Dokumentensicherheit gewährleisten

Fahrplan für KI, Arbeitsflexibilität und Vertrauen in einer vernetzten Welt

Holly Muscolino
Group Vice President,
Workplace Solutions, IDC

Grace Trinidad, PhD, MPH, MS
Research Director,
Trust Measurement and Metrics, IDC

Inhalt

ZUM ÖFFNEN EINES KAPITELS AUF DIE ENTSPRECHENDE ÜBERSCHRIFT UNTEN KLICKEN.

Überblick

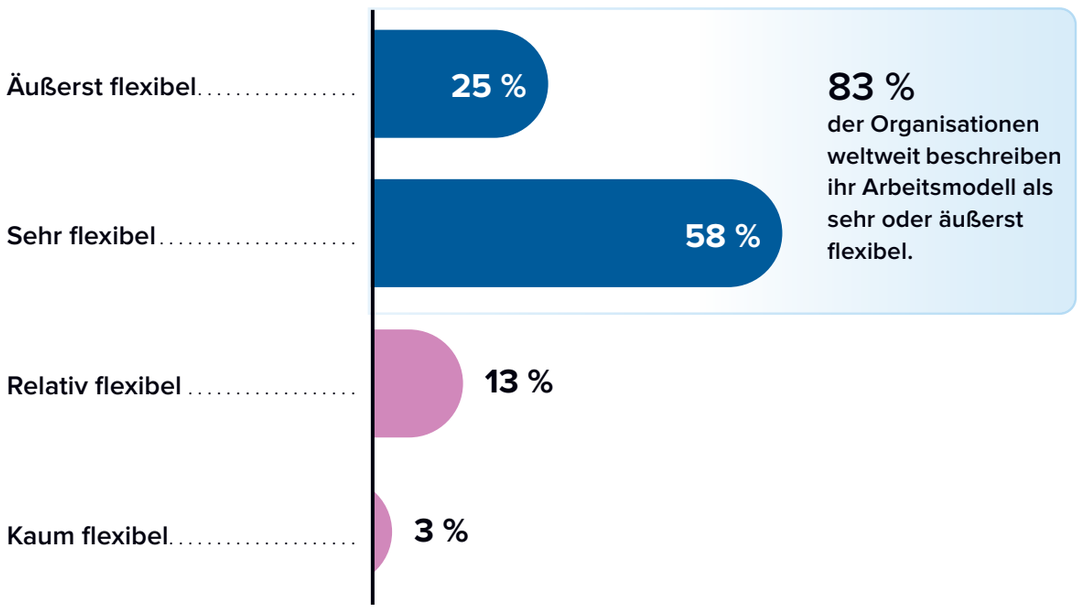
Im Zeitalter integrierter Technologieplattformen, generativer KI (GenAI), verteilter Teams und flexibler Arbeitsmodelle **müssen viele Organisationen ihre Konzepte für Sicherheit und Governance überdenken und anpassen. Dies betrifft auch die Dokumentensicherheit.**

Dieser InfoBrief beleuchtet einen oft vernachlässigten Aspekt in den Sicherheitsstrategien von Organisationen: den Schutz von (Daten in) Dokumenten. Analystinnen und Analysten von IDC haben mit 3 Entscheidungstragenden über die Herangehensweise ihrer Organisationen an das Thema Sicherheit und Compliance gesprochen. Dieser InfoBrief umfasst auch Einblicke aus IDC-Studien zur Sicherheit von Organisationen im Zeitalter von Arbeitsflexibilität und GenAI.

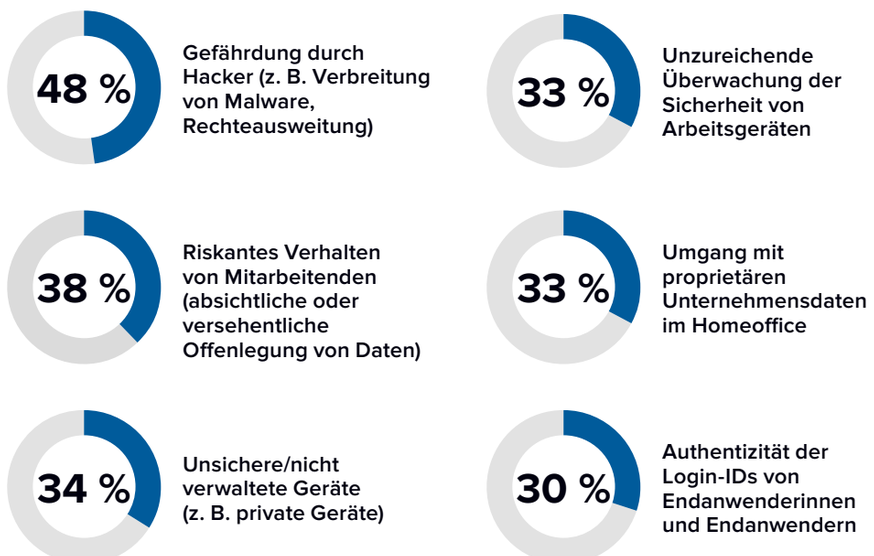
Flexibles Arbeiten erhöht Sicherheitsbedenken

Führungskräfte stufen die im Rahmen flexibler Arbeitsmodelle verwendeten Systeme als anfälliger für Hacking ein. Der Schutz vor Sicherheitsbedrohungen ist daher schwierig.

Wie flexibel ist das Arbeitsmodell eurer Organisation?



Was sind eure größten Sicherheitsbedenken im Zusammenhang mit flexiblem Arbeiten?



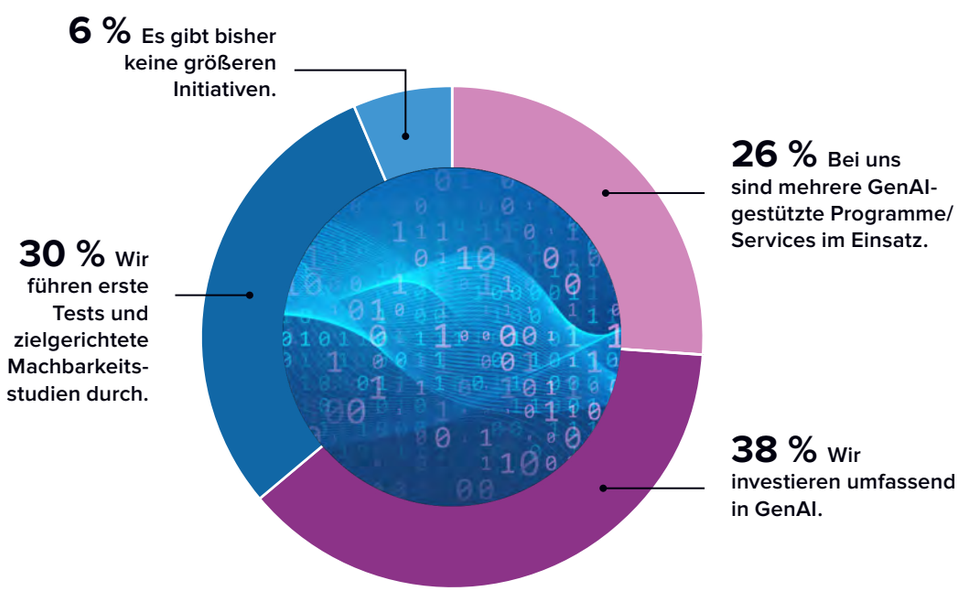
Hinweis: Die Werte sind gerundet, daher ergibt die Summe nicht unbedingt 100 %. n = 1.269. Quelle: *Worldwide Future of Work Survey*, IDC, Juni 2024

Flexible Arbeitsmodelle ergeben größere (oder neue) Sicherheitsbedenken.

GenAI bringt eine neue Ebene an Sicherheitsbedenken mit sich

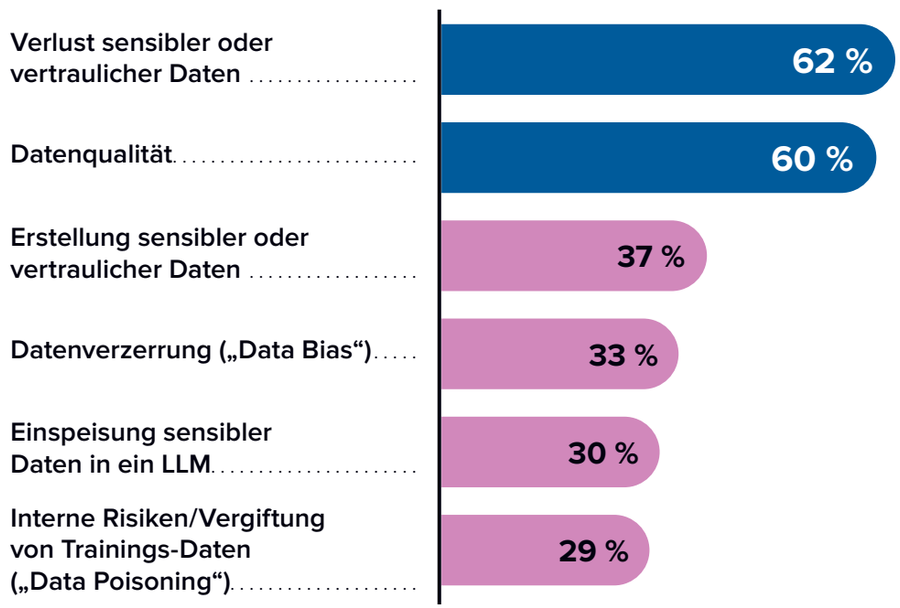
63 % der Organisationen investieren umfassend in GenAI oder haben bereits GenAI-Lösungen implementiert. Das führt zu **neuen Bedenken hinsichtlich Sicherheit und Compliance**.

Informiert ihr euch über oder verwendet ihr bereits GenAI?



Hinweis: Die Werte sind gerundet, daher ergibt die Summe nicht unbedingt 100 %. n = 891. Quelle: *Future Enterprise Resiliency & Spending Survey Wave 7*, IDC, Juli 2024

Was sind eure größten Sicherheitsbedenken bei der Verknüpfung eurer Systeme mit GenAI-Modellen?



Hinweis: LLM = Large Language Model. n = 619. Quelle: *Data Privacy Survey*, IDC, März 2024

Dokumente sind der Motor jedes Unternehmens

Obwohl 80–90 % der Daten von Organisationen unstrukturiert sind und bei den meisten Geschäftsprozessen Dokumente eine wesentliche Rolle spielen, wird der Schutz von Daten in Dokumenten bei organisationsweiten Sicherheitsstrategien oft vernachlässigt.

Vertrieb

- Verträge und Vereinbarungen
- Angebote und Ausschreibungen

Rechtswesen

- Vertragsverwaltung
- Vertraulichkeitsvereinbarungen

Finanzen

- Genehmigung von Budgets
- Genehmigung von Spesen
- Genehmigung von Rechnungen

Remote-Arbeit

- Programme
- Richtlinienänderungen
- Verträge und Vereinbarungen

Produkt-Management

- Änderungsberechtigungen
- Zustimmung zu Produktanforderungen
- Freigabe von Roadmaps

IT

- Lieferantenverträge
- Asset-Management
- Änderungsanträge

Marketing

- Onboarding von Kundschaft
- Selfservice
- Marketing-Verträge
- Freigabeerklärungen

Personalverwaltung

- Leistungspakete
- Mitarbeitenden-Onboarding
- Anträge auf Zusatzleistungen
- Selfservice

Dokumentensicherheit ist mit Herausforderungen verbunden

Die Sicherheit digitaler Dokumente ist von zentraler Bedeutung für Organisationen. Mit der zunehmenden Verbreitung flexibler Arbeitsmodelle wird sie umso bedeutender.

Dokumente als Angriffsvektor	Jeder Dateityp kann für Angriffe missbraucht werden (z. B. DOC, XLS, PPT, JPEG oder PNG). PDF-Dateien sind aufgrund ihrer weiten Verbreitung aber besonders beliebt. Palo Alto Networks hat 2020 gegenüber dem Vorjahr **einen Anstieg um 1.160 % bei manipulierten PDF-Dateien** festgestellt. (Quelle: unit42.paloaltonetworks.com/phishing-trends-with-pdf-files)
Unbefugter Zugriff oder Weitergabe	Da digitale Dokumente und PDF-Dateien leicht zu teilen sind, **führen lose Zugriffskontrollen schnell zur unerwünschten Weitergabe von oder zum unautorisierten Zugriff auf wichtige Dokumente.** Die ISO-Richtlinie 27001, Anhang A, Abschnitt 9.2.1, schreibt die Einschränkung des Zugriffs auf Informationen und Programme vor.
Unbefugte Datenextraktion und IP-Risiken	Kriminelle und fahrlässig handelnde Mitarbeitende **können eine Organisation dem Risiko der unberechtigten und schädlichen Extraktion von Daten aussetzen.** Manipulierte Metadaten, auswählbarer Text, eingebettete Objekte und Links sowie Formulardaten lassen sich in jedem Dokumententyp verbergen.
Compliance	Gemäß aktuellen Sicherheitsbestimmungen und -Frameworks wie der DSGVO, Artikel 32, Abschnitt 1, müssen Unternehmen „geeignete technische und organisatorische Maßnahmen [treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein: **Pseudonymisierung und Verschlüsselung personenbezogener Daten**“.

„Die organisationsinterne Identifizierung und Verwertung von Daten ist mir ein wichtiges Anliegen … Wenn Daten von einem System an ein anderes übergeben werden, wollen wir genau nachvollziehen können, um welche Daten es sich handelt.“

Leitung der Programmentwicklung bei einem großen Versicherungsunternehmen

HERAUSFORDERUNGEN IM DETAIL:

Dokumente als Angriffsvektor

Dokumente in beliebten Formaten wie PDF werden oft als Angriffsvektor genutzt. Sie sind flexibel, werden von zahlreichen Plattformen unterstützt und ermöglichen die leichte Einbettung von verschlüsselten Streams, JavaScript-Code, ausführbaren Dateien oder anderen manipulierten Elementen.

2022 entdeckte Sophos Labs eine Variante der Ransomware Locky in einem VBA-Makro in einem Word-Dokument, das in einer PDF-Datei verborgen war. Wenn die Bearbeitung gemäß den Anweisungen des Dokuments aktiviert wurde, lud das VBA-Makro die Ransomware herunter und führte sie aus.

„[Es braucht] ein mehrstufiges Sicherheitskonzept [...] Daten müssen bei der Übertragung verschlüsselt werden, aber auch im Ruhemodus. Dokumente müssen nachweislich für den beabsichtigten Zweck [sicher] sein [...] PDF ist der Goldstandard."

Leitung der Programmentwicklung bei einem großen Versicherungsunternehmen

HERAUSFORDERUNGEN IM DETAIL:

Dokumente als Angriffsvektor (Fortsetzung)

Häufig instrumentalisierte Dokumenttypen

- PDF
- MS Office-Dokumente (DOCX, PPTS, XSLX)
- Komprimierte Dateien (ZIP, RAR)
- Bilddateien (JPEG, PNG, GIF)
- Ausführbare Anhänge (EXE, MSI)

Häufige Angriffsvektoren

- Schädlicher Code oder Makros
- Verschlüsselte Streams, Bilder, ausführbare Dateien
- Schwachstellen in PDF-Viewern oder Microsoft-Programmen
- Phishing über gefälschte Inhalte

Sicherheitskontrollmaßnahmen

- Aufklärung und Training
- Sandboxing von Anhängen
- Einschränkungen bei Dateitypen
- Verschlüsselung von E-Mails
- Anti-Virus- und Anti-Malware für Endpunkte

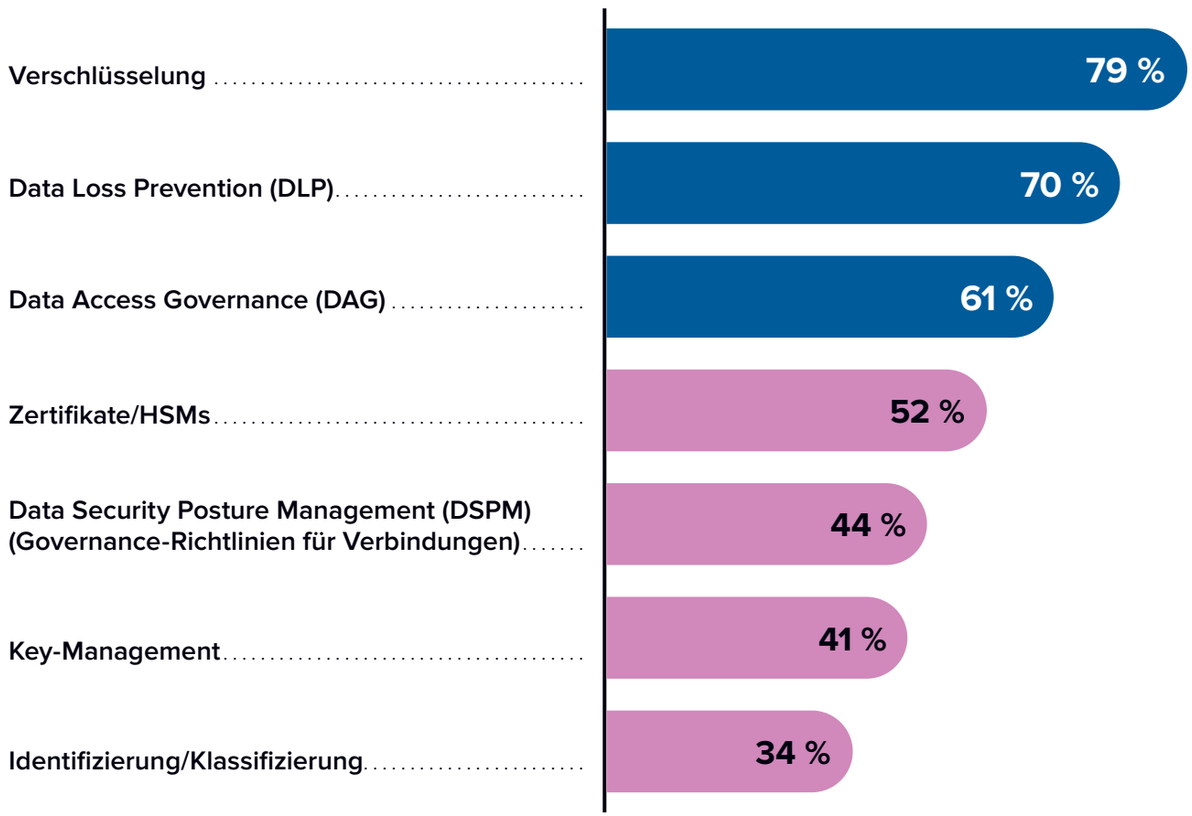
HERAUSFORDERUNGEN IM DETAIL:

Unbefugter Zugriff oder Weitergabe

Wichtige Sicherheitstechnologien

- Authentifizierung und vertrauenswürdige Sites
- Zugriffssteuerung
- Sicherheit auf Programmebene (Sandboxing, JavaScript-Sicherheit)
- Compliance-Zertifizierungen
- Digital Rights Management
- Digitale Signaturen
- Verschlüsselung
- Labels zum Informationsschutz
- Schwärzung
- Freigabe sicherer Links, Positivliste für Links
- Sicherer Speicher
- Sicherheitstests durch Dritte

Welche Sicherheitstechnologien werden weltweit zur Gewährleistung von Datenschutz/Compliance eingesetzt?



Hinweis: HSM = Hardware-Sicherheitsmodul. n = 227. Quelle: *North America eSignature Market Survey*, IDC, November 2021

HERAUSFORDERUNGEN IM DETAIL:

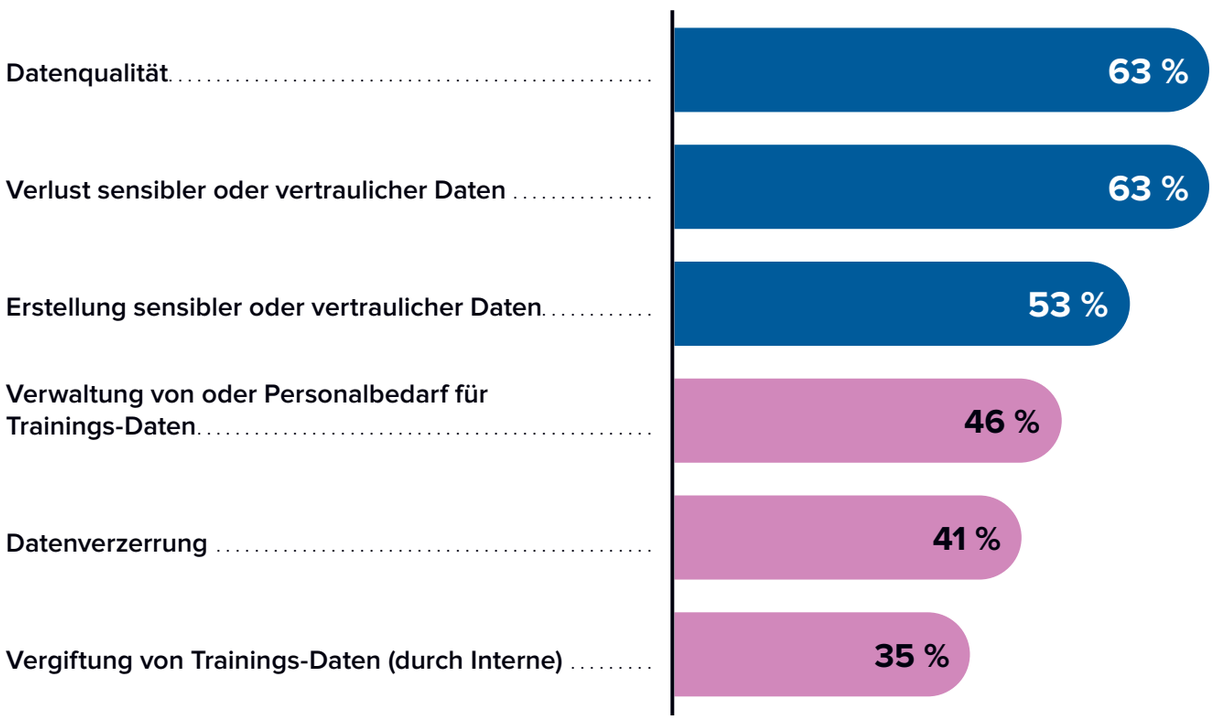
Unbefugte Datenextraktion und IP-Risiken

GenAI erhöht das Risiko unautorisierter Zugriffe auf sensible Daten.

„Wir wollen GenAI so verantwortungsvoll wie möglich nutzen. Für den Zugriff auf unstrukturierte Daten [wurde] über 10 Jahre [knapp] 1 Mrd. USD investiert, um Hadoop-Data Lakes einzurichten [...] Und als GenAI herauskam, hat man alles eingestampft, weil die Data Lakes jetzt angeblich überflüssig sind."

Leitung der Programmentwicklung bei einem großen Versicherungsunternehmen

Was sind eure größten Sicherheitsbedenken bei der Verwendung öffentlicher GenAI-Modelle?



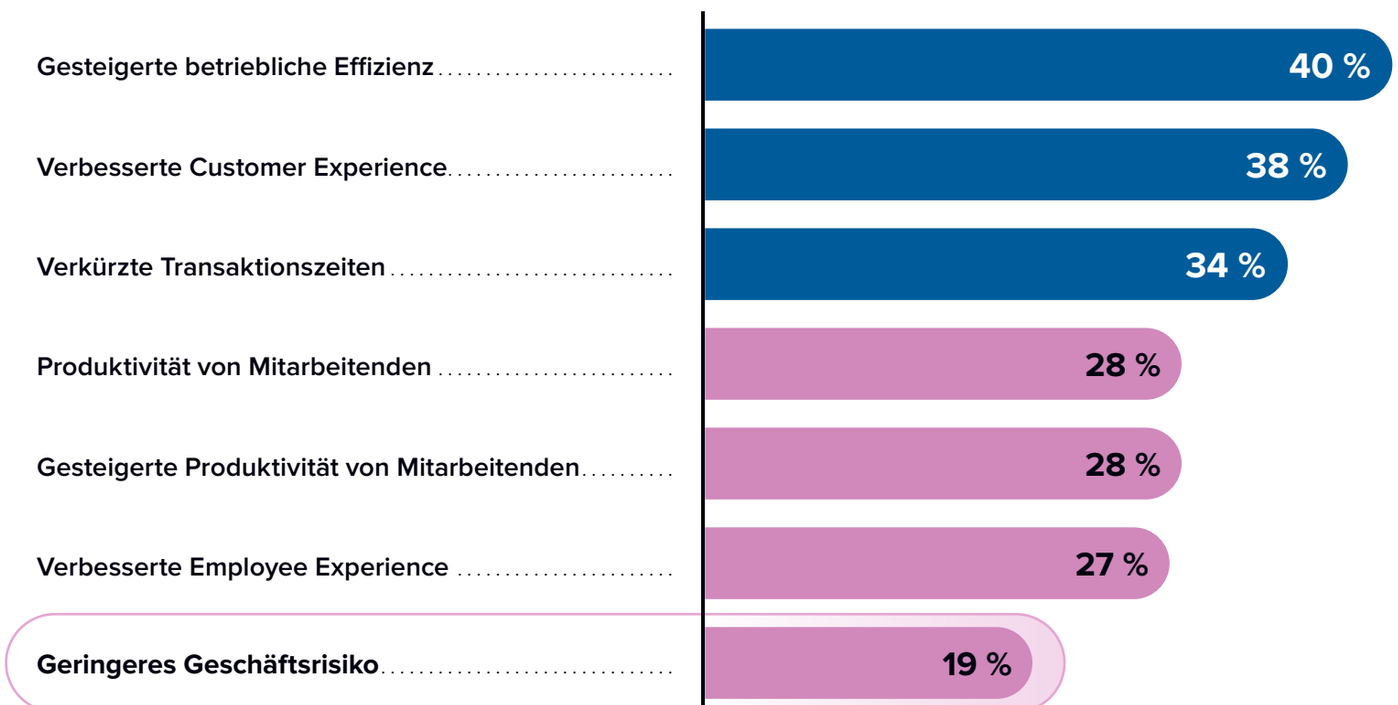
n = 610. Quelle: *Data Privacy Survey*, IDC, März 2024

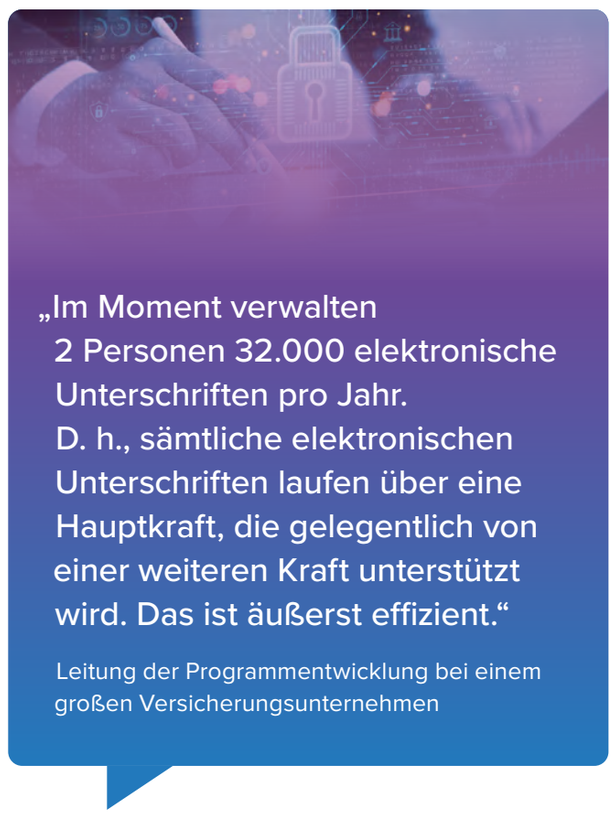
HERAUSFORDERUNGEN IM DETAIL:

Dokumentenintegrität

Die Verwendung elektronischer Unterschriften und digitaler Signaturen hat sich als effizient erwiesen.

Welche der folgenden Geschäftsvorteile verzeichnet ihr oder erhofft ihr euch durch den Einsatz von Technologien und/oder Services für intelligente, digitale Workspaces?





„Im Moment verwalten 2 Personen 32.000 elektronische Unterschriften pro Jahr. D. h., sämtliche elektronischen Unterschriften laufen über eine Hauptkraft, die gelegentlich von einer weiteren Kraft unterstützt wird. Das ist äußerst effizient."

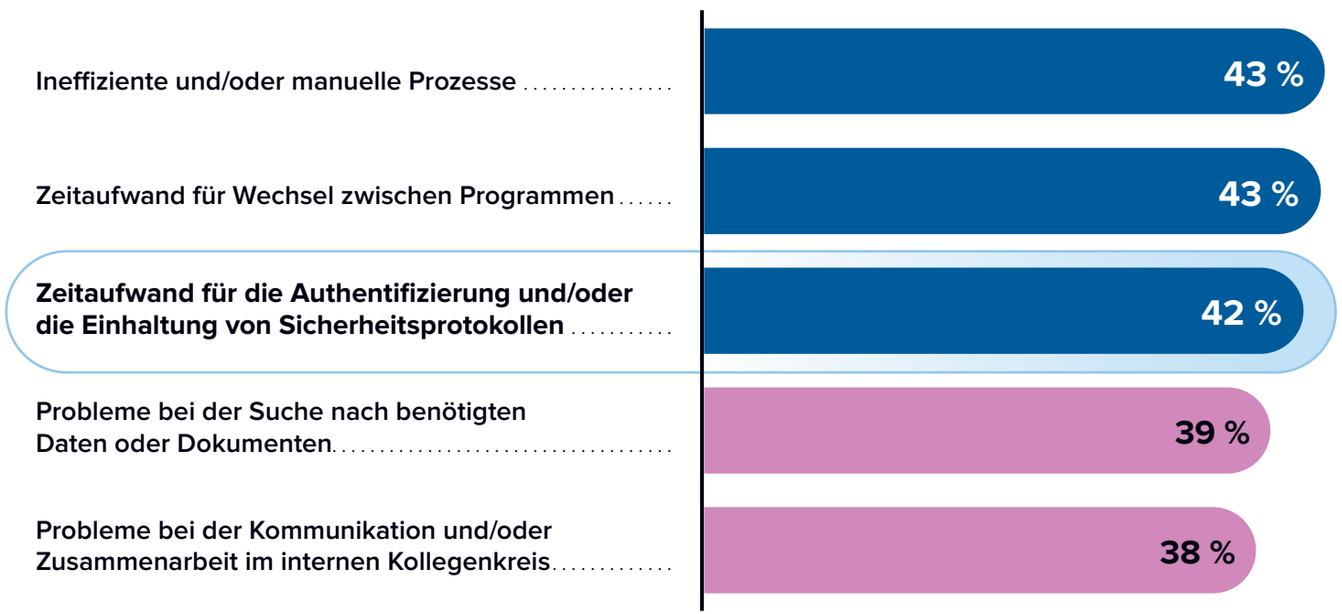
Leitung der Programmentwicklung bei einem großen Versicherungsunternehmen

n = 227. Quelle: *North America eSignature Market Survey*, IDC, November 2021

Eine weitere Herausforderung: Protokolle

Der Zeitaufwand für die Einhaltung von Sicherheitsprotokollen gehört zu den 5 größten Herausforderungen, die Mitarbeitende daran hindern, so effizient wie möglich zu arbeiten.

Was sind die 5 größten Herausforderungen, die Mitarbeitende daran hindern, so effizient wie möglich zu arbeiten?



„Es ist wichtig, [...] dass wir einen personenzentrierten Sicherheitsansatz haben. Als Sicherheits-Team müssen wir unbedingt die Beschäftigten vertreten, für die wir zuständig sind."

Chief Information Security Officer bei einem großen Software-Unternehmen

n = 609. Quelle: *Intelligent Digital Workspace Market Survey*, IDC, Mai 2022

Empfehlungen

Weltweit sind mehrere Billionen digitale Dokumente und PDF-Dateien in Gebrauch – und es kommen täglich neue hinzu. **Maßnahmen für sichere Dokumenten-Workflows sollten daher in der Sicherheitsstrategie einer Organisation nicht fehlen.**

- **Implementiert dokumentenzentrierte Programme**, die standardmäßig Funktionen wie das Sandboxing von Anhängen, Einschränkungen bei Dateitypen und Verschlüsselung nutzen.
- **Definiert Richtlinien und Verfahren**, die die Anzeige und Weitergabe von Dokumenten durch Unbefugte verhindern, inkl. Authentifizierungs-, Identitäts- und Zugriffskontrollen.
- **Informiert euch über Risiken und neue Sicherheitsbedrohungen durch KI**, und stimmt eure Sicherheitsstrategie darauf ab.
- **Denkt an den Faktor Mensch**. Fördert ein sicherheitsfokussiertes Mindset im Unternehmen. Verbessert Workflows und Richtlinien für Vor-Ort- und Remote-Arbeit. Erleichtert Mitarbeitenden die Einhaltung von Vorgaben.
- **Arbeitet mit einem erfahrenen Technologieanbieter zusammen**, der euch bei der Umsetzung dieser Empfehlungen unterstützen kann und sich selbst als Glied in der breiteren operativen Lieferkette sieht.

Anhang: Glossar

Flexibles Arbeiten bzw. Arbeitsflexibilität: bezeichnet ein dynamisches Arbeitsmodell, bei dem Beschäftigte ihre Aufgaben an unterschiedlichen Orten erledigen – z. B. im Büro, im Homeoffice oder im Außeneinsatz –, abhängig von Unternehmensrichtlinien und Geschäftsanforderungen. Dieses Modell nennt man auch **Hybridarbeit.**

- **Nicht flexibel:** Es gibt keine formelle Strategie zur Unterstützung von Arbeitsflexibilität.
- **Kaum flexibel:** Einige Führungskräfte ermöglichen flexible Modelle nach Bedarf, aber es gibt keine formelle Strategie.
- **Relativ flexibel:** Die Geschäftsleitung hat vorläufige Richtlinien definiert, die flexibles/hybrides Arbeiten in gewissem Rahmen ermöglichen.
- **Sehr flexibel:** Es gibt Richtlinien für flexibles Arbeiten. Beschäftigte können vor Ort und remote arbeiten – bei Bedarf über mehrere Abteilungen hinweg.
- **Äußerst flexibel:** Beschäftigte können beliebig und ohne Konflikte in Bezug auf Technik/Richtlinien zwischen Remote- und flexibler Arbeit wechseln.

Über die IDC-Analystinnen

Holly Muscolino

Group Vice President, Workplace Solutions, IDC

Als Group Vice President, Workplace Solutions, ist Holly Muscolino verantwortlich für Forschung im Zusammenhang mit Innovation und Transformation bei Content-Lösungen, z. B. für intelligente Dokumentenverarbeitung, elektronische Unterschriften, Bildbearbeitung, Druck und andere Content-Workflow-Services. Sie beschäftigt sich außerdem mit der Transformation der Arbeitswelt, Technologie und digitalen Skills sowie der Rolle von Technologie bei der Gestaltung der Zukunft der Arbeit.

Weitere Infos zu Holly Muscolino

Grace Trinidad, PhD, MPH, MS

Research Director,
Future of Trust, IDC

Grace Trinidad ist Research Director im Bereich Sicherheit und Vertrauen bei IDC und betreut das Forschungsprogramm „Future of Trust“. In dieser Rolle gibt sie strategische Anleitung und Unterstützung bei der Untersuchung verschiedener Aspekte von Vertrauen, darunter Risiken, Sicherheit, Compliance, Datenschutz, Ethik und soziale Verantwortung. Dr. Trinidad hat Peer-reviewte (von Sachverständigen aus demselben Fachgebiet begutachtete) Artikel über Datenschutz und Vertrauen veröffentlicht, in denen sie die Einstellungen der Öffentlichkeit gegenüber der kommerziellen Nutzung personenbezogener Gesundheitsinformationen untersucht. Weitere Forschungsschwerpunkte von Dr. Trinidad sind ethische Fragen rund um künstliche Intelligenz und Datenweitergabe, Vertrauen in das Gesundheitswesen, Einsatz und Barrierefreiheit von Gendatenbanken sowie Fairness im Umgang mit Daten.

Weitere Infos zu Grace Trinidad

Mitteilung des Sponsors

Adobe

Überzeugende Experiences beruhen auf Vertrauen.

Mit Adobe Acrobat können Organisationen zuverlässige Dokumentenerlebnisse bereitstellen, die zu Transformation und Wachstum ihres Business beitragen.

- Erweiterte Funktionen für Datenschutz und Compliance ermöglichen sicheres Arbeiten an jedem Ort.
- Mit hochwertiger Dokumenten-KI lassen sich verifizierbare Einblicke gewinnen und Aufgaben schneller erledigen.

Holt euch Adobe Acrobat noch heute

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
Tel. +1 508 872 8200

idc.com @idc @idc

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktforschungs- und Beratungsdienstleistungen sowie Veranstaltungen auf dem Gebiet der IT undTelekommunikation sowie der Verbrauchertechnologiemärkte. Mit mehr als 1.300 Analysten bietet IDC globale, regionale und lokale Expertise zu Chancen und Trends in Technologie und Wirtschaft in mehr als 110 Ländern. Analysen und Erkenntnisse von IDC unterstützen IT-Profis, Geschäftsleute und Investoren bei fundierten Entscheidungen über Technologien und die Erzielung ihrer wichtigsten Geschäftsziele.