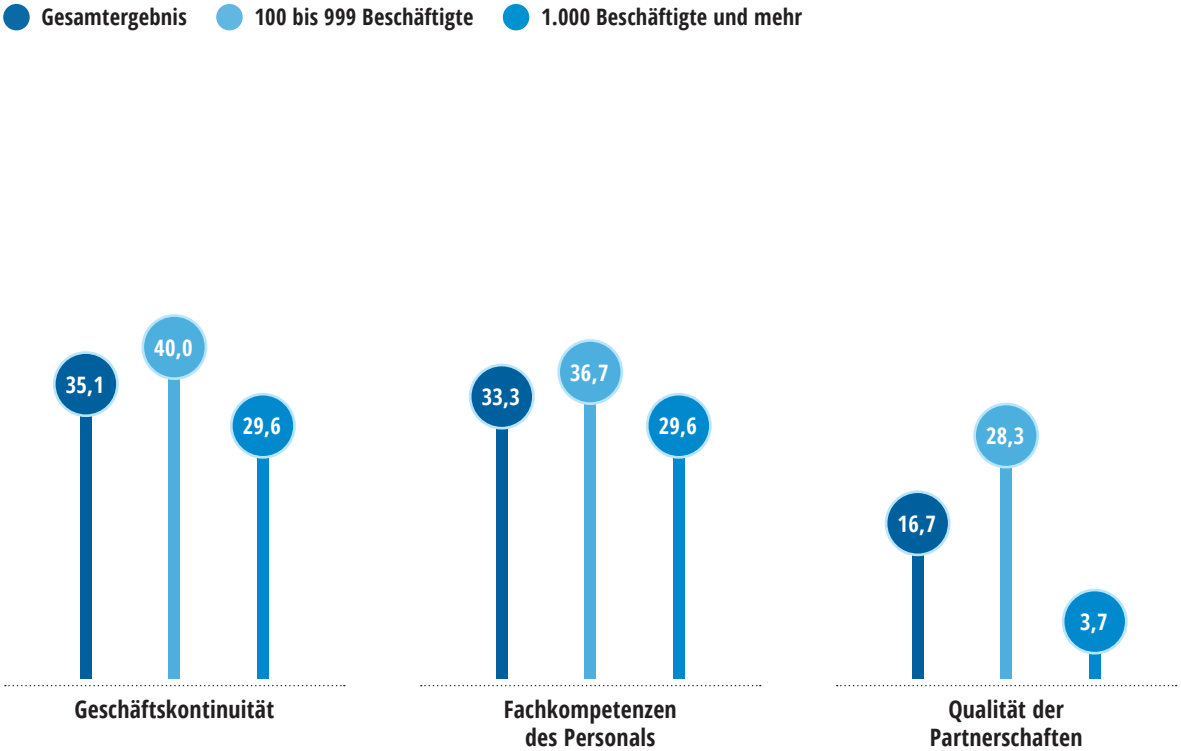
In den größeren Unternehmen kommt Datenschutz und Compliance noch deutlich größere Bedeutung zu: Hier ist es mit 63 Prozent der Antworten sogar das zweitwichtigste Kriterium hinter der sicheren Dateninfrastruktur.

Die Kriterien der Geschäftskontinuität, der Fachkompetenz und der Qualität der Partnerschaften liegen eindeutig auf den hinteren Plätzen. In diesem Kontext sollte aber nicht vergessen werden, dass zum Beispiel kompetentes Personal und hochwertige Partnerschaften eine große Bedeutung für eine sichere Dateninfrastruktur, die Anbieterunabhängigkeit und die Einhaltung von Datenschutz und Compliance spielen können.

„Datenschutz und Compliance gewinnen immer mehr an Bedeutung, insbesondere in größeren Unternehmen."

Bitte nennen Sie die drei wichtigsten Kriterien zur Bewertung und Aufrechterhaltung der digitalen Souveränität in Ihrer Organisation.

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 114



2

IT-Sicherheitsanbieter können mit Expertise und Datenschutz überzeugen

68 Prozent der befragten Unternehmen in Deutschland achten besonders auf die technologische Expertise und das Prozesswissen bei der Auswahl eines IT-Sicherheitsanbieters. Für 64 Prozent der Befragten kommt es besonders auf Datenschutz und Compliance bei dem Security-Anbieter an. Zertifizierungen spielen dagegen nur für jedes zehnte Unternehmen eine Rolle.

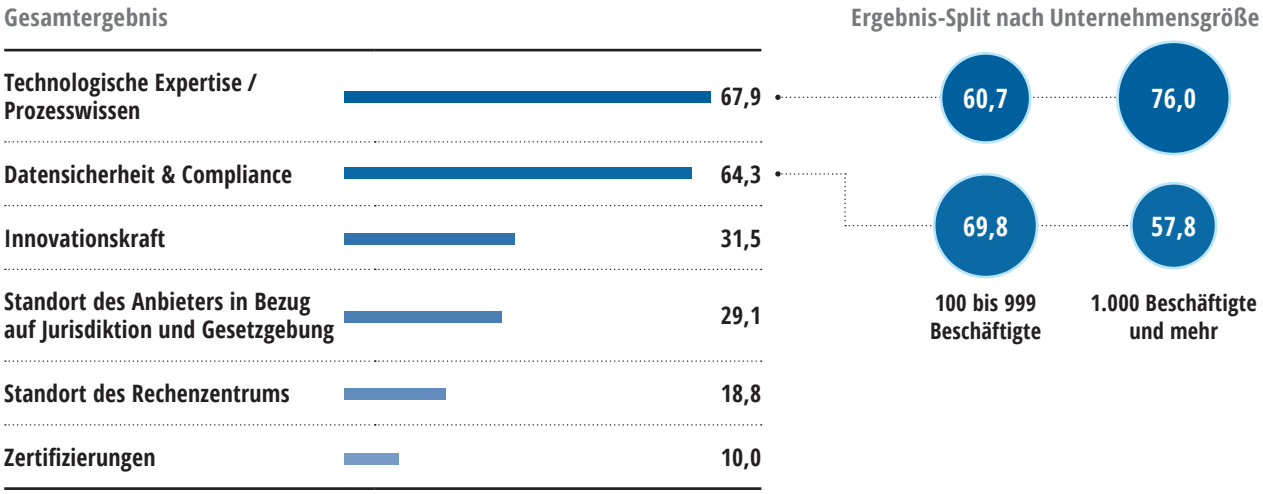
Es sind nicht nur die kleineren Unternehmen mit 100 bis 999 Beschäftigten, denen die Expertise in Technologie und Prozessen bei IT-Sicherheitsanbietern besonders wichtig ist, im Gegenteil. Während es 61 Prozent der kleineren Unternehmen sind, die dieses Kriterium nennen, steigt der Anteil der Antworten auf 76 Prozent bei den Unternehmen mit mindestens 1.000 Mitarbeitenden.

Obwohl Datenschutz und Compliance mit durchschnittlich 64 Prozent der Antworten auf Platz 2 der Auswahlkriterien für IT-Sicherheitsanbieter liegt, werden der Standort des Anbieters in Bezug auf Jurisdiktion und Gesetzgebung immerhin von annähernd einem Drittel der Unternehmen als wichtiges Kriterium genannt, der Standort des Rechenzentrums von knapp einem Fünftel der Befragten. Relativ geringe Bedeutung haben laut Umfrage Zertifizierungen, die nur von zehn Prozent der Unternehmen als Auswahlkriterium angeführt werden.

Dieses Ergebnis überrascht, da der Standort eines Anbieters oder Rechenzentrums Bedeutung haben kann für das gesetzlich zugesicherte Niveau im Datenschutz. Zudem ist es ohne Zertifizierungen nicht einfach, Datenschutz und Compliance bei einem IT-Sicherheitsanbieter nachprüfen zu können.

Welche der folgenden Kriterien sind Ihrem Unternehmen bei der Auswahl eines geeigneten IT-Sicherheitsdienstleisters am wichtigsten?

Angaben in Prozent. Basis je nach Antwortitem n = 80 - 106



Geopolitik und Datenhoheit beeinflussen Wahl des IT-Sicherheitsanbieters

87 Prozent der Befragten betonen, dass die aktuellen geopolitischen Entwicklungen sowie das Thema „Datenhoheit“ Einfluss auf die Auswahl eines IT-Sicherheitsanbieters durch ihr Unternehmen hätten. Und es sind nur 13 Prozent der befragten Unternehmen, die in diesem Kontext der Geopolitik und dem Thema der Datenhoheit keine (größere) Bedeutung beimessen.

Bei den größeren Unternehmen mit mindestens 1.000 Beschäftigten sind es sogar 93 Prozent, bei denen die Entscheidung für einen IT-Sicherheitsanbieter durch die aktuelle Diskussion zur geopolitischen Entwicklung und zur Datenhoheit beeinflusst wird. Bei den größeren Unternehmen ist mit über 57 Prozent auch der Anteil der „Ja, auf jeden Fall“-Nennungen auch besonders.

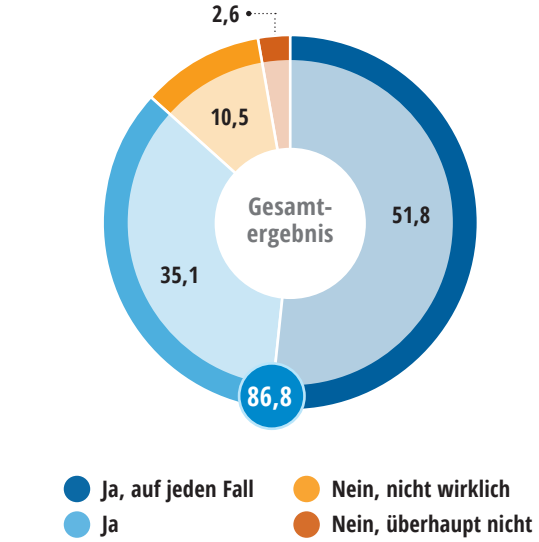
Bei den kleineren Unternehmen sind es immer noch 82 Prozent der Befragten, die eine Beeinflussung ihrer Entscheidung über IT-Sicherheitsanbieter durch Geopolitik und die Fragen zur Datenhoheit sehen oder ausdrücklich bestätigen.

Überhaupt keine Bedeutung von Geopolitik und Datenhoheit für die Entscheidung für einen IT-Sicherheitsanbieter sehen bei den kleineren Unternehmen in Deutschland nur fünf Prozent der Befragten, bei den größeren Unternehmen mit 1000 und mehr Mitarbeitenden sagt dies kein einziger der Befragten.

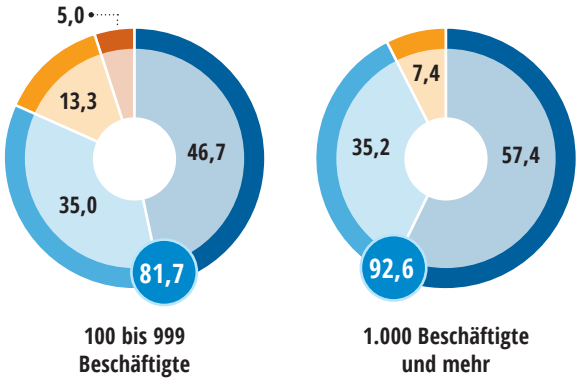
Dieses Ergebnis macht deutlich, wie stark geopolitische Entwicklungen und Fragen zur Datenhoheit die Auswahl von IT-Sicherheitsanbietern in Deutschland beeinflussen.

Haben die aktuellen geopolitischen Entwicklungen sowie das Thema „Datenhoheit“ einen Einfluss auf die Auswahl eines IT-Sicherheitsanbieters durch Ihr Unternehmen?

Angaben in Prozent. Basis: n = 114



Ergebnis-Split nach Unternehmensgröße



FAZIT

Datenschutz und Wunsch nach digitaler Souveränität prägen Suche nach IT-Sicherheitsanbietern

Auch wenn die Expertise eines IT-Sicherheitsanbieters besonders wichtig ist, achten die Unternehmen aus Deutschland stark auf Datenhoheit, Datenschutz und Compliance. Zertifizierungen dafür sind jedoch nicht besonders gefragt.

Von Oliver Schonschek

Während man von Wirtschaftsverbänden regelmäßig hört, der Datenschutz behindere die Wettbewerbsfähigkeit europäischer Unternehmen im Vergleich zu Unternehmen aus anderen Weltregionen, sehen dies die befragten Unternehmen aus Deutschland anders.

Geht es um IT-Sicherheit, achten mehr als 80 Prozent der Unternehmen auf die Entwicklungen in der Geopolitik und auf Fragen der Datenhoheit. Datenschutz und Compliance gehört zu den wichtigsten Auswahlkriterien bei der Suche nach einem IT-Sicherheitsanbieter. Innovationskraft für IT-Sicherheit suchen dagegen weniger als ein Drittel der befragten Unternehmen bei ihrem Anbieter der Wahl.

Immerhin fast ein Drittel der befragten Unternehmen aus Deutschland erachtet den Standort des Anbieters für wichtig, was angesichts des wichtigen Themas „Datenschutz und Compliance" sicher noch zu wenig ist. Zertifizierungen spielen dagegen eine untergeordnete Rolle. Hier sollten die Unternehmen noch für sich prüfen, wie sie sich von Datenschutz und Compliance überzeugen wollen, wenn nur jedes zehnte Unternehmen Zertifizierungen als wichtiges Kriterium bei der Anbietersuche in der IT-Sicherheit ansieht.

Auch die mögliche Bedeutung des Standortes von Anbieter oder Rechenzentrum für das gesetzlich garantierte Datenschutzniveau scheint nicht bewusst genug zu sein, denn auf dies achten nur 29 beziehungsweise 19 Prozent der befragten Unternehmen aus Deutschland.

44 Prozent der Unternehmen sind zudem der Meinung, Europa müsse stärker auf den Aufbau eigener, unabhängiger Cloud-Infrastrukturen setzen, um den eigenen Unternehmen Datensouveränität gewährleisten zu können, 25 Prozent der Befragten sehen dies nicht so.

Wer dies jedoch so sieht, sollte auch die Frage nach dem Standort genauer bewerten oder aber nach zusätzlichen Sicherheitsmaßnahmen fragen, die ein dem EU-Standard entsprechendes Datenschutzniveau gewährleisten sollen.

Es zeigt sich somit: Security-Anbieter mit Sitz in Europa, Datenschutz, Datenhoheit und Geopolitik spielen für die Unternehmen in Deutschland eine wichtige Rolle, auch und gerade in der IT-Sicherheit und im Cloud Computing. Dies dürfte sich auch in Zukunft nicht ändern, wenn es keine geopolitischen Veränderungen gibt, die laut der Umfrage zu den zentralen Faktoren gehören, die die Entscheidungen der Unternehmen in Sachen IT-Sicherheit prägen.

STUDIENSTECKBRIEF

Herausgeber ..... CIO, CSO und COMPUTERWOCHE

Exklusiver Studienpartner ..... Mimecast Germany GmbH

Grundgesamtheiten ..... Oberste (IT-)Verantwortliche in Unternehmen in Deutschland mit 100 und mehr Beschäftigten: Beteiligte an strategischen (IT-)Entscheidungsprozessen im C-Level-Bereich; Entscheidungsbefugte sowie Experten und Expertinnen aus dem IT-(Security-)Bereich Bereich, Risk-Management bzw. Finance Bereich

Teilnehmergenerierung ..... Persönliche E-Mail-Einladung über die exklusive Unternehmensdatenbank von CIO, CSO und COMPUTERWOCHE sowie – zur Erfüllung von Quotenvorgaben – über externe Online-Access-Panels

Untersuchungszeitraum ..... 30. Mai bis 06. Juni 2025

Methode ..... Online-Umfrage (CAWI), 114 abgeschlossene und qualifizierte Interviews

Durchführung ..... Custom Research Team von CSO, CIO und COMPUTERWOCHE

STICHPROBENSTATISTIK

Branchenverteilung **Mehrfachnennungen möglich**	Energie	7,0 %
	Wasserversorgung & Abwasserentsorgung	8,8 %
	Herstellung und Vertrieb von Chemikalien	6,1 %
	Herstellung von Maschinen, Fahrzeugen sowie elektrischen/elektronischen Geräten	14,9 %
	Informations- und Kommunikationstechnologie (IKT) - Dienstleistungsmanagement	64,0 %
	Digitale Infrastruktur	18,4 %
	Digitale Anbieter (z.B. Online-Marktplätze, Soziale Netzwerke)	16,7 %
	Lebensmittelproduktion, -verarbeitung und -vertrieb	2,6 %
	Sonstiger Groß- und Einzelhandel (außer Lebensmittel)	2,6 %
	Medien, Papier- und Druckgewerbe	3,5 %
	Baugewerbe, Handwerk	4,4 %
	Banken und Versicherungen & Finanzmarkt-Infrastruktur	7,0 %
	Transport, Logistik und Verkehr (inkl. Post- und Kurierdienste)	2,6 %
	Raumfahrt / Weltraum-Bodeninfrastruktur	1,8 %
	Dienstleistungen für Unternehmen	10,5 %
	Öffentliche Verwaltungen	4,4 %
	Forschungssektor, Forschungsinstitute	1,8 %
	Schule, Universität, Hochschule	1,8 %
	Herstellung von Medizinprodukten	1,8 %
	Gesundheit & Gesundheitswesen (z.B. Krankenhäuser, Gesundheitsdienstleister, Pharmazeutik, Medizinforschung)	10,5 %
	Andere Branchengruppe	5,3 %
Unternehmensgröße deutschlandweit	100 bis 249 Beschäftigte	11,4 %
	250 bis 499 Beschäftigte	18,4 %
	500 bis 999 Beschäftigte	22,8 %
	1.000 bis 4.999 Beschäftigte	27,2 %
	5.000 bis 9.999 Beschäftigte	12,3 %
	10.000 Beschäftigte und mehr	7,9 %
Jährliche Aufwendungen in IT-Systeme	Weniger als 1 Millionen Euro	11,4 %
	1 bis unter 10 Millionen Euro	28,1 %
	10 bis unter 100 Millionen Euro	43,0 %
	100 Millionen Euro und mehr	10,5 %
	Weiß ich nicht / keine Angabe	7,0 %
Softwarekäufe über AWS Marketplace	ja	57,0 %
	nein	34,2 %
	weiß nicht	8,8 %

ÜBER MIMECAST

Mimecast ist ein führendes Unternehmen im Bereich Cybersicherheit, das die Art und Weise, wie Unternehmen Human Risk verwalten, revolutioniert. Die KI-gesteuerte, API-fähige vernetzte Human-Risk-Management-Plattform ist speziell entwickelt worden, um Organisationen vor dem Spektrum von Cyberbedrohungen zu schützen. Durch die Integration modernster Technologie mit einem menschzentrierten Ansatz verbessert unsere Plattform die Sichtbarkeit und bietet strategische Einblicke.

Unsere Plattform ermöglicht entscheidungsrelevante Maßnahmen und stärkt Unternehmen dabei, ihre Kollaborationsumgebungen zu schützen. Sie sichert kritische Daten und bindet Mitarbeiter aktiv ein, um Risiken zu reduzieren und die Produktivität zu steigern. Über 42.000 Unternehmen weltweit vertrauen Mimecast, um der sich ständig weiterentwickelnden Bedrohungslandschaft einen Schritt voraus zu sein.

Von Insider-Risiken bis hin zu externen Bedrohungen erhalten Kunden mit Mimecast mehr. Mehr Sichtbarkeit. Mehr Agilität. Mehr Kontrolle. Mehr Sicherheit.

mimecast

Ansprechpartner:
Bernd Hohlweg – Director Marketing DACH
bhohlweg@mimecast.com

Mimecast Germany GmbH
Kistlerhofstraße 172
81379 München
Telefon: +49 89 904 200 800
Website: www.mimecast.com/de