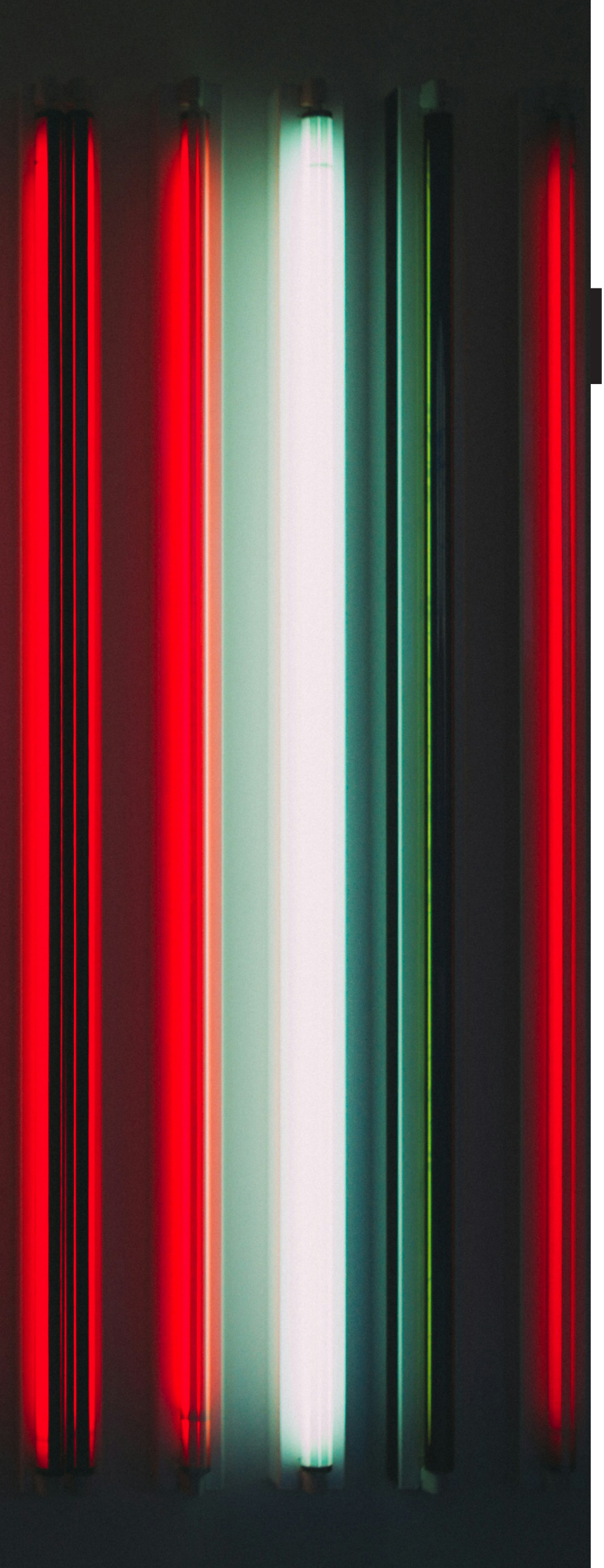


GDV Gesamtverband der Versicherer

FOKUS | DIGITALISIERUNG

# Digitalisierung … aber sicher

Resilienz und IT-Transformation in unsicheren Zeiten

## Einleitung

Mit dem Digital Operational Resilience Act (DORA) hat die EU ein Regelwerk geschaffen, das ab Januar 2025 gilt und darauf abzielt, die digitale operationale Resilienz zu stärken.

Neben der Regulatorik, Zertifizierungen sowie Informations- und Berichtspflichten steht die Versicherungswirtschaft vor der grundsätzlichen Herausforderung, sich gegen eine Vielzahl von Cyberbedrohungen zu verteidigen. Diese gefährden sowohl die Integrität als auch die Verfügbarkeit von kritischen IT-Systemen. Daher gilt es, die IT-Infrastruktur kontinuierlich zu testen und an die dynamischen Bedrohungsszenarien anzupassen. Mitarbeitende mit entsprechenden Expertenkenntnissen sind ein Erfolgsfaktor.

Die teils über Jahrzehnte laufenden Versicherungspolicen erfordern eine verlässliche und resiliente IT-Infrastruktur. Gleichzeitig gilt es einen laufenden Erneuerungsprozess der bestehenden System- und Anwendungslandschaft sicherzustellen. Versicherer bauen daher in der Regel nicht auf die eine neue Technologie, sondern planen innerhalb einer komplexen Umgebung in hybriden Architekturen. Von daher gilt es, die Herausforderung zu meistern und die bewährte IT-Welt mit modernen Ansätzen zu vereinen.

Im aktuellen Umfeld des Fachkräftemangels sticht allem voran die Altersspanne der Mitarbeitenden heraus, die von den Babyboomern bis hin zur Generation Z reicht. Es bleibt abzuwarten, wie es gelingt, in diesem Umfeld etwaige kulturellen und sprachlichen Barrieren zu überwinden.

## INFORMATIONSSICHERHEIT UND RESILIENZ

In Quantität und Qualität nehmen Cyber-Bedrohungen zu und führen zu einer andauernd angespannten Sicherheitslage.[1] Dabei liegt das höchste Gefährdungspotenzial sicherlich bei Ransomware-Angriffen, ob nun gesteuert durch die organisierte Kriminalität oder staatliche Akteure. Ebenfalls steigt die Gefahr durch mit Künstlicher Intelligenz (KI) und teils schon in Echtzeit gemachter Deep-Fakes. Gleichzeitig liegt ein immanentes Risiko in den weltweit vernetzten IT-Infrastrukturen. So hat ausgerechnet ein – nicht ausreichend getestetes – Sicherheitsupdate am 19. Juli 2024 zum bis dahin größten weltweiten IT-Ausfall geführt.

Diese verletzlichen Strukturen und die hochdynamische Sicherheitslage erfordern unbestritten eine Steigerung der Resilienz und damit eine verbesserte Fähigkeit der Unternehmen, Störungen, Notfälle und Krisen zu überstehen. Dazu zählen neben hoher Sicherheit weitere Faktoren wie finanzielle Stabilität, regulatorische Konformität und operative Belastbarkeit.

Den hohen Stellenwert, den die Cybersicherheit und Regulatorik schon heute im IT-Portfolio der Versicherer einnimmt, zeigen stetig auch die Ergebnisse der GDV-IT-Erhebung. Danach sind beide, die seit Jahren am höchsten priorisierten und am weitesten fortgeschrittenen Themenbereichen (vgl. Abb. 1).

Kritisch muss in diesem Zusammenhang konstatiert werden, dass die für Regulatorik und Zertifizierungen erforderlichen Ressourcen nicht für Innovations- und Transformationsvorhaben zur Verfügung stehen. Eine in Teilen überbordende Regulatorik geht damit eindeutig zu Lasten der Wettbewerbsfähigkeit der hochregulierten Versicherer.

Ungeachtet dessen ist Cybersicherheit nicht verhandelbar, sondern integraler Bestandteil der Versicherungs-IT. Dies zeigt sich einmal mehr durch deren Gewichtung innerhalb der IT-Schwerpunkte im direkten Vergleich von 2023 zu 2024. Hier zählt das Themenfeld Cybersicherheit (+3,3 Punkte) neben KI (+5,4 Punkte), Robotics Process Automation (+5,5 Punkte) und Cloud Infrastructure-as-a-Service (+3,3 Punkte) zu den Themen mit der perspektivisch höchsten Bedeutung.[2] In einer Detailbetrachtung lassen sich zum IT-Themenschwerpunkt Cybersicherheit folgende beiden Aspekte hervorheben.

### Penetrationstests

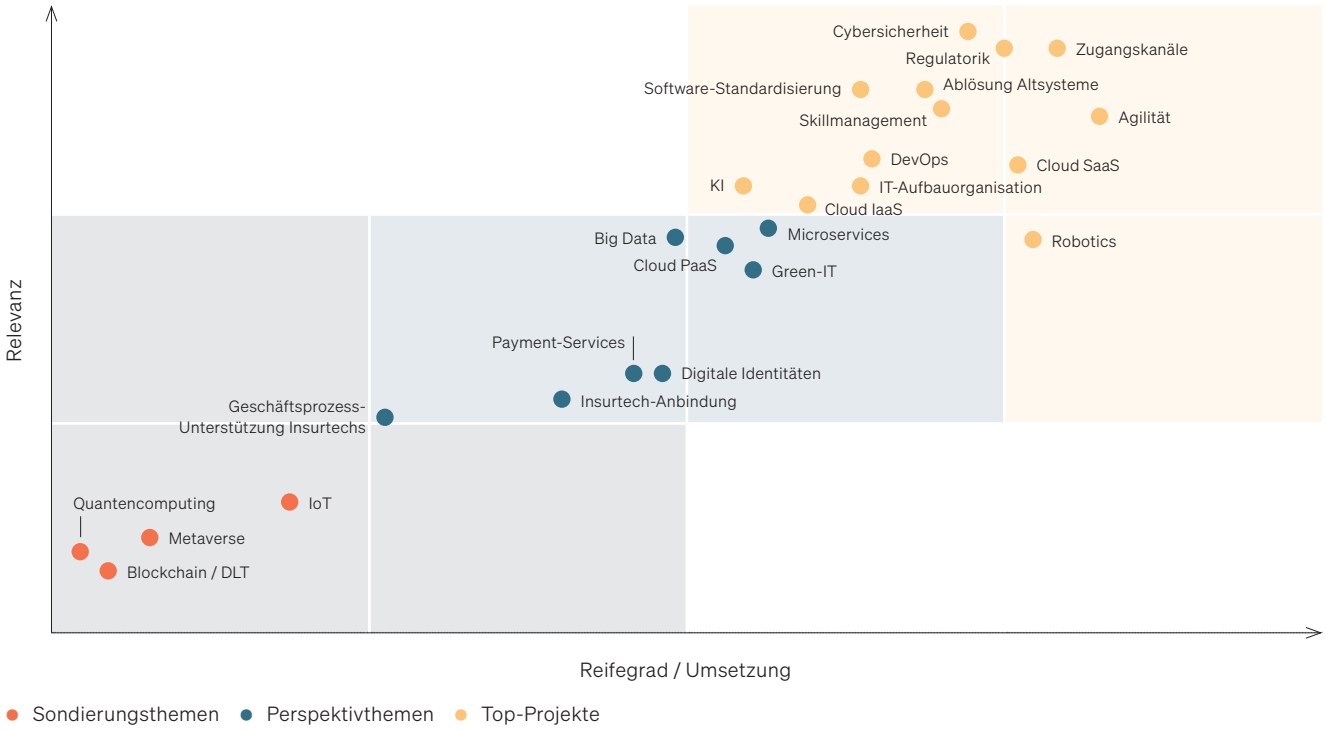
Bei der Durchführung sogenannter Penetrationstests greifen die Unternehmen, mit einem Anteil von über 90 %, fast ausschließlich auf externe Anbieter mit sehr spezialisiertem Expertenwissen zurück. Gründe dafür sind die sehr hohen Anforderungen an interne Tests und die begrenzten internen Mitarbeiterkapazitäten (MAK). Gleichzeitig können durch den Einsatz externer

[1] Zahlen, Daten und Fakten aus dem IT-Lagebericht, BSI, 2023

[2] Das Themenfeld Regulatorik verzeichnet 2024 einen leichten Rückgang in der perspektivischen Schwerpunktbetrachtung. Grund könnte sein, dass etwaige DORA-Projekte zum 17.01.2025 zumindest größtenteils abgeschlossen sein müssen und/oder auslaufen.

## Schwerpunkte der Digitalisierung 2024

**Abbildung 1** · Thematische Relevanz und Reifegrad




Quelle: GDV IT-Erhebung 2024

Anbieter ungewünschte Effekte wie Betriebsblindheit und Interessenkonflikte vorgebeugt werden.

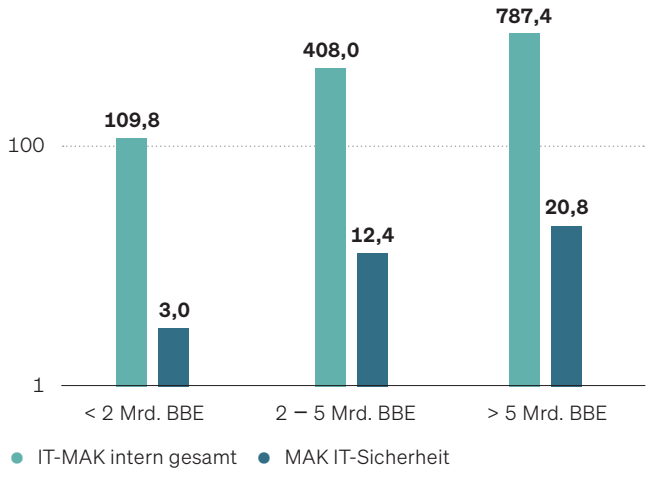
Im Schnitt führten die sehr großen Unternehmen (> 5 Mrd. Euro BBE)[3] im Jahr 2023 zwischen 40 und 50 Penetrationstests durch, was nahezu einem pro Woche entspricht. Perspektivisch erwarten Branchenexperten, dass die Anzahl der Penetrationstests unter DORA signifikant zunehmen werden. Damit einhergehend werden die Kosten für Testing steigen und die IT-Budgets belasten. Darüber hinaus führt diese Entwicklung zu einer zusätzlichen Bindung interner Mitarbeiterressourcen für Steuerung und Nachbearbeitung.[4]

### Mitarbeiterkapazitäten in der IT-Sicherheit

Die Versicherungsunternehmen investieren signifikant in Fachkräfte, um den wachsenden Anforderungen gerecht zu werden und um den demografischen Herausforderungen begegnen zu können. Hierzu zählen auch die in der IT und Informationssicherheit beschäftigten Personen beziehungsweise anteiligen MAK. Nach der aktuellen Branchenerhebung verhalten sich die für die IT-Sicherheit eingesetzten MAK proportional zur internen IT-Mitarbeiterzahl. Über die Unternehmensgröße sind nur marginale Degressionseffekte erkennbar (vgl. Abb. 2). Beispielsweise liegt der

## Personal für IT-Sicherheit

**Abbildung 2** · IT-Mitarbeiterkapazitäten (MAK) gesamt im Verhältnis zu MAK für IT-Sicherheit (Mittelwerte nach BBE-Größenklassen)




Quelle: GDV IT-Erhebung 2024

[3] BBE = Bruttobeitragseinnahmen

[4] Befragt wurden die Mitglieder des GDV-Expertennetzwerkes „Informationssicherheit", September 2024

MAK-Anteil bei kleinen (< 2 Mrd. BBE), mittelgroßen Unternehmen (2 – 5 Mrd. BBE) und großen Unternehmen (> 5 Mrd. BBE) im Schnitt bei 2,7 % bis 3,0 %; bei den sehr großen Unternehmen mit einem Anteil von 2,6 % kaum geringer, was die hohe Relevanz von Informationssicherheit für alle Unternehmensgrößen betont. Ob diese Proportionalität weiterhin gewahrt bleibt, wird sich mit Anwendung der DORA ab Januar 2025 zeigen.

## CLOUD, KÜNSTLICHE INTELLIGENZ UND AUTOMATISIERUNG

### Cloud und hybride IT-Architekturen

Der Mainframe wird nach den Zahlen der aktuellen Erhebung zumindest mittelfristig fester Bestandteil der Versicherungs-IT bleiben. Die Ablösung der Alt-Systeme ist demnach weiterhin von hoher Relevanz. Allerdings ist sie aufgrund ihrer Komplexität und vor dem Hintergrund stetig neuer regulatorischer Anforderungen nur schrittweise umsetzbar.

Trotz teilweiser Ablösung des Mainframes ist der Kostenanteil an den IT-Gesamtausgaben[5] im Verlauf der letzten fünf Jahre – nach dem Motto „weniger, dafür teurer“ mit 9 % stabil geblieben. Die Reduzierung der Betriebskosten wird damit durch einen gleichzeitigen Anstieg der Lizenzkosten egalisiert.

Mit Blick auf die Ausgaben für Cloud-Systeme ist eine dynamische Entwicklung zu konstatieren. Deren Kostenanteil liegt mit 3,2 % der gesamten IT-Ausgaben noch auf recht niedrigem Niveau. Insgesamt lässt sich für die Versicherungsbranche bei den Cloud-Ausgaben im Vergleich der Jahre 2023 und 2022 aber eine erhebliche Kostensteigerung in Höhe von rund 27 % feststellen. Dieser Anstieg liegt deutlich über den weltweit durchschnittlichen Ausgaben für Public-Cloud-Anwendungen in Höhe von 17,3 %.[6] In der Gesamtbetrachtung kann jedoch festgestellt werden, dass die Versicherungsbranche auf nationaler Ebene weder Vorreiter noch Nachzügler beim Einsatz von Cloud-Lösungen ist. So weisen mittlerweile 80 % der an der Verbandserhebung beteiligte Versicherungsunternehmen Kosten für Cloud-Lösungen auf, was in etwa dem Wert für die gesamte deutsche Wirtschaft entspricht (siehe Abb. 3).[7]

Der Reifegrad der Cloud-Lösungen bei den Versicherungsunternehmen steigt kontinuierlich an, ist aber längst nicht am Ende der Skala angelangt. Dies gilt für alle Anwendungsfelder, wobei Software-as-a-Service (SaaS) die Cloud-Dienstleistung mit der stärksten Durchdringung ist, gefolgt von IT-Lösungen betreffend Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS). Die nächsten Jahre werden zeigen, wie die weitere Entwicklung bei der Cloud-Nutzung vorangehen wird. Besonders wichtig ist hier die Sicherstellung der Flexibilität in einer dynamische IT-Welt durch Dual- und Multicloud-Strategien.

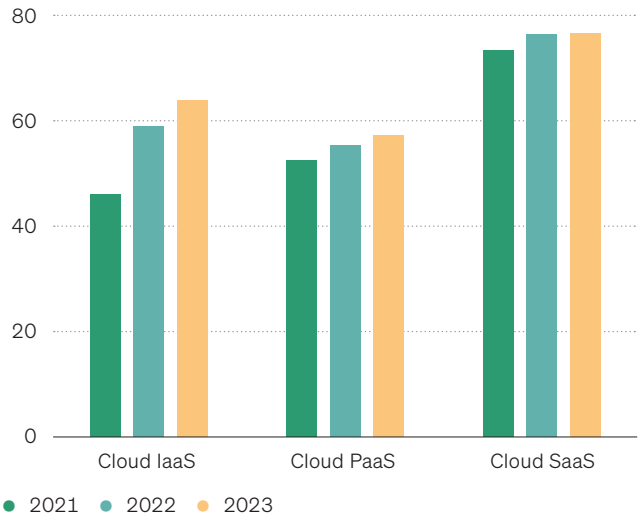
### Künstliche Intelligenz und Robotics Process Automation

Der Hype um KI hat in diesem Jahr einen neuen Höhepunkt erreicht. Große Sprachmodelle und generative KI haben eindrucksvoll unter Beweis gestellt, dass die hohe Erwartungshaltung an KI nicht unbegründet ist. Von Texterstellung, Coding, Bildgenerierung bis Sprachassistenz – das Einsatzspektrum von KI in der Versicherungswirtschaft ist so groß wie nie.

Wie eingangs erwähnt, liegt KI als Top-Thema in der perspektivischen Relevanz in etwa gleichauf mit Robotics Process Automation (RPA). Im Vergleich beider Technologien ist KI für die Versicherer relevanter, dafür sind Reifegrad und Umsetzung bei RPA weiter vorangeschritten (vgl. Abb. 1).

### Cloud-Lösungen nach Reifegrad

**Abbildung 3** · Cloud-Lösungen nach Reifegrad, Entwicklung des prozentualen Reifegrads in verschiedenen Cloud-Anwendungsfeldern 2021 bis 2023, in %




Quelle: GDV IT-Erhebung 2024

[5] Die IT-Ausgaben (Kosten) belaufen sich für das Jahr 2023 für die gesamte Branche auf 6,2 Mrd. Euro (Quelle: GDV IT-Erhebung)

[6] https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024, abgerufen im September 2024

[7] Welche Rolle spielt die Cloud für die deutsche Wirtschaft, Cloud-Report 2024, Berlin, bitcom-Research

Diese nuancierten Unterschiede in den beiden Technologien lassen sich damit begründen, dass KI über die Fähigkeit verfügt, zu lernen und komplexe unstrukturierte Aufgaben zu lösen. Das Potential und die Leistungsfähigkeit sind somit der des RPA überlegen, was sich in der höheren Relevanzeinstufung widerspiegelt. RPA ist hingegen eine Technologie, die darauf abzielt, wiederholbare, regelbasierte Aufgaben mittels vordefinierter Skripte zu automatisieren. Die Implementierung dieser Skripte ist um ein Vielfaches einfacher und schneller als das Training eines KI-Modells, weshalb RPA im Reifegrad und der Umsetzung noch vorne liegt.

Bei KI verfolgen Versicherer die ganze Bandbreite möglicher Anwendungsfälle, setzen jedoch auch bewusste Schwerpunkte (vgl. Abb. 4). Am weitesten fortgeschritten ist die Durchdringung bei unternehmensinternen KI-Tools wie „GitHub Co-Pilot“ und „Microsoft Co-Pilot“. In der Sachbearbeitung nennen die Unternehmen eine Reihe von Maßnahmen, die unter anderem die Texterkennung, automatisierte Erstellung von Schriftstücken, Large Language Models und semantische Textanalyse umfassen. Des Weiteren findet sich KI vermehrt unterstützend im Kundenservice. Neben einzelnen Chat- und Voice-Bots kommen auch ganzheitliche Sprachdialogsysteme zum Einsatz. In der Betrugserkennung setzen die Unternehmen sowohl interne als auch externe Tools ein. Mit diesen sollen Auffälligkeiten beispielsweise in Bilddaten, Dokumenten oder den Kernsystemen erkannt werden. Ebenso streben die Unternehmen einen höheren Automatisierungsgrad in der Schaden-Regulierung an, bspw. durch kanalgesteuerte Schadenmeldungen und Verfahren zur Dokumentenverifikation.

Im Bereich der Risikomodellierung und Tarifierung zeigen sich die Unternehmen noch zurückhaltend. Einige verweisen in diesem Zusammenhang auf zusätzliche Komplexität durch den EU AI Act. Ebenfalls noch in einem frühen Stadium befindet sich der Einsatz von (unternehmenseigenen) Sprachmodellen. Anlageberatung mittels KI hat eine geringe Relevanz. „Know Your Customer“ (KYC) ist für die Unternehmen durchaus ein Thema, allerdings wird dort im Wesentlichen Standard-Software ohne KI-Bezug eingesetzt.

## Automatisierung

Die sogenannte Dunkelverarbeitungsquote – als Indikator für vollautomatisierte Geschäftsprozesse – steigt signifikant in der privaten Krankenversicherung (2022: 25,2 %, 2023: 32,3 %) sowie in der Schaden-/

### KI-Anwendungsfälle

**Abbildung 4** · Relevanz und Reifegrad


Quelle: GDV IT-Erhebung 2024

Unfallversicherung „SHUK/RS“ (2022: 30,6 %, 2023: 33,5 %).[8]

Hinsichtlich der Digitalisierung der Kundenschnittstelle ist erstmalig eine Stagnation bei der E-Mail-Kommunikation mit einem Anteil von etwa 54 % sowie ein weiterhin rückläufiges Papierposteingangs von 36 % im Jahr 2019 auf 23 % in 2023 festzustellen. Seit vier Jahren steigt dagegen ungebrochen die Nutzung der Online-Serviceportale durch Kundinnen und Kunden von 10 % in 2019 auf einen beachtlichen Anteil von inzwischen 22 % in 2023 (vgl. Abb. 5).

Die erfreuliche Zunahme der Nutzung von Onlineservices erhöht – durch den gleichzeitigen Einsatz durchstrukturierter Prozessstrecken und Webdialoge – den Standardisierungsgrad gegenüber der unstrukturiert eingehenden E-Mail. Zudem trägt die Digitalisierung der Kundeninteraktion unter Nachhaltigkeitsgesichtspunkten wesentlich zur Papierreduktion bei. So war es den Versicherern möglich, die Anzahl der gedruckten Seiten um etwa 15 % gegenüber dem Vorjahr zu senken.

Die beschriebene Entwicklung in der allgemeinen Kundeninteraktion und der Automatisierung steht in Wechselwirkung mit der Quote der digitalen Abschlüsse im Neugeschäft. Diese stieg in den letzten Jahren ebenfalls kontinuierlich, sodass mittlerweile fast jeder fünfte Vertrag ohne menschliches Zutun abgeschlossen wird.[9] Im Spartenvergleich liegen die Anteile digitaler Abschlüsse in der Kranken- und Kraftfahrtversicherung mit fast 29 % bzw. 24 % am höchsten.

## Demografie, Diversität und Führungskräftestruktur

Die Babyboomer der geburtenstarken Jahrgänge der 1960er-Jahre scheiden nach und nach aus dem Arbeitsleben aus. Dies sollte niemanden überraschen, da die demografische Entwicklung absehbar war.

Für die Transformation und den Betrieb der IT-Systemlandschaft – einem Mix aus alter und neuer Technologie – gilt es vier Generationen mit unterschiedlichen Kenntnissen und Erwartungshaltungen in der heutigen Arbeitswelt produktiv zusammenzubringen. Dazu zählt die Generation der Babyboomer, die Generation X der Jahrgänge 1970 bis 1985, die Generation Y der Jahrgänge 1986 bis 1999 genauso wie die ab dem Jahr 2000 geborene Generation Z mit ihren neuen Ideen und Ansätzen.

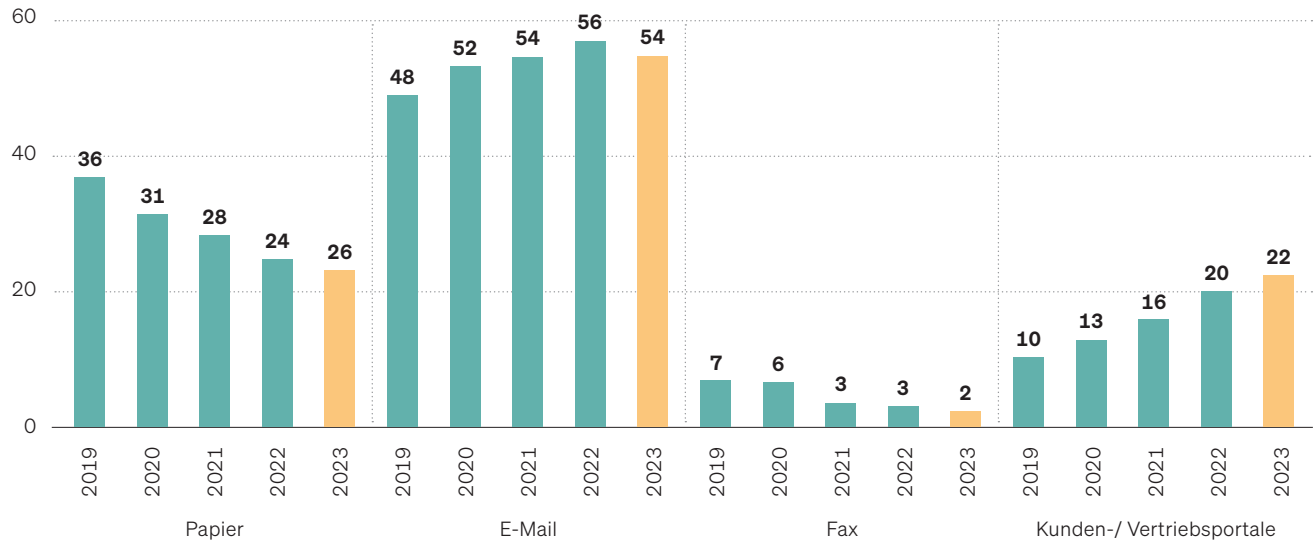
Die aktuellen Kennzahlen gemäß IT-Erhebung zeigen, dass der Anteil der Mitarbeitenden ab dem Alter 56 erstmalig alle jüngeren Alterskategorien dominiert

[8] SHUK/RS = Sach-, Unfall-, Kraftfahrtversicherung / Rechtsschutz

[9] https://www.gdv.de/gdv/medien/medieninformationen/versicherung-vertrieb-abschluesse-digital-181036, abgerufen im September 2024

### Eingangskanäle für Anliegen von Versicherungskunden/-innen

**Abbildung 5** · Prozentuale Verteilung der genutzten Medien




Quelle: GDV IT-Erhebung 2024

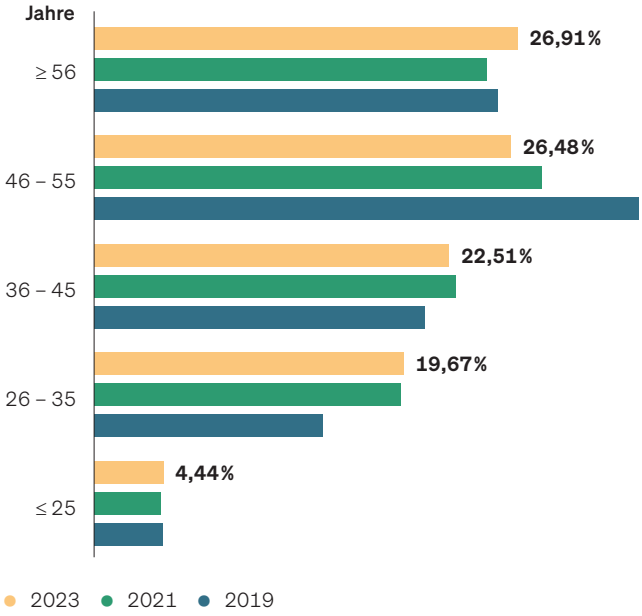
(vgl. Abb. 6). Dies ist umso bemerkenswerter, als dass die Anzahl der internen IT-Mitarbeitenden 2023 netto um 6 % zugenommen hat (Vorjahr: +3,9 %). Die neuen Mitarbeiter sind dabei internationaler und weiblicher, scheinbar jedoch nicht unbedingt jünger als der Durchschnitt der Belegschaft. Die Anstrengungen zum Gelingen eines internen Know-how-Transfers von alt zu jung, über Generations- und Sprachbarrieren hinweg, ist in jedem Fall eine enorme Herausforderung und letztendlich ein Erfolgsfaktor.

Die Erwartungen der jüngeren Generationen richten sich auch auf strukturelle Aspekte. Die Vorteile agiler Arbeitsweisen werden den Lernenden bereits in Bildungseinrichtungen nähergebracht. Streng hierarchische Strukturen dürften damit weniger attraktiv sein. Hier kann die Versicherungswirtschaft punkten, denn die Mehrheit der Unternehmen hat sich bereits mit 20 % bis 90 % ihrer IT-Mitarbeitenden agil aufgestellt. Abzulesen ist dieser Umstand auch am Verhältnis von disziplinarischen IT-Führungskräften zu IT-Mitarbeitenden. Dieses fällt mit durchschnittlich 1:11 im Vergleich zu klassischen Organisationsmodellen mit einem Verhältnis von 1:7 um einiges höher aus.[10]

[10] https://www.mehr-fuehren.de/fuehrungsspanne/ mit entsprechenden Quellenverweisen, abgerufen im September 2024

## Demografie in der Versicherungs-IT

**Abbildung 6** · Altersstruktur interne Mitarbeiter




Quelle: GDV IT-Erhebung 2024

**Gesamtverband der Deutschen Versicherungswirtschaft e. V.**
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax +49 30 2020–6000
www.gdv.de, berlin@gdv.de

**Verantwortlich**
Patrik Maeyer
Leiter Betriebswirtschaft, Prozesse und IT
Tel.: +49 30 2020–5452
E-Mail: p.maeyer@gdv.de

**Autoren**
Mario Heinemann
Patrik Maeyer

**Redaktionsschluss**
21.10.2024

**Publikationsassistenz**
Heike Strauß

**Bildnachweis**
Unsplash

**Alle Ausgaben**
auf GDV.DE