KMU im Zeitalter der Arbeitsflexibilität: Sicherheit als oberste Priorität.

LONDON RESEARCH
Research Powered Content

In Zusammenarbeit mit

Adobe

Inhalt

3 Einführung
4 Dokumenten-Management im Zeitalter der Arbeitsflexibilität
6 Die Bedeutung von Dokumenten-Management-Funktionen
8 Die Risiken
9 Empfehlungen für IT-Führungskräfte in KMU
11 Über uns

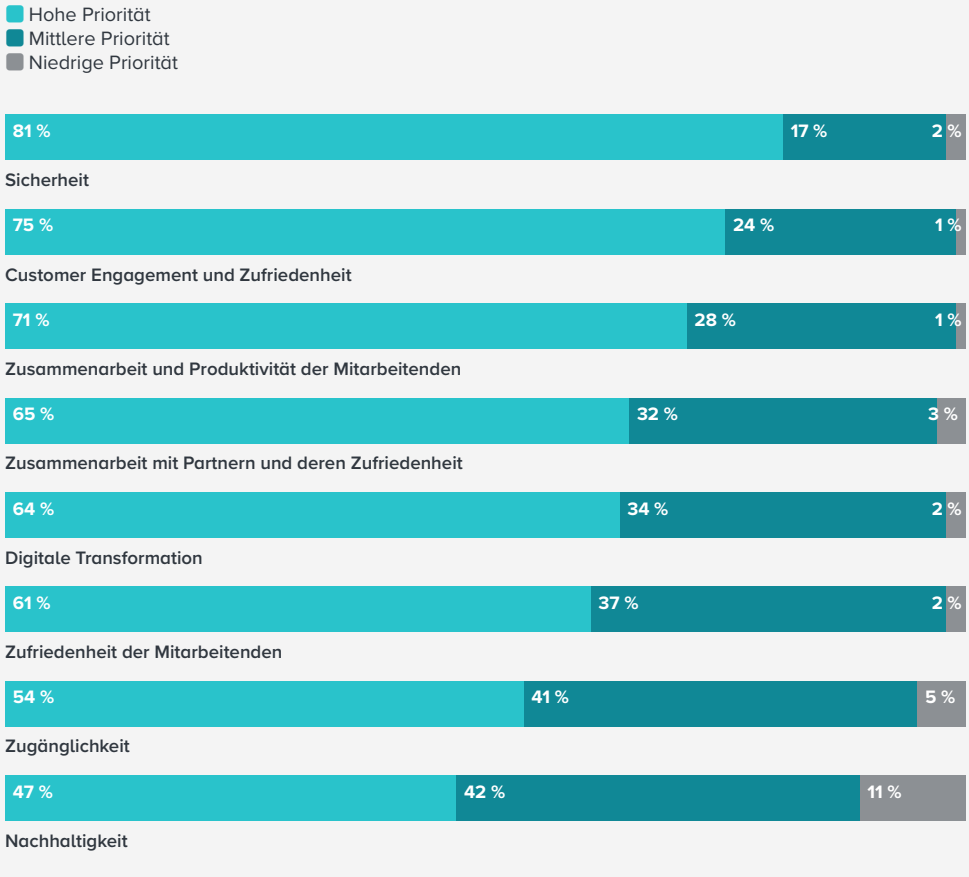
Einführung.

Arbeitsflexibilität stellt IT-Führungskräfte vor eine große Herausforderung. Das Problem ist nicht, dass das eigene Personal Zeit und Ort für die Arbeit selbst bestimmt. Das Problem ist, dass auch alle anderen Mitarbeitenden im Unternehmen das tun, was zu erheblichen Sicherheitsrisiken führt. In einer 2023 gemeinsam mit Adobe durchgeführten Umfrage unter IT-Führungskräften von kleinen und mittleren Unternehmen (KMU) in der EMEA-Region gaben vier von fünf Befragten (83 %) an, dass heute mehr Personal im Homeoffice arbeitet als je zuvor. Davon bestätigten fast drei Viertel (71 %), dass ihr Unternehmen durch die zunehmende Remote-Arbeit anfälliger für Sicherheitsprobleme ist.

Tatsächlich hat Sicherheit für 81 % der Befragten höchste Priorität (*Abbildung 1*), noch vor Kundenzufriedenheit (75 %), Mitarbeiterproduktivität (71 %) oder der Vorbereitung auf die digitale Zukunft (64 %). Für die meisten von ihnen (63 %) ist das Thema Sicherheit in den letzten 12 Monaten ein dringendes Anliegen geworden.

ABBILDUNG 1

Prioritäten verschiedener Bereiche für CTOs/CIOs im Jahr 2023.

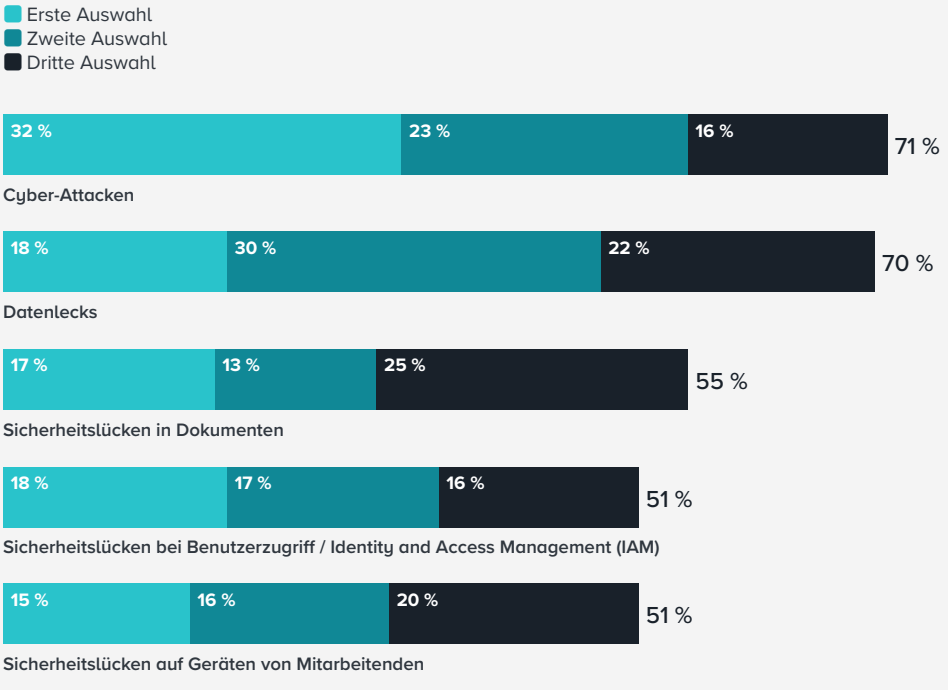


Der Grund dafür liegt auf der Hand. Solange alle Mitarbeitenden eines Unternehmens innerhalb der Firewall arbeiten, ist es in der Regel kein Problem, die Sicherheit und Integrität der IT-Infrastruktur zu gewährleisten. Deutlich schwieriger wird es, wenn über ungesicherte Netzwerke oder private Laptops,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

Als wir die IT-Führungskräfte in KMU nach ihren derzeit größten Bedenken fragten, überraschte uns die Antwort nicht: Sicherheitslücken in vertraulichen Dokumenten gehören nach Cyber-Attacken und Datenlecks zu den drei Problemen, die ihnen am meisten Kopfzerbrechen bereiten (*Abbildung 2*).

ABBILDUNG 2

Die drei größten Herausforderungen und Bedenken im Zusammenhang mit Sicherheit.



Dokumenten-Management im Zeitalter der Arbeitsflexibilität.
Dokumentensicherheit umfasst drei grundlegende Aspekte:

Zugriffssicherheit.

Wird der unerlaubte Zugriff auf Dokumente verhindert?

Content-Sicherheit.

Wird die unerlaubte Weitergabe ganzer Dokumente oder vertraulicher Informationen in Dokumenten verhindert? Lässt sich erkennen, wenn ein Dokument nach der Weitergabe manipuliert wurde?

Systemsicherheit.

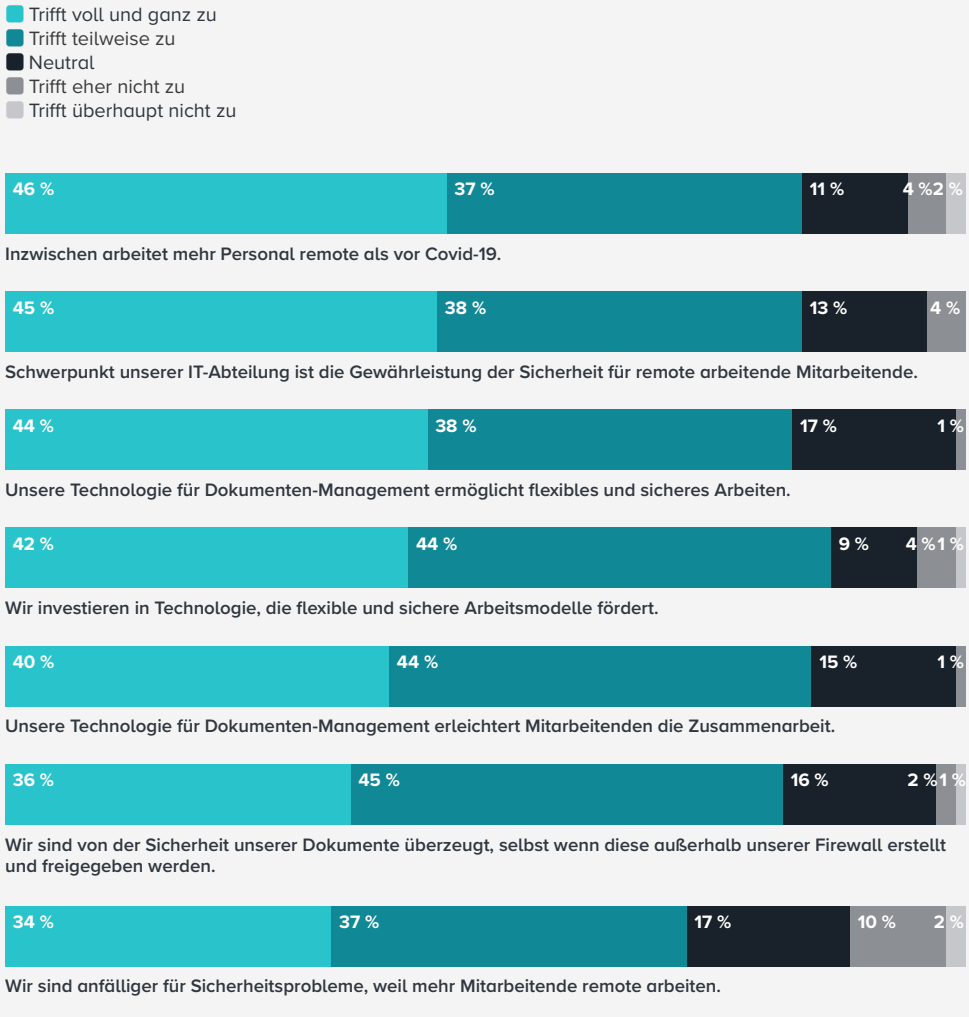
Werden die Systeme einer Organisation vor böswilligen Zugriffs- und Manipulationsversuchen der Dateisysteme einzelner Computer geschützt?

Tatsächlich ist sich mehr als die Hälfte der befragten IT-Führungskräfte nicht sicher, ob die Dokumente in ihrer Organisation effektiv geschützt werden. Eine der größten Herausforderungen ist Zusammenarbeit. Wie wir gesehen haben, hat effiziente Remote-Arbeit im Team für IT-Abteilungen Priorität. Die Sicherung der Punkt-zu-Punkt-Kommunikation zwischen Beschäftigten und Unternehmens-Server ist das eine. Wenn die Beschäftigten aber auch untereinander Dokumente austauschen und sie gemeinsam überprüfen und bearbeiten, steigt die Komplexität – und damit das Risiko – exponentiell an.

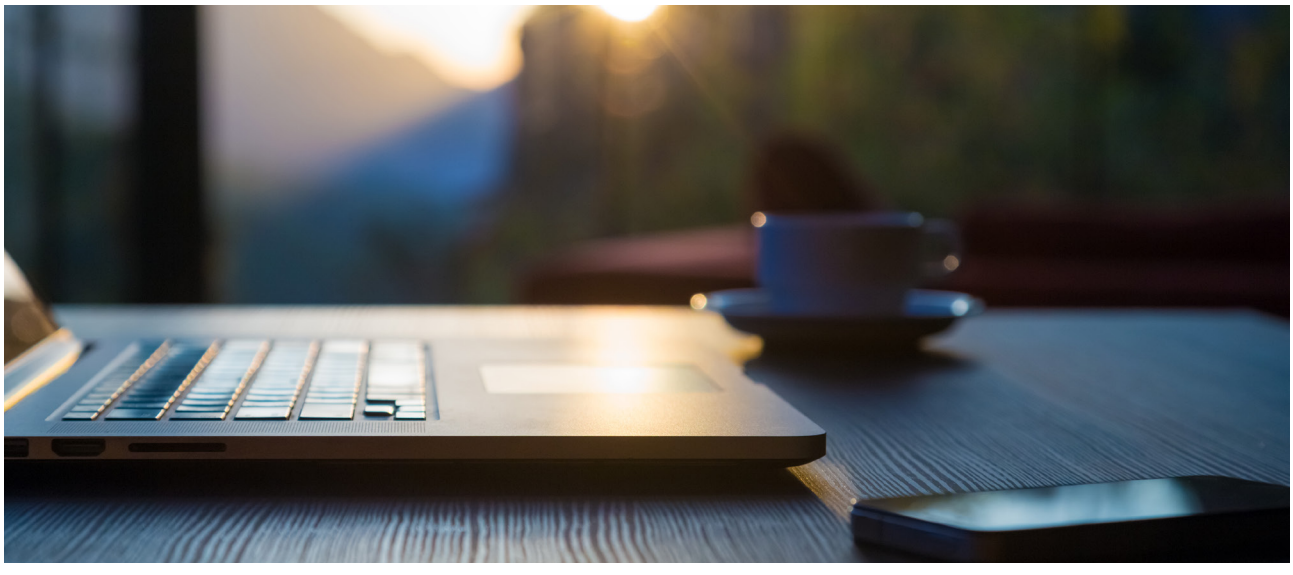
Wie *Abbildung 3* zeigt, denken nur 44 %, dass ihre Technologie für Dokumenten-Management flexibles und sicheres Arbeiten unterstützt. Ein noch geringerer Anteil (36 %) ist wirklich von der Sicherheit der eigenen Unternehmensdokumente überzeugt, selbst wenn diese außerhalb der Unternehmens-Firewall erstellt und freigegeben werden. Demgegenüber stehen 45 %, die Zweifel an der Sicherheit ihrer Dokumente haben.

ABBILDUNG 3

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



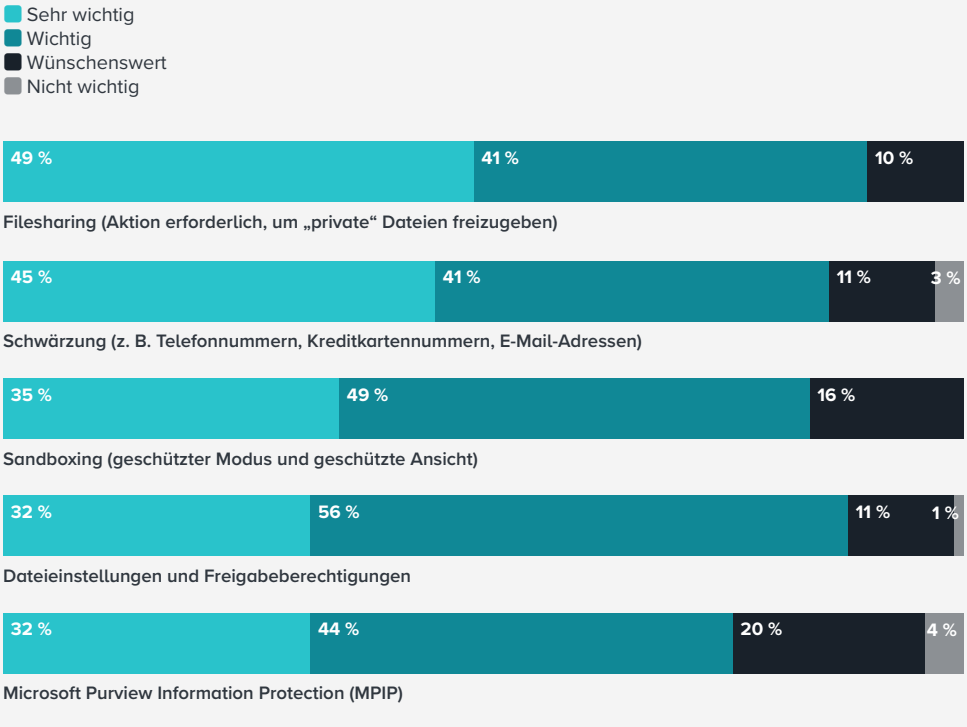
Aus Sicht der IT-Führungskräfte in KMU lohnt sich eine Investition in Dokumenten-Management-Systeme, weil diese Sicherheitsrisiken senken und die Mitarbeiterproduktivität erhöhen. Bei der Suche nach einer Technologie, die den Anforderungen von Remote-Arbeit gerecht wird, müssen Flexibilität und Sicherheit deshalb als gleich wichtig und gleichwertig betrachtet werden.



Die Bedeutung von Dokumenten-Management-Funktionen.
IT-Führungskräfte in KMU erwarten von einer sicherheitsorientierten Software für Dokumenten-Management vor allem zwei Dinge: die Gewährleistung des Datenschutzes beim Filesharing und die Möglichkeit zur Schwärzung sensibler bzw. vertraulicher Informationen in Dokumenten, bevor diese verteilt werden. Diese Funktionen wurden von 49 % bzw. 45 % der Befragten als „sehr wichtig“ erachtet (*Abbildung 4*).

ABBILDUNG 4

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

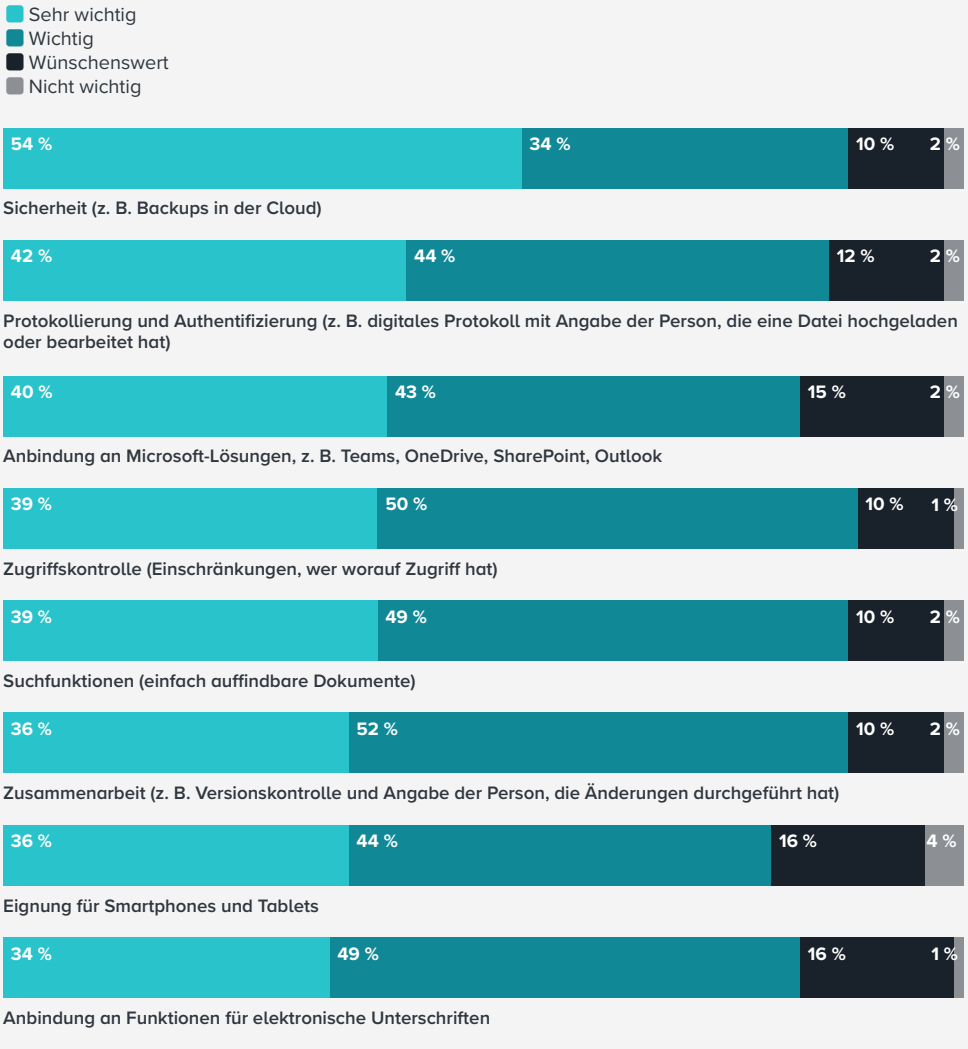


Andere Funktionen wie Sandboxing, Dateieinstellungen und Freigabeberechtigungen sowie Microsoft Purview Information Protection wurden von der Mehrheit zwar als „wichtig“ erachtet, aber nicht als zwingend notwendig.

Mehr als die Hälfte der von uns befragten IT-Führungskräfte sagte auch, dass die Mitarbeitenden ihrer Unternehmen großen Wert auf Sicherheit bei der täglichen Arbeit legen (*Abbildung 5*). Es ist das einzige Feature, das für mehr Befragte „sehr wichtig“ ist, als für Befragte, für die es „wichtig“ ist. Die wenigsten Befragten finden, dass Sicherheit lediglich „wünschenswert“ ist.

ABBILDUNG 5

Wichtigkeit von Funktionen im Dokumenten-Management aus der Sicht von Mitarbeitenden.



Auch an dieser Stelle wird deutlich, wie wichtig es ist, Sicherheit und Bedienfreundlichkeit ins Gleichgewicht zu bringen. Bestimmte Features wie Protokollierung, Authentifizierung oder Zugriffskontrolle, die eigentlich auch zu einem sicheren System gehören, werden von Mitarbeitenden deutlich seltener als „sehr wichtig“ bewertet.

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 Risiken.

Laut einer Studie von IBM[1] beliefen sich 2022 die weltweiten Durchschnittskosten von Datenlecks auf 4,35 Mio. $ – das sind 12,7 % mehr als 2020. In Großbritannien betrugen diese Kosten 5,05 Mio. $, in Deutschland 4,85 Mio. $ und in Frankreich 4,34 Mio. $. Die US National Cyber Security Alliance fand heraus, dass 70 % aller Cyber-Attacken gegen kleine und mittlere Unternehmen gerichtet sind, einfach weil Cyber-Sicherheit bei Firmen dieser Größe weniger stringent gehandhabt wird.[2] Dabei kann es sich z. B. um folgende Kosten handeln:

- **Lösegeldzahlungen**
- **Sinkender Aktienkurs (für börsennotierte Unternehmen)**
- **Umsatzeinbußen durch Systemausfälle**
- **Behebung/Wiederherstellung**
- **Rechts- und Audit-Kosten.** Harvard Business Review[3] 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**

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.[4]
- **Erschwerte und kostspieligere Finanzierungen**. HBR hebt zudem hervor, dass Cyber-Risiken zu einer Herabstufung der Kreditwürdigkeit führen können.
- **Image-Verlust.** (Potenzielle) Kundinnen und Kunden betrachten die Marke als weniger vertrauenswürdig. Laut einem Bericht von PwC[5] 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[6] können nationale Datenschutzbehörden 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.

1 https://www.ibm.com/reports/data-breach
2 https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses
3 https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach
4 https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/
5 https://www.pwc.com/gx/en/news-room/press-releases/2022/global-digital-trust-insights-survey.html
6 https://gdpr.eu/fines/

Empfehlungen für IT-Führungskräfte in KMU.

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 eure Organisation.

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 kleinen und mittleren 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 KMU werden Unternehmen mit einem Jahresumsatz von höchstens 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