IDG RESEARCH SERVICES

STUDIE CLOUD SECURITY 2019

DIE WICHTIGSTEN KEY FINDINGS

PRÄSENTIERT VON MICRO FOCUS

MICRO FOCUS®

Die DSGVO beeinflusst stark den Umgang mit den Daten in der Cloud

Für fast 60 Prozent der Unternehmen hat die Datenschutz-Grundverordnung (DSGVO) einen starken oder sehr starken Einfluss darauf, wie sie mit Daten umgehen, die in einer Cloud verarbeitet werden. Keine Auswirkung der DSGVO sehen gerade einmal zwei Prozent der befragten Unternehmen.

Während 16 Prozent der befragten Unternehmen meinen, die DSGVO hat nur einen sehr schwachen bis eher schwachen Einfluss auf ihren Umgang mit Daten in der Cloud, berichten 82 Prozent von einer eher starken bis sehr starken Wirkung des neuen EU-Datenschutzrechts.

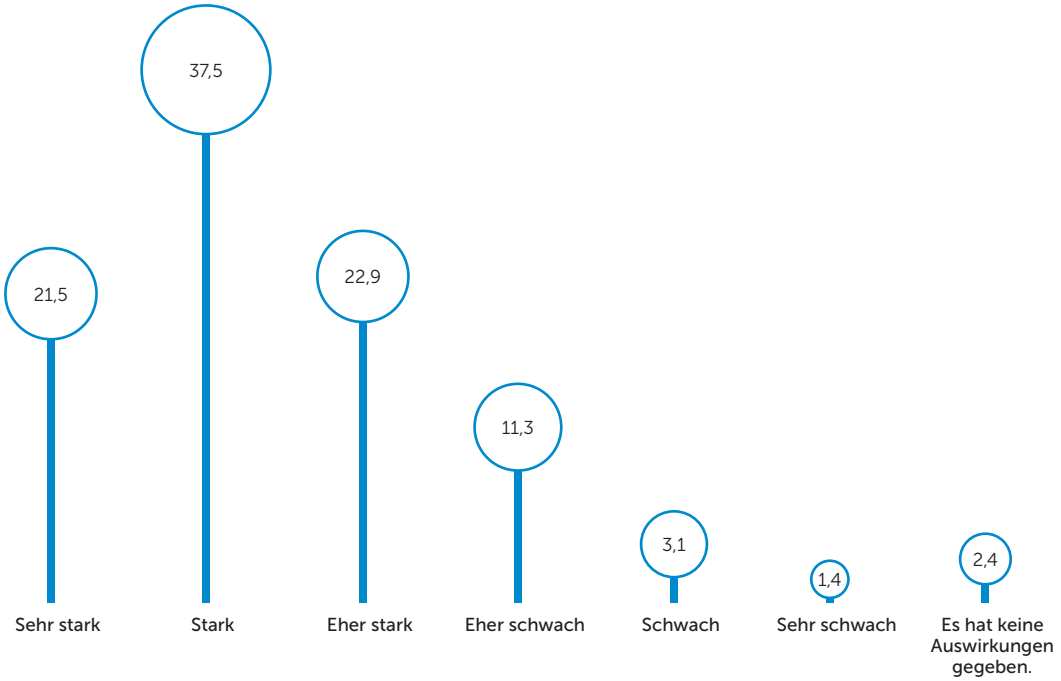
Ob der Einfluss der DSGVO als sehr stark angesehen wird, hängt weniger von der Mitarbeiterzahl der Unternehmen in Deutschland ab als vielmehr von der Höhe der jährlichen Investitionen in Cloud-Services.

Betragen die Aufwendungen für Cloud-Dienste weniger als eine Million Euro pro Jahr, sind es nur 15 Prozent der Unternehmen, die einen sehr starken Einfluss der DSGVO sehen, bei einer bis 100 Millionen Euro pro Jahr 21 Prozent, bei mehr als 100 Millionen Euro jährlicher Aufwendungen für Cloud-Services sogar 36 Prozent.

Den sehr starken Einfluss der DSGVO sehen dabei insbesondere die Geschäftsführer mit 34 Prozent Zustimmung; bei der IT-Leitung sind es noch 22 Prozent, in den Fachbereichen 19 Prozent und beim CIO sogar nur 13 Prozent.

Wie stark sind die Auswirkungen der EU-DSGVO (EU-Datenschutz-Grundverordnung) bezogen auf den Umgang Ihres Unternehmens mit Daten in der Cloud?

Angaben in Prozent. Filter: Nur Unternehmen, die Cloud-Services bereits eingeführt haben oder es konkret planen. Basis: n = 300



Neue Security-Ansätze kommen eher bei hohen Cloud-Investitionen zum Einsatz

Wenn es um die technische Cloud-Sicherheit geht, setzen viele Unternehmen auf vertraute Security-Konzepte wie Verschlüsselung, Firewall und lokale Backups. Trotz der zahlreichen DDoS-Attacken landet der DDoS-Schutz nur auf Platz vier der Security-Maßnahmen.

Gute Endpoint-Kontrolle, verbesserte Zugangs- und Rechtekontrolle (IAM) und ein verbessertes Passwortmanagement gehören bei 31 Prozent der Unternehmen zum technischen Schutz ihrer Cloud-Nutzung. Für 29 Prozent gehört auch die Integritätskontrolle bei Cloud-Daten dazu.

Bei 35 bis 37 Prozent der Unternehmen geht es in der Cloud-Sicherheit klassisch zu, sie vertrauen auf Maßnahmen wie Verschlüsselung, Firewall und Backups.

Eine starke Kontrolle über System-Level-Ressourcen und Virtual Machines, Cloud IDS / IPS und CASB (Cloud Access Security Broker) nutzt maximal ein Viertel der Unternehmen. Dabei ist die Umsetzung dieser neueren Ansätze für Cloud-Sicherheit abhängig davon, wie hoch die jährlichen Aufwendungen für Cloud-Services sind. Bei bis zu einer Million pro Jahr sind es bis zu 16 Prozent der Unternehmen, bei mehr als 100 Millionen Aufwendungen pro Jahr aber schon bis zu 34 Prozent.

Offensichtlich steigt das Interesse an neuen Security-Verfahren bei höheren Investitionen in die Cloud.

Welche technischen Vorkehrungen sind in Ihrem Unternehmen in Bezug auf Cloud Security getroffen worden?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 351

	Gesamt	Jährliche Aufwendungen in Cloud Services		
		< 1 Mio.	1-100 Mio	100 Mio. +
Verschlüsselte Datenübertragung vom und zum Cloud-Provider (z.B. VPN)	36,8	42,4	34,6	40,0
Cloud-Firewall	36,5	32,3	39,7	28,0
Lokale Daten-Backups möglich	35,0	33,3	35,3	38,0
Schutz vor DDoS-Attacken	32,5	22,2	33,1	40,0
Gute Endpoint-Kontrolle (sichere Clients)	30,8	35,4	33,1	18,0
Verbesserte Zugangs- und Rechtekontrolle (IAM)	31,1	33,3	29,4	28,0
Verbessertes Passwortmanagement (starke Passwörter, kurze Wechselzyklen, Passwort-Tools ...)	31,1	32,3	30,9	20,0
Integritätskontrolle bei Cloud-Daten	28,2	24,2	33,1	30,0
Starke Kontrolle über System-Level-Ressourcen und Virtual Machines	25,1	16,2	26,5	34,0
Cloud IDS / IPS	24,2	14,1	33,8	30,0
CASB (Cloud Access Security Broker)	17,9	12,1	19,9	34,0

Sicherheitsrisiken der Cloud-Dienste werden zu einseitig gesehen

Obwohl von DDoS-Attacken berichtet wird und die Forderung nach einer Datensicherung durch den Cloud-Anbieter vorherrscht, stehen bei den Unternehmen andere Risiken im Fokus als DDoS-Angriffe und Datenverlust. Insbesondere Hacker-Angriffe und der Diebstahl von Daten werden gefürchtet, weniger Gefahren durch Innentäter.

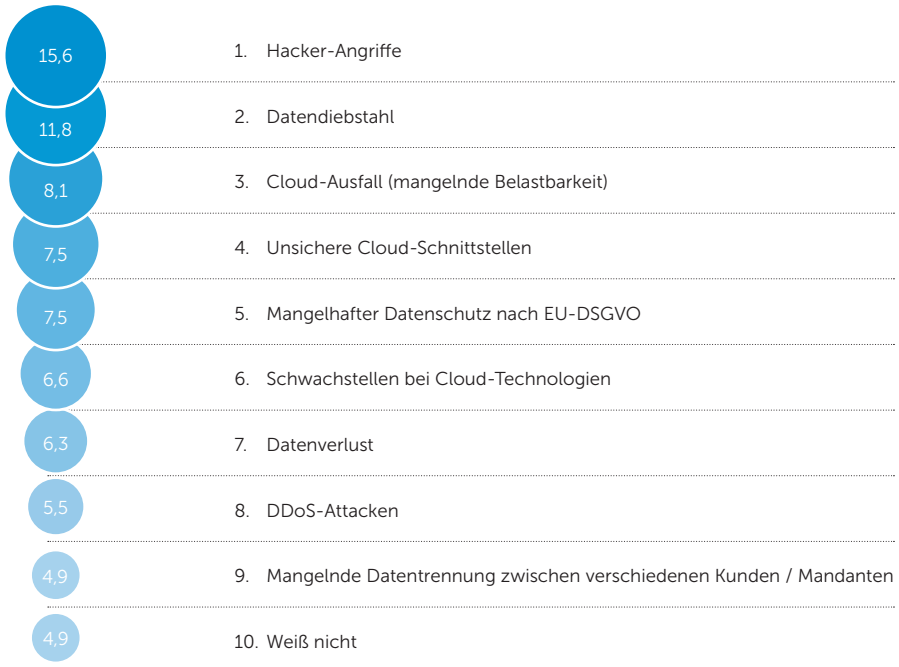
Nur drei bis fünf Prozent der Unternehmen sehen große Risiken für Cloud-Dienste, wenn die Datenintegrität fehlt, der virtuelle Zugriffsschutz mangelhaft ist oder Daten aus der Cloud durch Insider-Attacken abfließen. Auch APTs (Advanced Persistent Threats) und mangelhafter physischer Zugriffsschutz gehören nicht zu den Top-Risiken in den Augen der Cloud-Nutzer.

Als besonders riskant dagegen bezeichnen 16 Prozent der Unternehmen Angriffe von Hackern, zwölf Prozent fürchten Datendiebstahl. DDoS-Attacken und Datenverlust nennen nur sechs Prozent der Unternehmen als große Bedrohung.

Interessant ist auch, dass der Datenschutz grundsätzlich als sehr wichtig erachtet wird, ein Mangel an Datenschutz jedoch nur für acht Prozent ein großes Risiko darstellt. Offensichtlich wird nicht der Zusammenhang gesehen zwischen Sicherheitsrisiken und Datenschutzmängeln. Das zeigt sich auch daran, dass mangelnde Belastbarkeit und fehlende Datentrennung nach Mandanten in der Rangfolge der Sicherheitsrisiken weiter unten stehen. Beide Risiken führen zu Problemen bei der Einhaltung der Datenschutz-Grundverordnung, die eigentlich einen hohen Stellenwert bei den Cloud-Nutzern hat.

Was schätzen Sie ganz allgemein als größtes Security-Risiko bei Cloud-Services ein?

Angaben in Prozent. Auflistung der Top 10. Basis: n = 347



Der Cloud-Datenschutz wird teils besser bewertet als der interne Datenschutz

Die Forderungen an den Datenschutz des Cloud-Anbieters sind hoch. 13 Prozent der Unternehmen denken trotzdem, dass der Cloud-Datenschutz besser ist als der Datenschutz bei intern betriebenen IT-Diensten. Die Datenverfügbarkeit in der Cloud sehen sogar 18 Prozent als besser an, wenn sie sie mit der Verfügbarkeit bei On-Premise-Lösungen vergleichen.

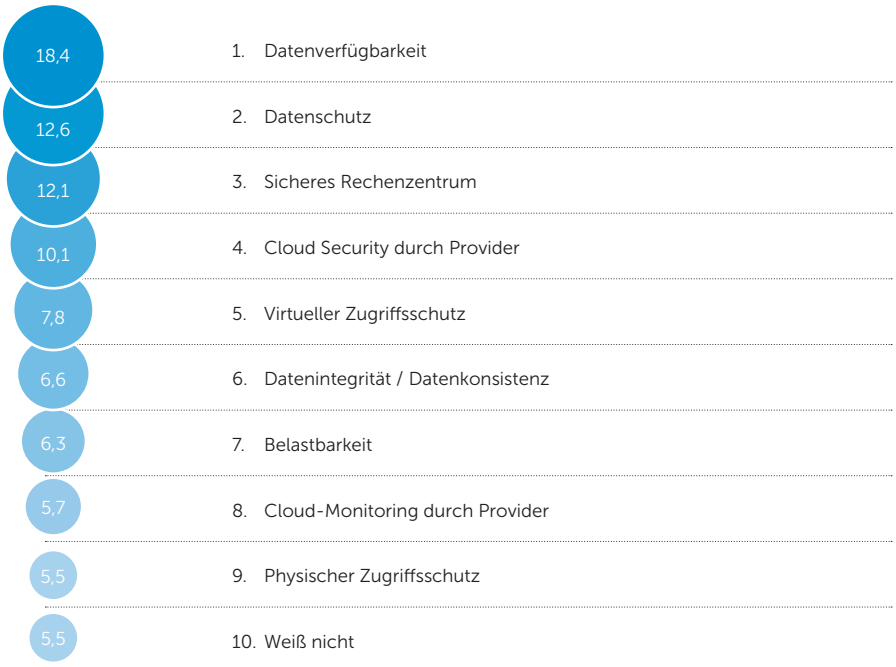
Cloud-Anbieter sind erfolgreicher als die Unternehmen selbst, wenn es um Datenschutz und Sicherheit geht; das denken immerhin zwischen zehn und 18 Prozent der Unternehmen. Eine höhere Verfügbarkeit der Daten, ein besserer Datenschutz, ein sicheres Rechenzentrum und die Maßnahmen für die Cloud-Sicherheit, das sind die wesentlichen Vorzüge für die Sicherheit, wenn man Cloud-Dienste und On-Premise-Services vergleicht.

Selbst das Cloud-Monitoring durch den Provider wird von sechs Prozent der Unternehmen als Vorteil gesehen. Dabei wird jedoch vergessen, dass ein Monitoring der Cloud-Dienste auch der Kontrolle des Providers dienen soll. Macht er dieses Monitoring selbst, kann die Aufgabe der Kontrolle, die auch aus der Datenschutz-Grundverordnung (DSGVO) erwächst, gar nicht erfüllt werden.

Die Unternehmen schätzen offensichtlich ihre bestehenden Security-Probleme im eigenen Unternehmen als höher ein als die des Cloud-Anbieters. Automatisch kann man jedoch nicht von diesen Vorteilen des Cloud-Anbieters ausgehen, wie zahlreiche Vorfälle bei Providern zeigen, etwa Cloud-Ausfälle, die die Datenverfügbarkeit bedrohen.

Was schätzen Sie als größten Security-Vorteil von Cloud-Services im Vergleich zu On-Premise-Lösungen ein?

Angaben in Prozent. Auflistung der TOP 10. Basis: n = 348



Backup der Cloud-Daten sehen viele Nutzer als Aufgabe des Providers

Die Unternehmen erwarten vom Cloud-Anbieter ähnliche Schutzmaßnahmen, wie sie auf ihrer Seite selbst durchführen. Neben der Datensicherung wünschen sich die Nutzer insbesondere die Authentifizierung und Verschlüsselung bei Übertragung und Speicherung vom Anbieter der Wahl.

Anforderungen wie eine provider-unabhängige Verschlüsselung (25 Prozent) und die Zugangskontrolle über SSO (Single-Sign-On, 19 Prozent) gehören ebenso wenig zu den Top 10 der gewünschten Sicherheitsmaßnahmen wie der Ausschluss von Servertechnik aus den USA (21 Prozent) oder China (19 Prozent).

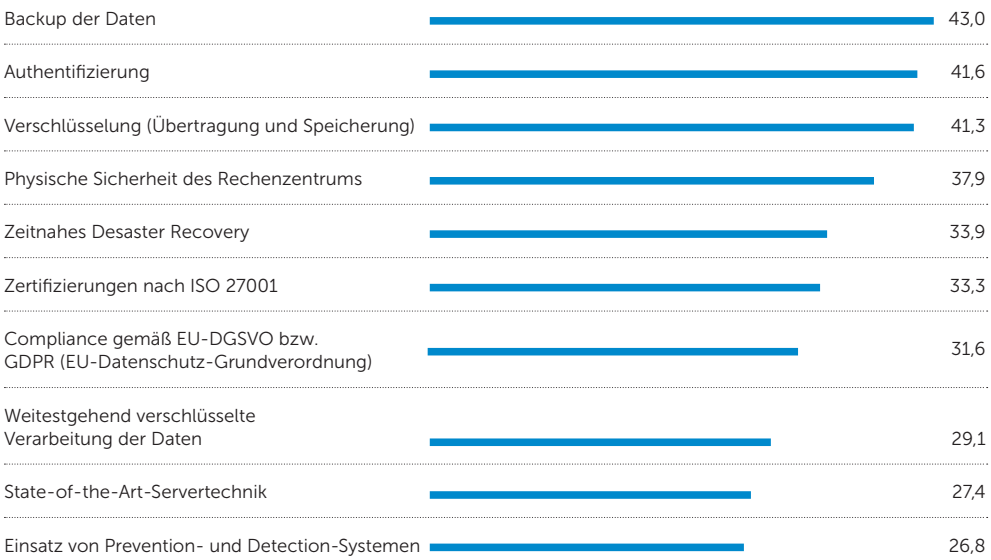
Forderungen an technische Maßnahmen des Cloud-Providers wie Backup der Daten werden von 43 Prozent der Unternehmen genannt, das Schlusslicht der Top-10-Forderungen ist der Einsatz von Prevention- und Detection-Systemen mit 27 Prozent.

Die Zertifizierung nach ISO 27001 liegt mit 33 Prozent knapp vor der Compliance mit der Datenschutz-Grundverordnung (32 Prozent). Dabei sollte aber nicht vergessen werden, dass viele der technischen Maßnahmen, die als wichtiger eingestuft werden als die DSGVO-Compliance, grundsätzlich notwendig sind, um die DSGVO einzuhalten. Nur dann kann der Provider auch die Vorgaben an eine Auftragsverarbeitung (Artikel 28 DSGVO) nach EU-Datenschutz erfüllen.

Welche technischen Maßnahmen erwarten Sie von einem Cloud-Provider zum Schutz der Daten?

Angaben in Prozent. Mehrfachnennungen möglich. Auflistung der Top 10. Basis: n = 351

Gesamt



Die zehn technischen Maßnahmen der Cloud-Provider, die insgesamt als besonders wichtig angesehen werden, betrachten die verschiedenen Funktionen im Unternehmen aber durchaus unterschiedlich.

Geschäftsführer stufen die Authentifizierung (42 Prozent) als wichtiger ein als die Backups (38 Prozent). Backups landen bei den Geschäftsführern auf Platz zwei unter den Top-10-Maßnahmen der Cloud-Provider für den technischen Schutz der Daten.

Die CIOs sehen ebenfalls die Authentifizierung (41 Prozent) als besonders wichtig an, gleichzeitig aber auch die physische Sicherheit im Rechenzentrum des Cloud-Anbieters (ebenfalls 41 Prozent). Das Backup der Daten nennen unter den CIOs nur 28 Prozent.

Ganz anders sehen dies die Fachbereiche: 53 Prozent halten die Backups für die zentrale technische Maßnahme des Cloud-Anbieters, 45 Prozent nennen die Verschlüsselung der Daten bei Übertragung und Speicherung, die Authentifizierung kommt bei den Fachbereichen auf 40 Prozent.

Ergebnis-Split nach Funktion im Unternehmen

	Geschäftsführung/ COO/CFO/ sonst. Vorstand	CIO/IT-Vorstand/ CDO/CTO/ Technikvorstand	Fachbereiche (Vertrieb, Marketing, Produktion, Einkauf, anderer FB)
Backup der Daten	37,8	28,4	52,8
Authentifizierung	41,9	40,9	39,8
Verschlüsselung (Übertragung und Speicherung)	31,1	39,8	45,4
Physische Sicherheit des Rechenzentrums	28,4	40,9	36,1
Zeitnahes Desaster Recovery	23,0	37,5	31,5
Zertifizierungen nach ISO 27001	32,4	34,1	28,7
Compliance gemäß EU-DGSVO bzw. GDPR (EU-Datenschutz-Grundverordnung)	25,7	29,5	29,6
Weitestgehend verschlüsselte Verarbeitung der Daten	28,4	26,1	30,6
State-of-the-Art-Servertechnik	21,6	29,5	17,6
Einsatz von Prevention- und Detection-Systemen	21,6	23,9	31,5

Cloud – mit Sicherheit!

Die IDG Cloud Security 2019 Studie hat es wieder gezeigt: An der Cloud kommt kommt eigentlich kein Unternehmen vorbei: Schnelle und flexible Bereitstellung von IT Services, Kosteneinsparungen und Qualitätssteigerungen werden häufig als Gründe für den Einsatz „der Cloud" genannt. Allerdings kommt nach den ersten eher pragmatischen Jahren immer mehr die Erkenntnis, dass Sicherheit nicht einfach vom Cloudanbieter eingekauft werden kann: Unternehmen müssen ihre Sicherheitskonzepte kontinuierlich für die hybriden IT-Liefermodelle ertüchtigen – ihre Mitarbeiter, Prozesse und Werkzeuge entsprechend weiterentwickeln.

Automatisierung, Transparenz darüber, was am wichtigsten ist, sowie Änderungen, Erweiterungen und Veränderungen der Art und Weise, wie wir Daten nutzen und verteilen, werden durch neue Technologien ständig verändert. So wichtig es ist, Spitzentechnologien zu liefern die das Wachstum vorantreiben, so wichtig ist es auch, neben diesen Innovationen Sicherheit zu bieten. Der Einsatz neuer Technologien sollte daher immer kombiniert werden mit einer starken Sicherheitsinfrastruktur zum Schutz der Daten, Kunden und Marken.

Unternehmen optimieren Anwendungen mit Cloud-Technologie und nutzen die Cloud für traditionelle Anwendungen, um eine höhere Leistung, eine bessere Benutzerfreundlichkeit und niedrigere Kosten zu erzielen. Wie bei jeder Innovation müssen Unternehmen jedoch ihre bestehende Architektur an neue Anforderungen anpassen wie auch die traditionellen Methoden zur Datensicherung in einer Cloud-Umgebung überdenken. Während die Cloud-Infrastruktur Ihr Unternehmen verändern kann, ist die Hauptsorge beim Wechsel in die Cloud die Sicherheit.

Public Cloud kann sogar sicherer sein als eine eigene Umgebung. Doch auch in einer hybriden Welt müssen Unternehmen Maßnahmen ergreifen, um sicherzustellen, dass Identitätsmanagement, Datenschutzkontrollen und Datensicherheit sowie die Einhaltung der gesetzlichen Bestimmungen umgesetzt und berücksichtigt werden.

Das Micro Focus Security Lösungsportfolio ist einzigartig positioniert, um Sicherheitsprobleme im gesamten modernen IT-Hybrid-Ökosystem zu lösen – vom Mainframe über die traditionelle IT bis hin zur Public Cloud. Es trägt dazu bei Ihr Unternehmen zu schützen, während Sie alte und neue IT-Welt verbinden. Unser ganzheitlicher Sicherheitsansatz geht über die bloße Erkennung von Ereignissen hinaus. Wir bieten Unternehmen die Möglichkeit, Vorfälle zu identifizieren, zu schützen, zu erkennen, zu reagieren und wiederherzustellen, um das Gesamtrisikoprofil zu reduzieren und ein modernes und sicheres IT-Ökosystem zu schaffen.

„Die Flexibilität und Agilität, die Cloud Lösungen mit sich bringen, sind für Business Entscheider wichtige Argumente. Dieser Schritt in Richtung Digitalisierung zieht eine generelle und kulturelle Veränderung im Umgang mit der IT Infrastruktur nach sich. Wir helfen Unternehmen auf dieser Reise in Bezug auf Datenschutz und Datensicherheit."

Alexander Neff
Vice President DACH
Micro Focus GmbH

Herausgeber:

IDG Business Media GmbH

Anschrift
Lyonel-Feininger-Str. 26
80807 München
Telefon: 089 36086 – 0
Fax: 089 36086 – 118
E-Mail: info@idg.de

Vertretungsberechtigter
York von Heimburg
Geschäftsführer

Registergericht
Amtsgericht München
HRB 99187

Umsatzsteueridentifikations-
nummer: DE 811 257 800

Weitere Informationen unter:
www.idg.de

Gold-Partner:

Micro Focus GmbH

Herrenberger Str. 140
71034 Böblingen

Tel.: +49 69 66308025
Web: www.microfocus.com/de

Studienkonzept / Fragebogenentwicklung
Simon Hülsbömer,
IDG Research Services

Endredaktion / CvD Studienberichtsband:
Simon Hülsbömer,
IDG Research Services

Analysen / Kommentierungen:
Oliver Schonschek,
Bad Ems

Umfrageprogrammierung und Ergebnisauswertungen:
Thamar Thomas-Ißbrücker,
IDG Research Services

Hosting / Koordination Feldarbeit:
Armin Rozsa,
IDG Research Services

Artdirector:
Daniela Petrini, Reutte

Umschlagkonzept:
Simon Hülsbömer,
IDG Research Services
(unter Verwendung eines Farbfotos für Vorder- und Rückseite von © Blackboard - shutterstock.com)

Grafik:
Jutta Weber-Vidal, Würzburg
www.erdenbuerger.de

Lektorat:
Dr. Renate Oettinger,
München

Druck:
Peradruck GmbH
Hofmannstr. 7b
81379 München

Ansprechpartner:
Matthias Teichmann
Director Research
IDG Research Services
Telefon: 089 36086 – 131
mteichmann@idgbusiness.de