Die Bedeutung von Unternehmenssicherheit im Zeitalter der Arbeitsflexibilität.

LONDON RESEARCH
Research Powered Content

In Zusammenarbeit mit

Adobe

Inhalt.

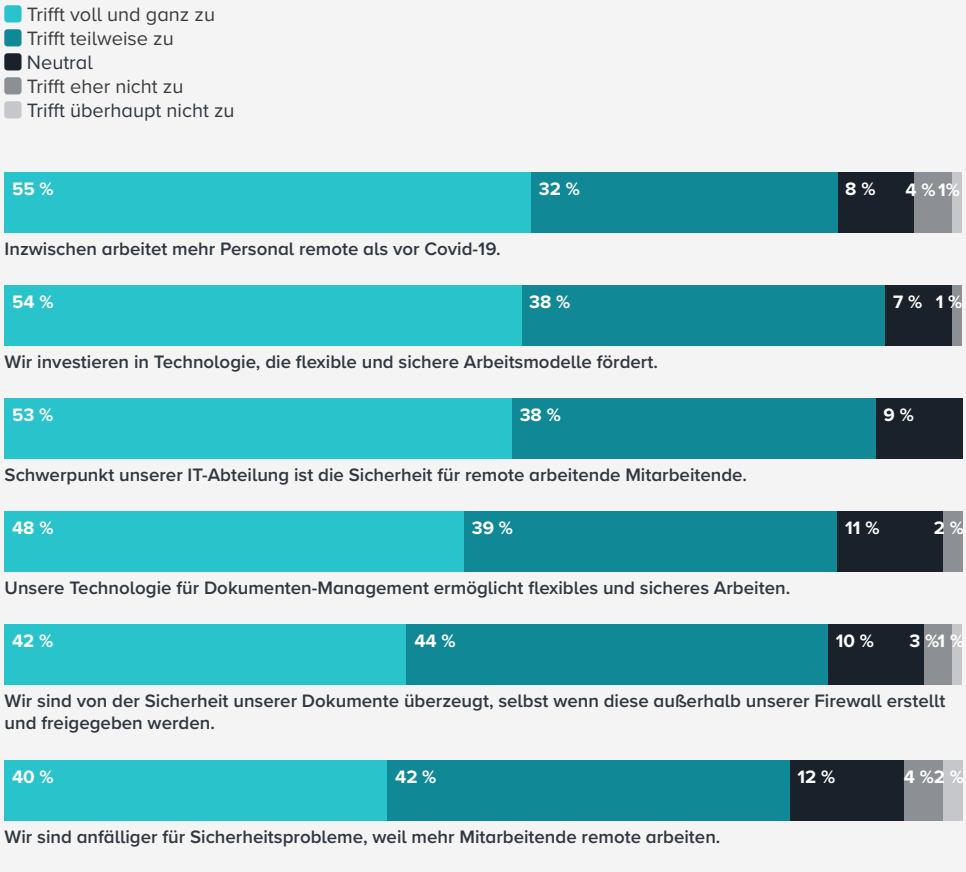
Einführung.

Datensicherheit war für Unternehmen schon immer ein wichtiges Thema. Der Unterschied im Vergleich zu früher ist, dass die damit verbundenen Herausforderungen heute ein ganz neues Ausmaß angenommen haben. Das liegt unter anderem daran, dass die Durchschnittskosten infolge von Datenlecks im Jahr 2022 weltweit auf $ 4,35 Mio. gestiegen sind, in Großbritannien auf $ 5,05 Mio., in Deutschland auf $ 4,85 Mio. und in Frankreich auf $ 4,34 Mio. Das eigentliche Problem ist aber, dass Unternehmen inzwischen viel anfälliger für Sicherheitsrisiken sind. Zurückzuführen ist diese Entwicklung auf flexible Arbeitsmodelle.

In einer Umfrage von London Research im Auftrag von Adobe gaben fast neun von zehn IT-Führungskräften in Unternehmen (87 %) an, dass mehr Personal als je zuvor remote arbeitet. Vier von fünf Befragten sagten, dass ihr Unternehmen dadurch anfälliger für Sicherheitsprobleme ist (*Abbildung 1*).

ABBILDUNG 1

Zustimmung von IT-Führungskräften zu Aussagen über sichere Arbeitspraktiken innerhalb der Organisation.



Der Grund dafür liegt auf der Hand. Die Lösung allerdings nicht. Solange alle Mitarbeitenden eines Unternehmens innerhalb der Firewall arbeiten, ist es in der Regel kein Problem, die Sicherheit und Integrität der technologischen Infrastruktur zu gewährleisten. Deutlich schwieriger wird es, wenn über ungesicherte Netzwerke oder private Laptops, Tablets und Smartphones auf Unternehmensressourcen zugegriffen wird.

Die Konsequenzen von Sicherheitsmängeln.
Die direkten Folgen von Sicherheitsmängeln sind naheliegend:

- **Lösegeldzahlungen**
- **Sinkender Aktienkurs**
- **Umsatzeinbußen durch Systemausfälle**
- **Image-Verlust.** (Potenzielle) Kundinnen und Kunden betrachten die Marke nach einem Datenleck als weniger vertrauenswürdig. Laut einem Bericht von PwC[1] aus dem Jahr 2022 haben Cyber-Attacken oder Datenschutzverletzungen in den drei Vorjahren dazu geführt, dass 27 % der Unternehmen weltweit einen Teil ihrer Kundschaft verloren, und 23 % mussten eine Schädigung ihres Rufs oder ihrer Marke in Kauf nehmen. Ein Image-Verlust bedeutet auch höhere PR-Kosten für die Wiederherstellung eines guten Rufs.
- **Bußgelder.** Wenn ein Datenleck dazu führt, dass persönliche Daten von Kundinnen und Kunden offen gelegt werden, kann dies als Rechtsverstoß bewertet werden. Gemäß Datenschutzgrundverordnung[2] können nationale Datenschutzbehörden in Europa bei Verstößen gegen den Datenschutz Bußgelder von bis zu 20 Millionen Euro bzw. 4 % des weltweiten Jahresumsatzes des Unternehmens erheben, je nachdem, welcher Betrag höher ist. Verhältnismäßig mildere Sanktionen sind Verwarnungen, ein vorübergehendes oder dauerhaftes Verbot der Datenverarbeitung, die Verpflichtung zur Berichtigung, Löschung oder Einschränkung der Bearbeitung von Daten sowie das Verbot der Datenübermittlung an Drittländer.

Die Auswirkungen können sich aber auch noch auf weitere Bereiche erstrecken, wie zum Beispiel:

- **Verlust von geistigem Eigentum**
- **Preiserhöhungen.** Laut Ponemon Institute müssen 60 % der Unternehmen, die mit einem Datenleck konfrontiert waren, die Kosten durch Preiserhöhungen auf ihre Kundschaft umlegen[3].
- **Erschwerte und kostspieligere Finanzierungen.** HBR hebt zudem hervor, dass Cyber-Risiken zu einer Herabstufung der Bonität führen können.
- **Behebung/Wiederherstellung**
- **Rechts- und Audit-Kosten.** Harvard Business Review[4] berichtet: „Die Audit-Kosten für Unternehmen, die mit Datenlecks zu kämpfen hatten, können rund 13,5 % höher sein als für Unternehmen ohne diese Art von Sicherheitsproblem.“
- **Höhere Versicherungsprämien**

1 https://www.pwc.com/gx/en/news-room/press-releases/2022/global-digital-trust-insights-survey.html
2 https://www.taylorwessing.com/-/media/taylor-wessing/files/germany/2019/10/german-data-protection-supervisory-authorities-model.pdf
3 https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/
4 https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Datensicherheit ist 2023 somit das größte Anliegen für CTOs und CIOs (*Abbildung 2*): 86 % räumen dem Thema eine hohe Priorität ein. Datensicherheit hat sogar mehr Priorität als andere wichtige Bereiche wie digitale Transformation (77 %), Customer Engagement und Kundenzufriedenheit (73 %) sowie Nachhaltigkeit (56 %). Drei Viertel (75 %) halten Datensicherheit für wichtiger als vor einem Jahr (*Abbildung 3*).

ABBILDUNG 2

Prioritäten verschiedener Bereiche für CTOs/CIOs im Jahr 2023.

ABBILDUNG 3

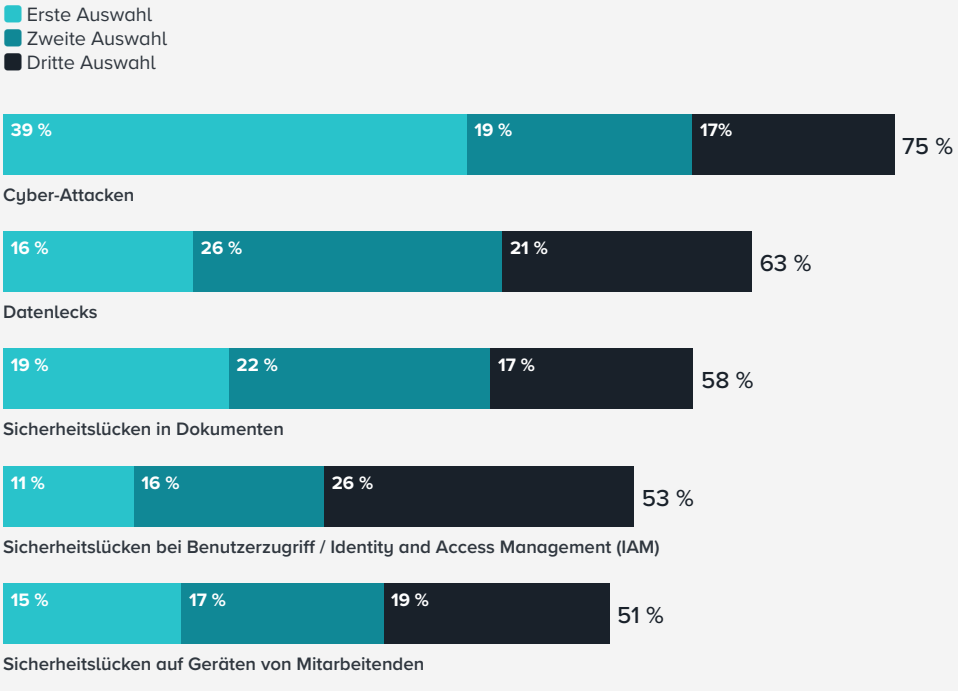
Wichtigkeit dieser Themen für CTOs/CIOs im Vergleich zum Vorjahr.

Gleichzeitig wollen Unternehmen von den Vorteilen flexibler Arbeitsmodelle profitieren. Diese Vorteile umfassen laut CIPD die „Reduzierung der Büroflächen“ und eine „bessere Abstimmung von Ressourcen und Nachfrage, z. B. um die Kundschaft rund um die Uhr zu betreuen“. Eine Studie der Cranfield University zeigt zudem, dass „flexible Arbeitskräfte im Vergleich zu ihren nicht flexiblen Kolleginnen und Kollegen zufriedener mit ihrem Job sind und ihrem Unternehmen gegenüber loyaler sind“.

Dokumenten-Management im Zeitalter der Arbeitsflexibilität.
Wenn immer mehr Mitarbeitende außerhalb der Unternehmens-Firewall arbeiten, muss also ein Schwerpunkt von Sicherheitsinitiativen das Dokumenten-Management sein. Als wir IT-Führungskräfte nach ihren derzeit größten Herausforderungen und Bedenken hinsichtlich Sicherheit fragten, gaben sie an, dass Cyber-Attacken ihnen am meisten Kopfzerbrechen bereiten. An zweiter Stelle kamen Datenlecks, gefolgt von Sicherheitslücken in Dokumenten, Sicherheitslücken bei Benutzerzugriff / Identity and Access Management und Sicherheitslücken auf Geräten von Mitarbeitenden (*Abbildung 4*).

ABBILDUNG 4

Die drei größten Herausforderungen und Bedenken im Zusammenhang mit Sicherheit.



Gleichzeitig sind viele Unternehmen davon überzeugt, dass sie den richtigen Weg eingeschlagen haben. 87 % der IT-Führungskräfte gaben an, dass ihre eingesetzte Technologie für Dokumenten-Management flexibles und sicheres Arbeiten ermöglicht. Nichtsdestotrotz bestehen immer noch Zweifel. Weniger als die Hälfte ist „voll und ganz“ von der Sicherheit ihrer Dokumente überzeugt, selbst wenn diese außerhalb der Firewall erstellt und freigegeben werden (*Abbildung 1*).

Um diese Bedenken aus dem Weg zu räumen, sind weitere Investitionen in sicherere Technologie erforderlich. Mehr als neun von zehn befragten IT-Führungskräften (92 %) gaben an, dass sie in Technologie für flexible und sichere Arbeitsabläufe investieren (Abbildung 1). Aus Sicht der IT profitieren Unternehmen doppelt durch diese Investitionen: einerseits durch eine Senkung der Sicherheitsrisiken, andererseits durch eine höhere Produktivität und Zufriedenheit von Mitarbeitenden (*Abbildung 5*).

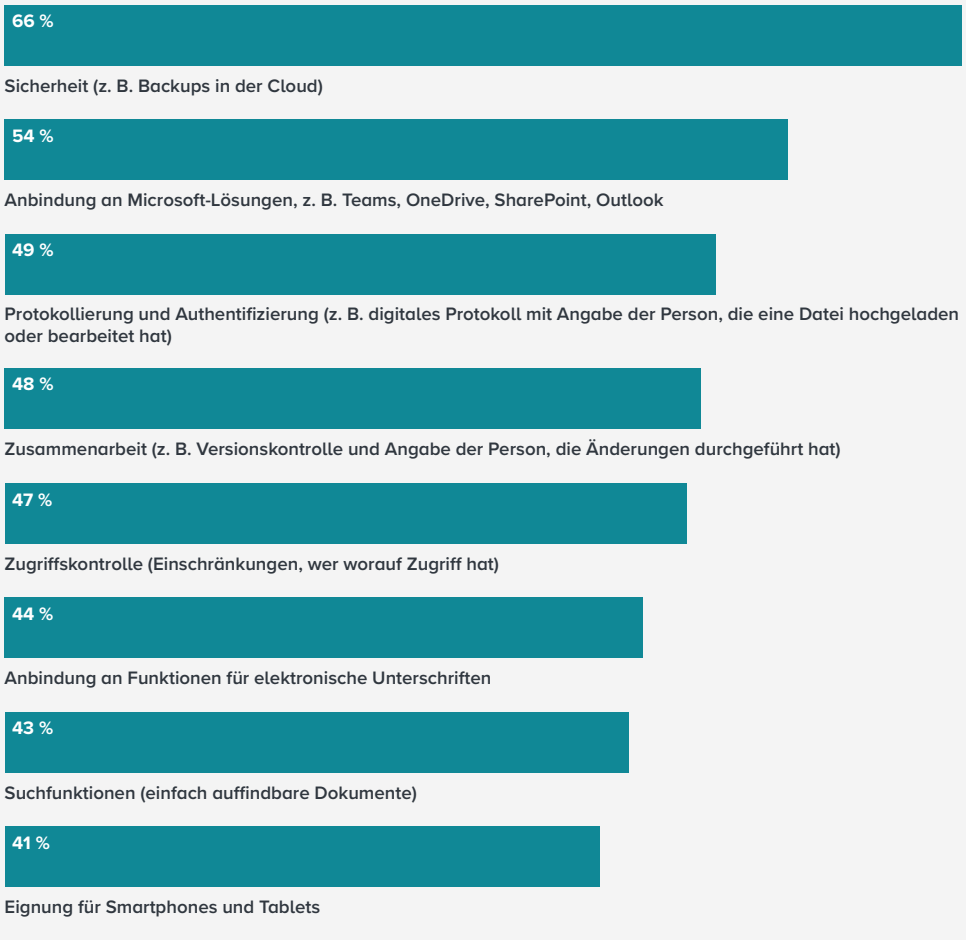
ABBILDUNG 5

Woran werden die Auswirkungen von Investitionen in Software für Dokumenten-Management gemessen?

Die Erwartungen von Userinnen und Usern.
Die Endanwenderinnen und -anwender der neuen Systeme für Dokumentensicherheit haben andere Erwartungen an die Programme als die IT (*Abbildung 6*). Sie legen großen Wert auf Sicherheit und Protokollierung/Authentifizierung, wünschen sich aber auch Anbindungen an andere Lösungen (z. B. Microsoft) und effiziente Zusammenarbeit (z. B. Versionskontrolle und Angaben zu Personen, die Änderungen durchgeführt haben). Dies zeigt, wie wichtig es für IT-Abteilungen ist, Sicherheit mit Bedienfreundlichkeit in Einklang zu bringen.

ABBILDUNG 6

Anteil der Organisationen, die die folgenden Funktionen für Dokumenten-Management als „sehr wichtig“ bei der täglichen Arbeit erachten.



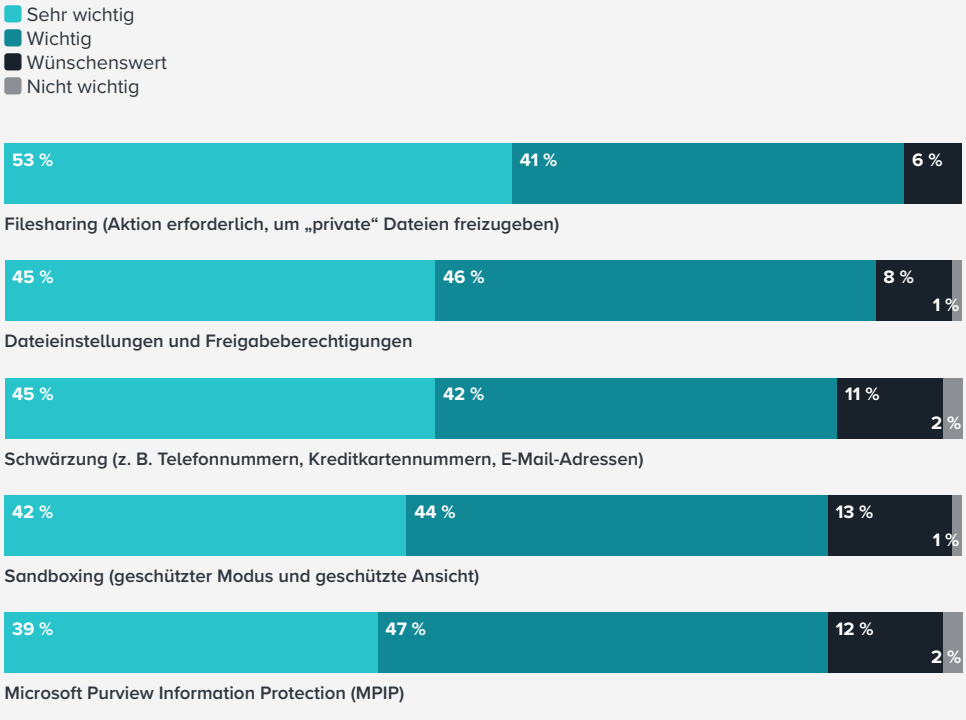
Diese Zahlen weisen auch darauf hin, dass „Sicherheit“ für Mitarbeitende eine andere Bedeutung hat als für IT-Führungskräfte. Gleichzeitig wird ein weiteres Problem ersichtlich, das der steigende Anteil an Remote-Arbeit mit sich bringt.

Mitarbeitenden ist zwar durchaus bewusst, wie wichtig Sicherheit ist. Bei engen Terminvorgaben besteht jedoch durchaus eine Tendenz zur Nachlässigkeit. Schulungen spielen hier eine wichtige Rolle. Noch besser aber sind Systeme mit „eingebauter“ Sicherheit, die Mitarbeitenden die Einhaltung der Sicherheitsvorgaben leicht machen und sie nicht in ihrer Arbeit ausbremsen.

Die Anforderungen der IT.
Der Trend zu „eingebauter Sicherheit“ wurde auch deutlich, als wir IT-Führungskräfte fragten, welche Funktionen sie von einem System für Dokumentensicherheit erwarten. An erster Stelle stand eine Aktion zur Freigabe „privater“ Dateien (*Abbildung 7*).

ABBILDUNG 7

Wichtigkeit von Funktionen für sicheres Dokumenten-Management aus der Sicht von IT-Führungskräften.



Hinzu kommt, dass Unternehmen immer mehr nach Lösungen für Dokumenten-Management suchen, mit denen sie nicht nur PDF-Dokumente, sondern auch andere Arten von Dokumenten schützen können, z. B. Videodateien. Ein integriertes System ist außerdem sicherer als ein System, das aus mehreren Lösungen zusammengesetzt wurde.

Empfehlungen für IT-Führungskräfte in Unternehmen.

Eine flexible, sichere Arbeitsumgebung.

Es nützt nichts, eure Teams überall arbeiten zu lassen, wenn dadurch das Risiko von Sicherheitsverletzungen und Cyber-Attacken steigt und die Sicherheit eurer Dokumente beeinträchtigt wird. Auf der anderen Seite ist es ebenso wenig praktikabel, die Sicherheitsmaßnahmen so streng zu definieren, dass Mitarbeitende die autorisierten Plattformen nicht mehr sinnvoll nutzen können. Ohne Zugang zu den offiziellen Kanälen suchen sie sich andere Wege – und dann ist überhaupt keine Sicherheit mehr gewährleistet.

Integrierte Lösungen.

Viele externe Mitarbeitende zu verwalten, ist komplex genug – auch ohne die kanalübergreifende Zusammenführung von Dokumenten-Management, Filesharing und elektronischen Unterschriften. Je einfacher ihr euren Teams das Leben macht, desto produktiver sind sie bei ihrer Arbeit, und desto rentabler ist euer Unternehmen.

Sicherheit als Selbstverständlichkeit.

Mitarbeitende sollten sich auf ihre eigentlichen Aufgaben konzentrieren können, ohne sich Gedanken um Sicherheit machen zu müssen. Gebt ihnen Tools an die Hand, die es ihnen leichter machen, das Richtige zu tun.

Adobe.

Maximiert die Sicherheit eurer vorhandenen Technologie-Stacks und Daten mit integrierten Lösungen für digitale Dokumente – von einem Anbieter, für den Sicherheit generell oberste Priorität hat.

Adobe

Zuverlässigkeit und Identitätsprüfung in Acrobat Sign.

Acrobat Sign: Vertrauen an erster Stelle.

Acrobat Sign ermöglicht die Verwendung der fortgeschrittenen und qualifizierten Unterschriften mit der Gewissheit, dass die Sicherheit einer einfachen E-Signatur mit einem zusätzlichen digitalen Zertifikat kombiniert wird. Da diese Zertifikate manipulationssicher sind, werden vor allem qualifizierte Signaturen von vielen Ländern als die rechtssicherste Signatur gegenüber der einfachen E-Signatur anerkannt, z. B. in der EU und in einigen Ländern außerhalb des Commonwealth. Mittels Verschlüsselung wird das zusätzliche digitale Zertifikat untrennbar mit dem Dokument verbunden. Dadurch wird die Identität der Unterzeichnenden belegt. Zeitstempel und ein manipulationssicheres Siegel schaffen auch bei einfachen Signaturen zusätzliches Vertrauen in die Echtheit des Dokuments.

Rechenzentren in der EU / EMEA.

Regionale Rechenzentren: mehr Performance und Sicherheit für euer Business.

Mehrere Document Cloud-Rechenzentren befinden sich in EMEA bzw. in der EU.
Das bedeutet, dass eure Daten DSGVO-konform gespeichert werden – für optimale Performance, Zusammenarbeit und sichere Zugriffsmöglichkeiten. Da Document Cloud und Creative Cloud einen gemeinsamen Speicherplatz nutzen, stehen euch das volle Potenzial und alle Features der Document Cloud-Services zur Verfügung, z. B. beim Erstellen, Bearbeiten und Freigeben von PDF-Dokumenten direkt in Microsoft 365-Programmen.
Die größere Kontrolle über Features ermöglicht zudem die schnellere Akzeptanz im Unternehmen und höhere Speichereffizienz.

BSI C5-Testat.

C5: Eure Sicherheit hat stets oberste Priorität.

Adobe Document Cloud erfüllt die Vorgaben von C5 (Cloud Computing Compliance Criteria Catalogue), ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) eingeführtes Testatschema. Mit dem BSI C5-Testat wird Cloud-Service-Providern bescheinigt, dass sie international anerkannte IT-Sicherheitsstandards befolgen und damit ein konsistentes Sicherheits-Framework bereitstellen. Das BSI C5-Testat ist Teil unseres Bestrebens zur Bereitstellung von höchster Cloud-Sicherheit – durch Transparenz beim Datenschutz und die Beachtung von IT-Sicherheitsstandards bei der Verwaltung eurer Daten.

Methodik.

Dieses von Adobe in Auftrag gegebene Whitepaper von London Research basiert auf einer Umfrage unter 200 IT-Führungskräften in Unternehmen, die für die Dokumenten-Management-Software verantwortlich sind. Die Teilnehmenden arbeiten im Vereinigten Königreich, in Frankreich und in Deutschland. Die Umfrage wurde im Februar 2023 durchgeführt. Als Unternehmen werden Organisationen mit einem Jahresumsatz von mehr als 100 Mio. £ betrachtet.

Über uns.

LONDON RESEARCH
Research Powered Content

London Research wurde von Linus Gregoriadis gegründet, ehemals Research Director bei Econsultancy. Wir produzieren auf Forschungsergebnissen basierenden Content für den B2B-Markt. Hauptsitz des Unternehmens ist London, wir agieren aber auf internationaler Ebene. In erster Linie (aber nicht ausschließlich) arbeiten wir mit Technologieanbietern und Agenturen zusammen, die überzeugenden Content auf Basis von zuverlässigen und aufschlussreichen Daten bereitstellen möchten.

Als Teil von Communitize Ltd arbeiten wir eng mit unseren Schwestergesellschaften Digital Doughnut (weltweite Community von mehr als 1,5 Millionen Marketern) und Demand Exchange (Plattform für Lead-Generierung) zusammen, um gemeinsame Forschungserkenntnisse zu konsolidieren und hochwertige Leads zu erzeugen.

Weitere Infos

Adobe Acrobat

Dokumente sind die Basis von Geschäftsabläufen. Teams von heute wollen von überall aus arbeiten können – mit vertrauenswürdiger Software, die sich gut an andere Lösungen anbinden lässt. Adobe Acrobat wurde vom Erfinder des PDF-Formats entwickelt. Damit erhaltet ihr ein umfassendes Toolset für die Arbeit mit PDF-Dokumenten und elektronischen Unterschriften an jedem Ort. Ihr erhaltet alles, was ihr für nahtlose Dokumentenprozesse braucht, mit einer einzigen Lösung von einer verlässlichen Marke.

Weitere Infos


LONDON
RESEARCH
Research
Powered
Content