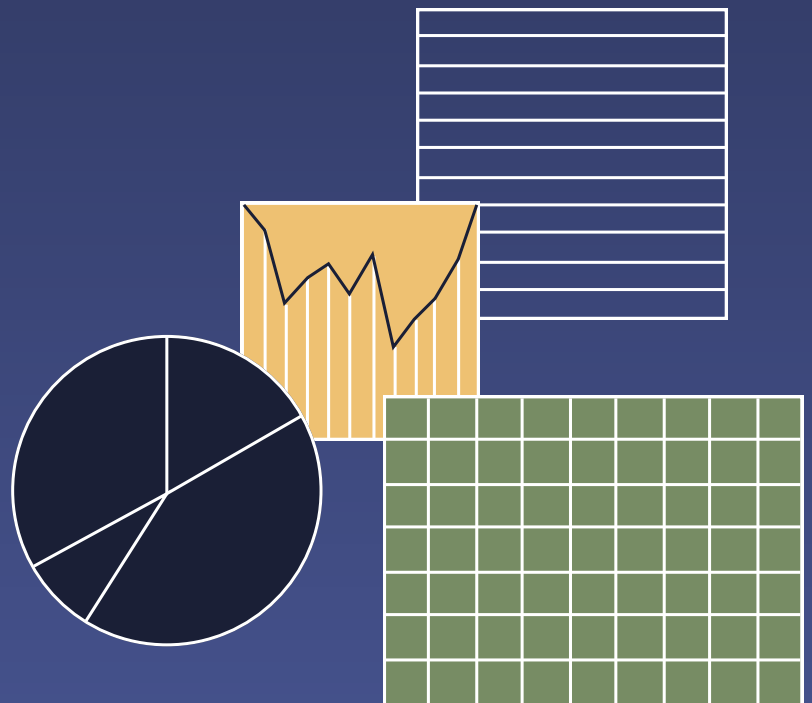

Trendreport geschäftliche E-Mails 2025:

Infrastruktur, Risiken und die nächste Chance für IT



Inhaltsverzeichnis

Zusammenfassung

S. 02

Methodik

S. 05

1

Kapitel 1: Die Rolle der E-Mail im
modernen Kommunikations-Stack

S. 07

2

Kapitel 2: Posteingang unter Beschuss: Wie sich das
Risikoprofil der E-Mail verändert

S. 20

3

Kapitel 3: E-Mail-Verwaltung im großen Maßstab:
Integration, Effizienz und Beschaffungsverhalten

S. 34

4

Kapitel 4: E-Mail-Signaturen für Professionalität,
Konsistenz und Kontrolle

S. 44

5

Kapitel 5: Die Zukunft der geschäftlichen E-Mail

S. 53

Fazit

S. 62

Über Exclaimer

S. 64

Zusammenfassung

Auch im Jahr 2025 bleibt E-Mail das Rückgrat der geschäftlichen Kommunikation – branchenübergreifend und weltweit. Instant-Messaging- und Kollaborationsplattformen gewinnen zwar an Bedeutung, doch keine Lösung kommt an die E-Mail heran, wenn es um Nachvollziehbarkeit, Verbindlichkeit und Professionalität geht. Wenn es zählt, senden Unternehmen eine E-Mail.

Der diesjährige State of Email-Trendreport – basierend auf Erkenntnissen von 4.009 IT-Führungskräften aus dem Vereinigten Königreich, den USA, Deutschland und Australien – zeigt ein Paradoxon: E-Mails sind geschäftskritischer denn je, werden aber häufig mit veralteten Prozessen und zu wenig Ressourcen verwaltet. Von IT-Verantwortlichen wird erwartet, dass sie den am häufigsten angegriffenen Teil der Infrastruktur absichern, veraltete Abläufe modernisieren, Compliance gewährleisten und ein konsistentes Markenbild unterstützen – oft ohne passende Tools, Automatisierung oder Entscheidungsbefugnis.

E-Mail ist nicht nur „noch da“ – sie bleibt geschäftskritisch. Und sie steht unter Druck.

Zentrale Erkenntnisse



1. Mail dominiert weiterhin die geschäftliche Kommunikation

- **89 %** der IT-Führungskräfte halten 1:1-E-Mails für wichtig – etwas wichtiger als Kollaborationstools (**86 %**) und auf Augenhöhe mit Instant Messaging und Videokonferenzen.
- E-Mail bleibt die bevorzugte Lösung für die Kommunikation mit Kunden, interne Mitteilungen sowie IT- und Sicherheitswarnungen – überall dort, wo Zuverlässigkeit und Nachvollziehbarkeit entscheidend sind.

Zusammenfassung

2. Sicherheits- und Compliance-Lücken nehmen zu

- **83 %** der Unternehmen berichten von sicherheitsrelevanten Vorfällen im Zusammenhang mit E-Mails – bei **48 %** traten diese im vergangenen Jahr auf.
- Nur **47 %** fühlen sich hinsichtlich ihrer Compliance-Strategie sehr sicher.
- Phishing und Spoofing zählen zu den größten Sorgen. Dennoch haben weniger als ein Drittel DMARC, DKIM oder SPF implementiert – ein kritisches Sicherheitsdefizit.

3. Zeit wird am falschen Ende investiert

- **37 %** der IT-Verantwortlichen geben an, dass das Reduzieren von Spam und unerwünschten E-Mails unverhältnismäßig viel Zeit in Anspruch nimmt.
- **35 %** der IT-Teams nennen die Verwaltung von E-Mail-Signaturen als eine der zwei zeitaufwendigsten Aufgaben – ein Indikator dafür, wie manuell und ineffizient Governance in vielen Unternehmen noch ist.
- Nur **41 %** haben E-Mail in ihre Sicherheits- und Compliance-Systeme integriert – trotz des hohen operativen Aufwands.

4. Professionalität und Compliance stehen auf dem Spiel

- **92 %** der Führungskräfte sind sich einig: Konsistente, zentral verwaltete E-Mail-Signaturen stärken Vertrauen und Professionalität.
- Trotzdem setzen **80 %** weiterhin auf manuelle Methoden oder Nutzer-Selbstverwaltung – was Konsistenz, Compliance und Kontrolle gefährdet.

Zusammenfassung

5. KI und Automatisierung sind unverzichtbar geworden

- **43 %** der IT-Leader glauben, dass KI-gesteuerte E-Mail-Automatisierung die geschäftliche Kommunikation in den nächsten fünf Jahren prägen wird.
- Ihre Prioritäten: bessere Sicherheit (41 %), erweiterter Schutz vor Spam und Phishing (38 %), mehr Automatisierung (38 %), einfacheres Management (37 %) und bessere Integrationen (36 %) – ein klares Signal für intelligentere, skalierbare E-Mail-Infrastrukturen.

Dieser Report zeigt, wo E-Mail heute steht, wohin sie sich entwickelt und welche nächsten Schritte für IT-Verantwortliche entscheidend sind. Denn wenn es um professionelle, vertrauenswürdige Kommunikation geht, bleibt E-Mail das Mittel der Wahl.

”

„E-Mail betrifft jedes Team, jeden Kunden und jeden wichtigen Meilenstein Ihres Unternehmens. Dieser Trendreport zeigt, warum es an der Zeit ist, E-Mail nicht länger nur als Hintergrundinfrastruktur zu sehen – sondern als das operative System, das sie tatsächlich ist.“

— Vicky Wills, Chief Technology Officer, Exclaimer

Dieser Trendreport basiert auf einer unabhängigen Studie, die Exclaimer in Zusammenarbeit mit Censuswide in Auftrag gegeben hat. Ziel war es, zu verstehen, wie IT-Führungskräfte die Entwicklung der geschäftlichen E-Mail-Kommunikation steuern – von Infrastruktur und Governance bis hin zu Sicherheit, Integration und Automatisierung.

Die Untersuchung wurde als quantitative Querschnittsbefragung durchgeführt und durch qualitative Einschätzungen interner Fachexpertinnen und -experten ergänzt. Die Datenerhebung erfolgte online zwischen dem 4. und 16. April 2025.

Befragt wurden 4.009 IT-Fachkräfte in vier Kernmärkten:

Vereinigtes Königreich (1.003)
Vereinigte Staaten (1.000)
Deutschland (1.006)
Australien (1.000)

Die Teilnehmenden wurden im Rahmen eines nicht-probabilistischen Stichprobenverfahrens ausgewählt. Ziel war es, Personen mit aktiver Verantwortung für E-Mail-Systeme, Kommunikationsrichtlinien oder Sicherheits- und Compliance-Infrastrukturen anzusprechen. Zur Gewährleistung einer ausgewogenen Stichprobe wurden Quoten festgelegt für:

Unternehmensgröße: Kleinstunternehmen (1–100 Mitarbeitende), Kleinunternehmen (101–250), mittelständische Unternehmen (251–500), oberes Mid-Market-Segment (501–1.000) Großunternehmen (1.001–5.000), Enterprise-Unternehmen (ab 5.001)

Branchen: Technologie, Finanzdienstleistungen, Gesundheitswesen, Fertigung, Bauwesen, Bildung, Gastgewerbe, Rechtswesen, Medien, Einzelhandel/E-Commerce, öffentlicher Sektor, professionelle Dienstleistungen, gemeinnützige Organisationen und weitere

Rollen: IT-Manager, IT-Direktoren, CIOs, CTOs, Administratoren sowie Verantwortliche für Sicherheit und Compliance

Mail-Plattformen: Microsoft 365 (Office 365), Microsoft Exchange und Google Workspace (Gmail for Business)

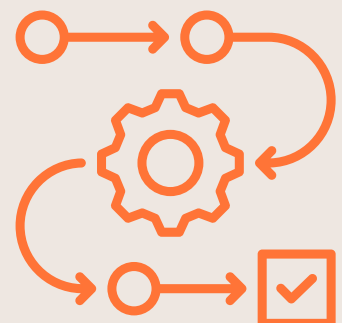
Methodik

Die Umfrage bestand aus strukturierten Multiple-Choice-Fragen mit Fokus auf fünf Themenbereiche:

- | |
|--|
| 1. Kommunikationswerkzeuge und Nutzungsmuster |
| 2. E-Mail-Sicherheit, Risikopotenziale und Compliance |
| 3. Signaturverwaltung und operative Governance |
| 4. Integration in den Tech-Stack und Workflow-Automatisierung |
| 5. Zukünftige Trends: KI, Personalisierung und strategische E-Mail-Nutzung |

Die Ergebnisse wurden mithilfe gängiger beschreibender Analysemethoden ausgewertet. Die quantitativen Daten bildeten die Grundlage der Erkenntnisse, wurden jedoch durch qualitative Einschätzungen der Fachexpertinnen und -experten von Exclaimer ergänzt.

Die Studie wurde gemäß den ESOMAR-Richtlinien durchgeführt. Alle Teilnehmenden haben einer informierten Teilnahme zugestimmt. Auch wenn die Umfrage ein fundiertes Stimmungsbild der IT-Landschaft im Jahr 2025 liefert, spiegeln die Ergebnisse eine Momentaufnahme wider und sollten im jeweiligen Kontext interpretiert werden.



Die Rolle der E-Mail im modernen Kommunikations-Stack

Im Jahr 2025 verwalten IT-Verantwortliche eine vielfältigere Kommunikationslandschaft als je zuvor – von Instant Messaging und Videokonferenzen bis hin zu Kollaborationsplattformen. Doch trotz wachsender Verbreitung ersetzen diese Tools die E-Mail nicht. Sie ergänzen sie. Wenn Kommunikation formell, konsistent und teamübergreifend nachvollziehbar sein muss, bleibt E-Mail der Standard.

In diesem Kapitel geht es darum, warum E-Mail nach wie vor das Fundament der geschäftlichen Kommunikation bildet – selbst in Zeiten neuer, dynamischer Werkzeuge. Es zeigt, wie IT-Führungskräfte einen sich wandelnden Kommunikations-Stack ausbalancieren: Sie unterstützen moderne Plattformen und verlassen sich gleichzeitig auf E-Mail, um Abläufe zu koordinieren und klare Kommunikation sicherzustellen.

Trotz wachsender Nutzung von Messaging- und Kollaborationstools bleibt E-Mail der wichtigste Kanal für geschäftskritische Kommunikation.

89 % der IT-Führungskräfte halten direkte 1:1-E-Mails für wichtig in ihrem Unternehmen.

In Deutschland und Australien liegt dieser Wert sogar bei **94 %**, gefolgt von **86 %** in den USA und **81 %** im Vereinigten Königreich. Auch in zentralen Branchen wie professionelle Dienstleistungen, Technologie und Finanzwesen übersteigt die Bedeutung die **90 %**-Marke. Nahezu die Hälfte aller Befragten (**48 %**) stuft E-Mail als „sehr wichtig“ ein.”

Trotz der Verbreitung von Messaging-Apps bleibt E-Mail der vertrauenswürdige Standard für professionelle Kommunikation. **48 %** der Befragten geben an, dass mehr als die Hälfte ihrer internen und externen Kommunikation über direkte E-Mails erfolgt – ein deutliches Zeichen für die zentrale Rolle der E-Mail im Tagesgeschäft.

Hier geht es nicht nur um persönliche Vorlieben – sondern um den konkreten Zweck. E-Mail ist das bevorzugte Medium für sichtbare, geschäftskritische Kommunikation, bei der Compliance, Konsistenz und Nachvollziehbarkeit nicht verhandelbar sind:

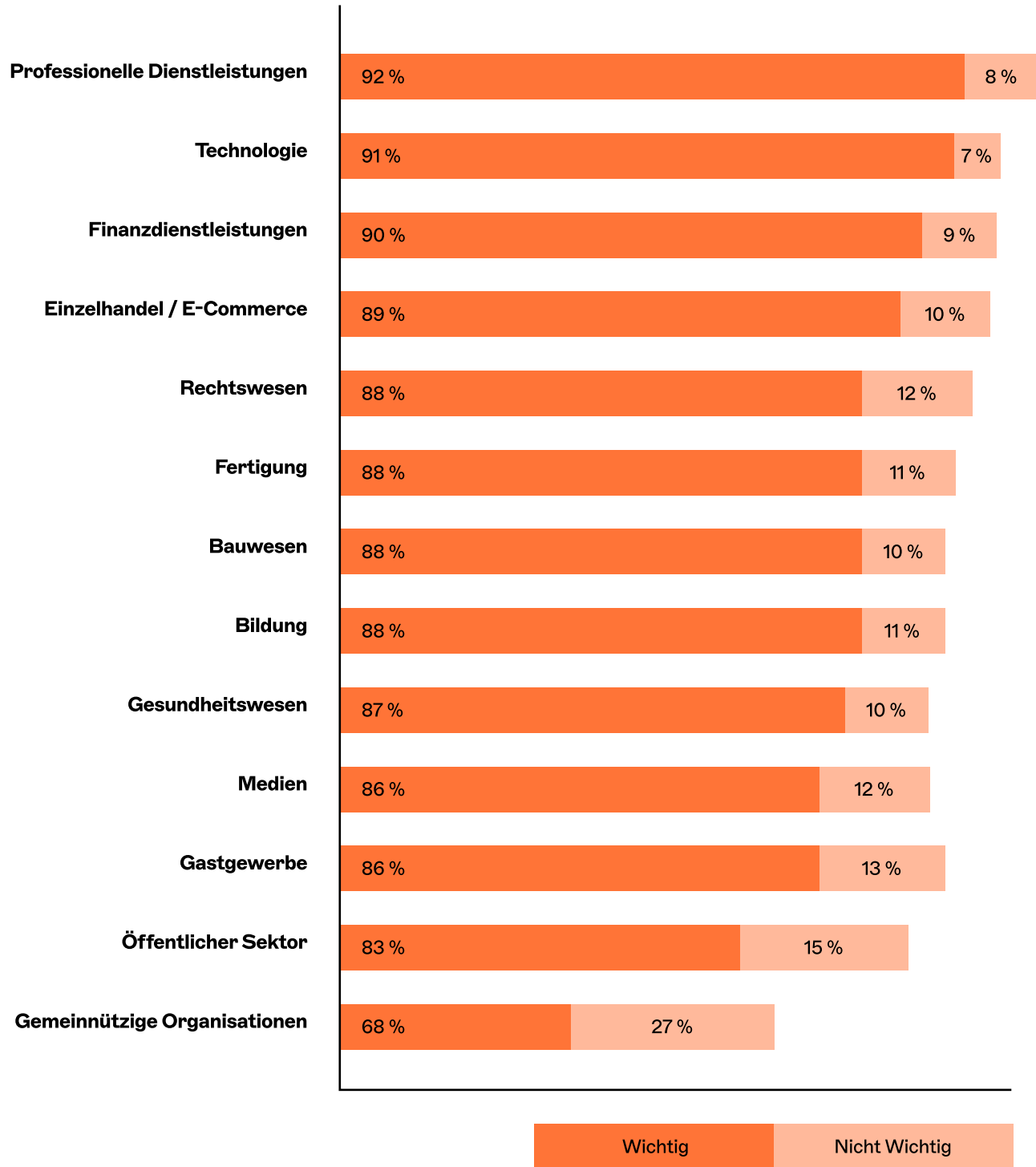
49 % nutzen E-Mail für IT- und Sicherheitsbenachrichtigungen.

36 % setzen E-Mail für interne Zusammenarbeit ein.

34 % verlassen sich bei der Kundenkommunikation auf E-Mail.

Solche Nachrichten erfordern eine klare Dokumentation, garantierte Zustellung und ein einheitliches Format. Genau darin liegt die Stärke der E-Mail – und die Schwäche von Chat-Apps.

Die Bedeutung von E-Mails nach Branche



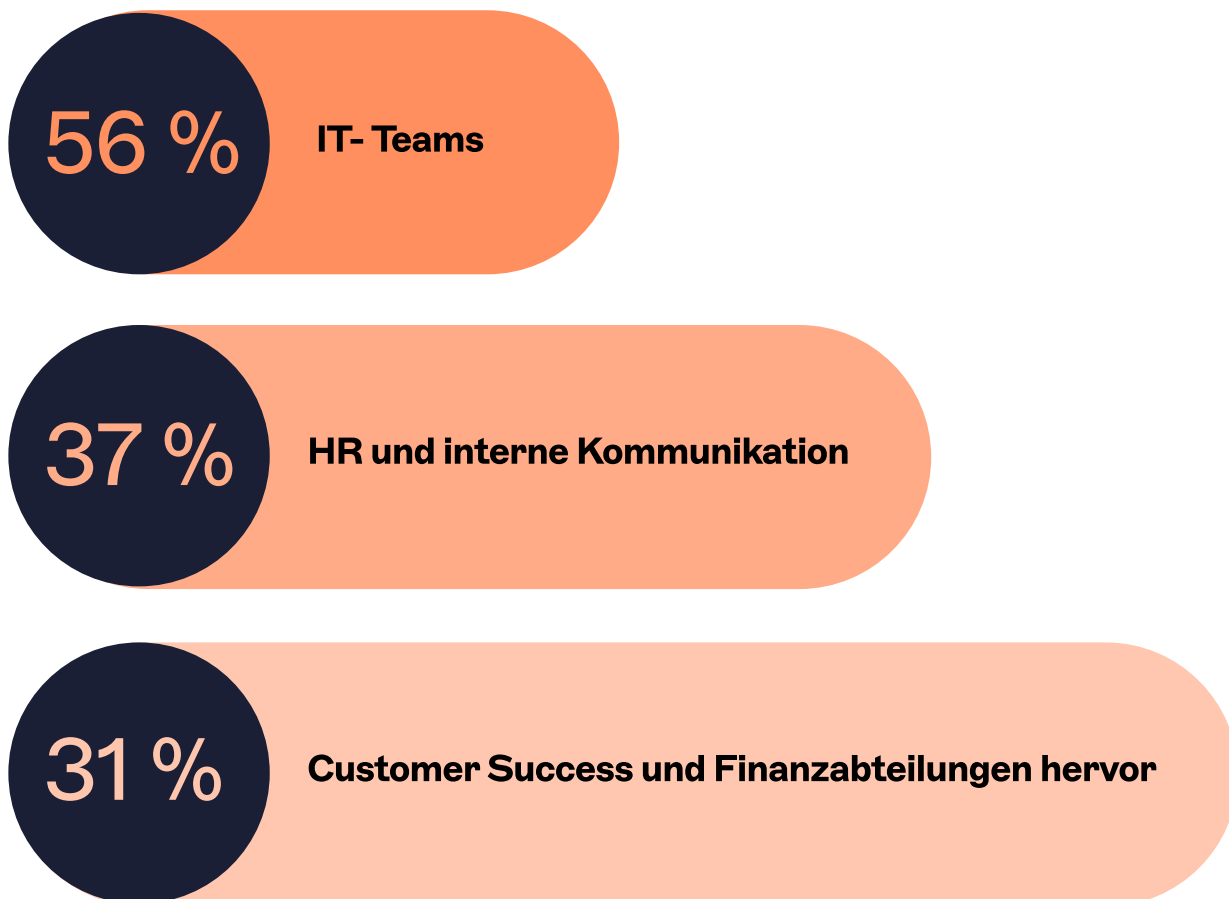
Nicht Wichtig:

Wenn es wichtig oder offiziell ist, wird es per E-Mail versendet.

Die Bedeutung der E-Mail steigt zudem mit der Komplexität. Selbst in großen Unternehmen, in denen asynchrone Tools weit verbreitet sind, bleibt das E-Mail-Volumen hoch: **49 %** der IT-Leader in Unternehmen mit über 5.001 Mitarbeitenden geben an, dass typische Nutzer täglich mehr als 16 E-Mails versenden – ein deutliches Zeichen für die zentrale Rolle der E-Mail in funktionsübergreifenden, volumenstarken Arbeitsabläufen.

Auch auf Abteilungsebene zeigt sich die Bedeutung der E-Mail deutlich. Besonders stark nutzen sie jene Teams, die für Infrastruktur, Mitarbeitende und Servicebereitstellung verantwortlich sind:

Teams, die sich am stärksten auf E-Mails verlassen



Mit der zunehmenden Vielfalt digitaler Tools behält E-Mail eine besondere Stellung: Sie funktioniert rollenübergreifend, skaliert mit wachsender Komplexität und bietet die Klarheit und Nachvollziehbarkeit, die anderen Plattformen oft fehlen.

Tool-Nutzung: Vergleich zwischen E-Mail, Kollaborationstools und Instant Messaging

Basierend auf den Antworten zur Frage: **“Welcher Prozentsatz der internen und externen Kommunikation Ihres Unternehmens erfolgt über ...”**

Nutzungsstufe	Direkte E-Mail	Kollaborations- und IM-Tools
Hohe Nutzung (51–100 %)	48 %	43 %
Mittlere Nutzung (31–50 %)	40 %	39 %
Geringe Nutzung (≤30 %)	11 %	17 %

Erkenntnis:

Unternehmen setzen häufiger stark auf direkte E-Mail-Kommunikation als auf moderne Kollaborations- oder Messaging-Plattformen:

Beinahe die Hälfte der Befragten (**48 %**) nutzt E-Mail für mehr als die Hälfte aller Kommunikationsvorgänge – gegenüber **43 %**, die auf Tools wie Slack, Teams oder Asana zurückgreifen..



Wenn Kommunikation sensibel, strategisch oder risikobehaftet ist, bleibt E-Mail der Kanal, dem Unternehmen vertrauen.



Was das für IT bedeutet

Messaging-Tools entwickeln sich weiter – aber sie ersetzen die E-Mail nicht, sondern verändern ihren Stellenwert. Für IT-Verantwortliche ist E-Mail kein Altsystem, das man nur noch mitlaufen lässt – sondern ein zentraler Bestandteil der Infrastruktur, der modernisiert werden muss. Denn wenn Kommunikation wirklich zählt, übernimmt E-Mail nach wie vor die Schlüsselrolle.

Instant-Messaging-Tools sind für dynamische Teams unverzichtbar geworden. Für schnelle Abstimmungen, kurze Statusmeldungen oder spontane Updates bieten Plattformen wie Slack, Microsoft Teams und Google Chat die nötige Geschwindigkeit. Doch trotz wachsender Nutzung ersetzen IM-Tools die E-Mail nicht – sie ergänzen sie.

E-Mail vs. Instant Messaging: Wofür sich die jeweiligen Kanäle am besten eignen

E-Mail: Nachvollziehbarkeit, Sicherheitsmeldungen, Kundenkommunikation, interne Richtlinienkommunikation

Instant Messaging: Geschwindigkeit, schnelle Koordination, informelle Updates, projektbezogene Zusammenarbeit

IT-Verantwortliche sehen den Mehrwert beider Kanäle. Tatsächlich geben 89 % an, dass direkte 1:1-E-Mails für ihr Unternehmen wichtig sind – genauso viele sagen das auch über Instant Messaging. Doch beim Blick auf die tatsächliche Nutzung wird der Unterschied deutlich:

48 %

der Unternehmen nutzen E-Mail für mehr als die Hälfte ihrer internen und externen Kommunikation

43 %

sagen dasselbe über **Instant Messaging-** und **Kollaborationsplattformen**

17 %

verwenden Instant Messaging nur selten (≤ 30 % der **Kommunikation**) – bei E-Mail sind es lediglich 11 %

Auch wenn beide Kanäle als geschäftskritisch gelten, übernimmt E-Mail weiterhin den größeren Anteil – sie spielt teamübergreifend eine konstantere und tragendere Rolle.

Instant Messaging punktet dort, wo Geschwindigkeit wichtiger ist als Struktur – etwa bei Projektabstimmungen, Support-Triage oder standortübergreifenden Daily-Standups. Doch wenn eine Nachricht dokumentiert, weitergeleitet oder Compliance-konform sein muss, landet sie am Ende doch im Posteingang.

Selbst in großen Unternehmen, in denen IM-Tools zunehmend eingesetzt werden, verliert E-Mail nicht an Bedeutung. Bei Organisationen mit über 5.000 Mitarbeitenden zeigt sich:

85 % der IT-Führungskräfte sagen, dass Instant Messaging wichtiger ist als E-Mail

Dennoch halten **78 %** E-Mail für geschäftskritisch

Teammitglieder versenden im Schnitt **16 E-Mails pro Tag**

Instant Messaging ersetzt E-Mail nicht – es entwickelt sich parallel weiter. Plattformen wie Slack, Teams und Google Chat wandeln sich von Nebenkanälen zu operativen Hubs. Doch E-Mail bleibt das führende System für nachvollziehbare Kommunikation.

Das Vertrauen in Instant Messaging ist groß – unabhängig von der Plattform:

90 %

der Microsoft
365-Nutzer halten
IM für wichtig

89 %

der Google
Workspace-Nutzer
stimmen dem zu

86 %

der Microsoft
Exchange-Nutzer
ebenso

Das zeigt ein plattformunabhängiges Vertrauen in IM als zentrales Kommunikationsmittel. Doch es geht nicht darum, einen Favoriten zu küren. E-Mail übernimmt die Kommunikation mit Gewicht. IM liefert die Geschwindigkeit. Für IT-Verantwortliche liegt die eigentliche Aufgabe darin, beides bereitzustellen – sicher, reibungslos und skalierbar.

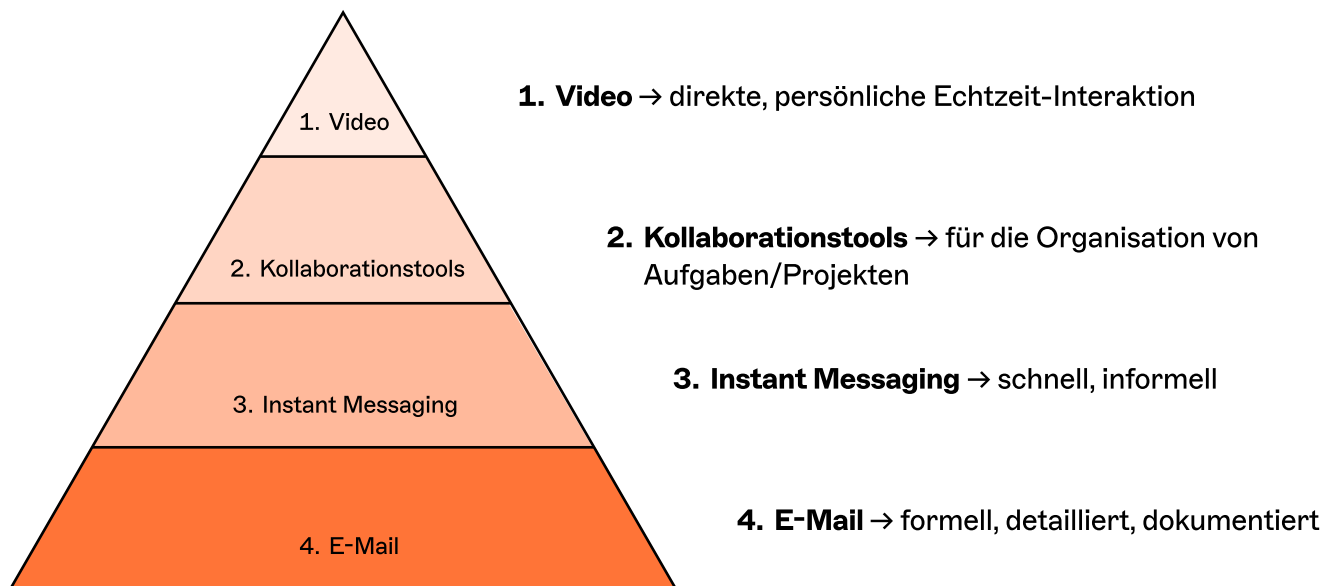
Schnelligkeit findet im Chatfenster statt. Aber Verantwortung bleibt im Posteingang.

Warum das für IT relevant ist

E-Mail und Instant Messaging erfüllen heute unterschiedliche, sich ergänzende Aufgaben. Für IT-Verantwortliche geht es nicht darum, sich für eines zu entscheiden – sondern darum, sicherzustellen, dass beide Lösungen reibungslos und sicher zusammenarbeiten. Denn wenn Teams zwischen Schnelligkeit und Nachvollziehbarkeit wechseln, muss die Kommunikation weiterhin konsistent, überprüfbar und geschützt bleiben.



Neben E-Mail und Instant Messaging nutzen Unternehmen heute ein breiteres Set an Werkzeugen: Videokonferenzen, Kollaborationsplattformen und externe Messaging-Tools. Diese Kanäle sind essenziell für modernes, dezentrales Arbeiten. Aber sie bilden nicht die Basis. Sie unterstützen Workflows – sie definieren sie nicht.



Moderne Unternehmen setzen zunehmend auf einen wachsenden Kommunikations-Stack. Weltweit sagen **89 %** der IT-Führungskräfte, dass Videokonferenzen eine wichtige Rolle in ihren digitalen Abläufen spielen – in der Technologiebranche, wo Remote- und Hybrid-Teams zum Alltag gehören, liegt dieser Wert sogar bei **94 %**. Auch Kollaborationstools wie Asana, Monday.com oder Notion werden hoch bewertet: **86 %** der Führungskräfte halten sie für unverzichtbar – besonders in Regionen wie Deutschland und Australien sowie in größeren mittelständischen Unternehmen.

Doch „wichtig“ bedeutet nicht automatisch „weit verbreitet“. Diese Tools sind nicht in jedem Team oder Anwendungsfall fest verankert:

- **15 %** der Kleinstunternehmen (1–100 Mitarbeitende) halten Videokonferenzen nicht für wichtig
- Selbst in Großunternehmen (5.001+ Mitarbeitende) sagen **14 %** dasselbe
- Im Vereinigten Königreich stufen nur **79 %** der Befragten Kollaborationstools als wichtig ein – bei gemeinnützigen Organisationen sinkt dieser Wert sogar auf **60 %**
- Fast ein Drittel der Nonprofit-Teilnehmenden (**31 %**) bezeichnet Kollaborationsplattformen als unwichtig

Diese Lücken sprechen für sich. Tools wie Videokonferenzen oder Projektmanagement-Plattformen erfüllen reale, praktische Anforderungen – doch oft nur im spezifischen Kontext. Sie funktionieren besonders gut in klar definierten Workflows, bei regelmäßigen Team-Routinen oder in Remote-Umgebungen. Sie sind nicht universell – und sie sind nicht der Standard. **E-Mail ist es.**

Unabhängig von Region, Unternehmensgröße oder Branche bleibt E-Mail die Konstante – teamübergreifend, zeitzoneunabhängig und plattformübergreifend. Sie bietet das, was andere Tools nicht liefern: Sichtbarkeit, Nachvollziehbarkeit und Konsistenz. Und sie braucht dafür keinen Kalendereintrag, kein gemeinsames Board und keine Freigabe – sie funktioniert einfach.

Was das für IT bedeutet

Video- und Kollaborationstools sind wertvoll – aber ihr Nutzen ist kontextabhängig. **E-Mail hingegen ist Infrastruktur.**

Für IT-Führungskräfte bedeutet das: Der Fokus sollte darauf liegen, neue Tools rund um die E-Mail zu integrieren – nicht sie zu ersetzen. Denn wenn Aufgaben im Chat untergehen oder Videocalls nicht dokumentiert werden, ist es das Postfach, das alles wieder zusammenführt.

Der Kommunikations-Stack mag wachsen. Aber **E-Mail hält ihn zusammen.**

E-Mail bleibt das Rückgrat der geschäftlichen Kommunikation – doch IT-Abteilungen müssen einen zunehmend komplexen, mehrkanaligen Stack unterstützen, der neue Anforderungen und Risiken mit sich bringt. Hier sind die wichtigsten Erkenntnisse darüber, was die Geschäftskommunikation im Jahr 2025 prägt:

E-Mail bleibt das Fundament der Unternehmenskommunikation.

Trotz einer wachsenden Tool-Landschaft ist E-Mail nach wie vor der am weitesten verbreitete und am stärksten genutzte Kanal für sichtbare, nachvollziehbare Kommunikation.

Instant Messaging ist unverzichtbar – aber nicht führend.

Tools wie Slack und Microsoft Teams sind wichtig für schnelle, kollaborative Zusammenarbeit in Echtzeit. Aber sie decken andere Anforderungen ab und haben E-Mail in den meisten Workflows nicht ersetzt.

Video- und Kollaborationstools schließen funktionale Lücken.

Plattformen wie Zoom, Asana oder Trello unterstützen verteiltes Arbeiten und teambasierte Koordination – doch Nutzung und Relevanz variieren stark je nach Branche und Unternehmensgröße.

Tool-Nutzung ist kontextabhängig.

Die Bedeutung einzelner Kommunikationskanäle hängt von Organisationsstruktur, Teamfunktion und regionaler Reife ab – Integration statt Standardisierung ist daher der Schlüssel.

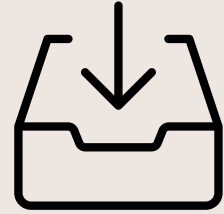
IT muss ein Multi-Tool-Umfeld orchestrieren.

Es geht nicht darum, ein einziges Tool zu wählen – sondern darum, den gesamten Stack sicher, effizient und skalierbar zusammenzuführen.

Posteingang unter Beschuss: Wie sich das Risikoprofil der E-Mail verändert

E-Mail ist nach wie vor einer der am häufigsten angegriffenen Einstiegspunkte im Unternehmen – und gleichzeitig einer der am meisten unterschätzten. Zwar haben die meisten IT-Teams in Schutzmaßnahmen investiert, doch der Posteingang ist weiterhin für einen erheblichen Anteil an Sicherheitsvorfällen verantwortlich. Grundlegende Schutzmaßnahmen wie DMARC, DKIM und SPF werden nach wie vor nur unzureichend eingesetzt. Das Ergebnis: eine Angriffsfläche, die aktiv bleibt und uneinheitlich abgesichert ist.

Die Folgen dieser Sicherheitslücken nehmen zu. Mit durchschnittlichen Kosten von 4,88 Millionen US-Dollar pro Datenschutzverletzung im Jahr 2024 – dem höchsten jemals gemessenen Wert – ist das E-Mail-Risiko längst nicht mehr hypothetisch. Da sich Bedrohungen je nach Region, Branche und Unternehmensgröße unterscheiden, reichen Richtlinien allein nicht mehr aus. IT-Verantwortliche brauchen mehrstufige, kontextbewusste Schutzmechanismen – Systeme, die nicht nur schützen, sondern diesen Schutz auch nachweisen können.



”

„Sicherheits- und Compliance-Anforderungen enden nicht beim Posteingang. Und doch bleibt E-Mail einer der am stärksten angegriffenen, exponiertesten und am wenigsten gesteuerten Bereiche der IT-Infrastruktur. Diese Erkenntnis sollte IT-Führungskräften helfen, die nächste Generation von Kontrollmaßnahmen richtig zu priorisieren.“

— Karl Bagci, Head of Information Security, Exclaimer

Trotz jahrelanger Investitionen in die E-Mail-Sicherheit bleibt der Posteingang ein zentrales Einfallstor für Angriffe – und wird von vielen IT-Verantwortlichen weiterhin unterschätzt.

83 % der Unternehmen haben mindestens einen sicherheitsrelevanten Vorfall im Zusammenhang mit E-Mail erlebt – fast die Hälfte davon allein im vergangenen Jahr.

Diese Vorfälle konzentrieren sich nicht auf bestimmte Regionen oder Branchen – sie treten überall auf. Das zeigt: E-Mail-Bedrohungen nehmen nicht ab. Sie nehmen zu.

Noch kritischer: E-Mail ist nicht nur ein Teil der allgemeinen Bedrohungslage – sie gehört zu den aktivsten und unbeständigsten Angriffsflächen. **Mehr als 53 %** der Unternehmen geben an, dass E-Mail für **zwischen einem Viertel und der Mehrheit** ihrer gesamten Sicherheitsvorfälle verantwortlich ist. Das ist keine Nebenrolle – das ist **direkte Frontlinieneinwirkung**.

Zu den am häufigsten genannten Herausforderungen aus Sicht der IT-Verantwortlichen gehören:

44 % Externe Bedrohungen wie Phishing, Spoofing und Spam

42 % End-to-End-Verschlüsselung und Sicherheitslücken in E-Mail-Workflows

40 % Der Spagat zwischen Schutz und Benutzerfreundlichkeit, insbesondere in hybriden Umgebungen

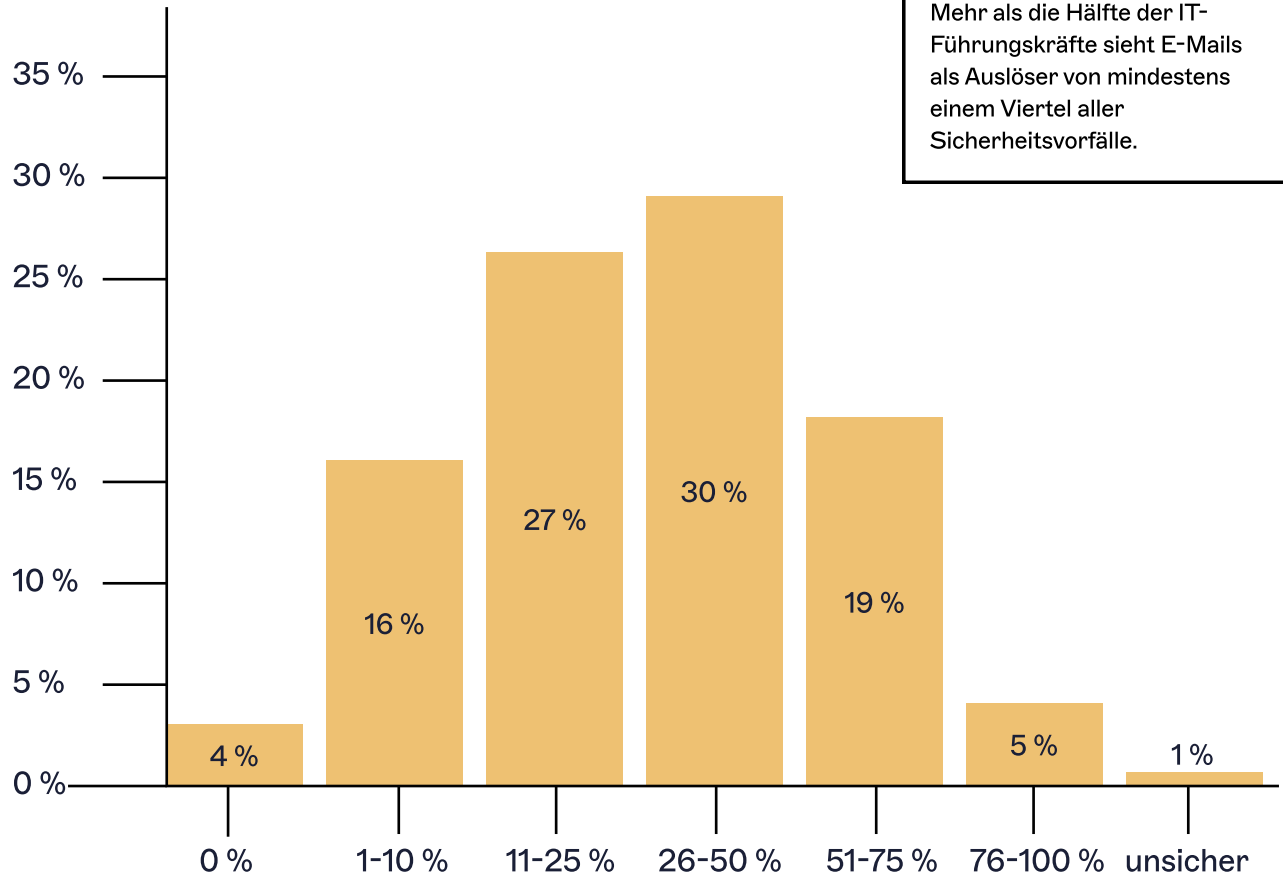
Trotz dieser Bedrohungslage sind grundlegende Schutzmaßnahmen oft lückenhaft:

Nur **33 %** der Unternehmen geben an, zentrale Sicherheitsprotokolle wie **DMARC, DKIM** oder **SPF** implementiert zu haben – Technologien, die gezielt vor Identitätsmissbrauch und Spoofing schützen sollen. Das zeigt eine wachsende Diskrepanz: Die Bedrohungen nehmen zu, aber viele Umgebungen arbeiten weiterhin mit veralteten oder unvollständigen Schutzmechanismen. Das ist nicht nur ein technisches Defizit – es ist ein strategisches.

Solange E-Mail ein unzureichend geschützter Kanal bleibt, werden Angreifer ihn weiterhin ausnutzen – nicht nur über externe Bedrohungen, sondern auch durch interne Fehler, fehlgeleitete Nachrichten und blinde Flecken in der Compliance.

Die Rolle von E-Mails bei Sicherheitsvorfällen – laut IT-Führungskräften

% der IT-Führungskräfte, die diesen Bereich angeben



Anteil der E-Mail-bedingten Vorfälle

Quelle: Exclaimer Umfrage unter 4.009 IT-Führungskräften

Was IT jetzt tun muss

Der Posteingang darf nicht länger als Nebenfunktion betrachtet werden – sondern als Risikobereich mit hoher Priorität. Dafür braucht es mehrschichtige Schutzmaßnahmen: Protokolle wie DMARC, aber auch kontinuierliche Schulungen, automatisierte Richtliniendurchsetzung und plattformweite Transparenz. E-Mail-Systeme verdienen denselben Fokus und dieselbe Widerstandsfähigkeit, die IT-Abteilungen auch auf Netzwerksicherheit oder Identitätsmanagement legen. Das Risikoprofil lässt keinen anderen Schluss zu.

IT-Verantwortliche sind sich einig: E-Mail stellt ein erhebliches Sicherheitsrisiko dar – doch **die Art dieses Risikos variiert deutlich**, je nachdem, wo ein Unternehmen tätig ist und in welchem Umfeld es operiert.

Weltweit sagen **76 %** der IT-Leader, dass bis zur Hälfte ihrer Sicherheitsvorfälle mit E-Mails zusammenhängt. Im Durchschnitt schätzen sie, dass E-Mails für **33 %** aller Vorfälle verantwortlich sind. Dieser Wert steigt im Vereinigten Königreich auf **36 %** und fällt in Australien auf **29 %**. Ein Unterschied von sieben Prozentpunkten mag gering erscheinen – doch er zeigt, wie regionale Vorschriften, Cloud-Adoptionsraten und lokale Bedrohungsakteure das Risikoprofil entscheidend prägen.

"Was sind aktuell die größten E-Mail-Sicherheitsherausforderungen für IT-Teams?" So haben IT-Führungskräfte in den USA, UK, Australien und Deutschland geantwortet.

UK:

43 % Abwehr externer E-Mail-Bedrohungen (z. B. Phishing, Spoofing, Spam)

38 % Sicherstellung von E-Mail-Verschlüsselung und Sicherheit

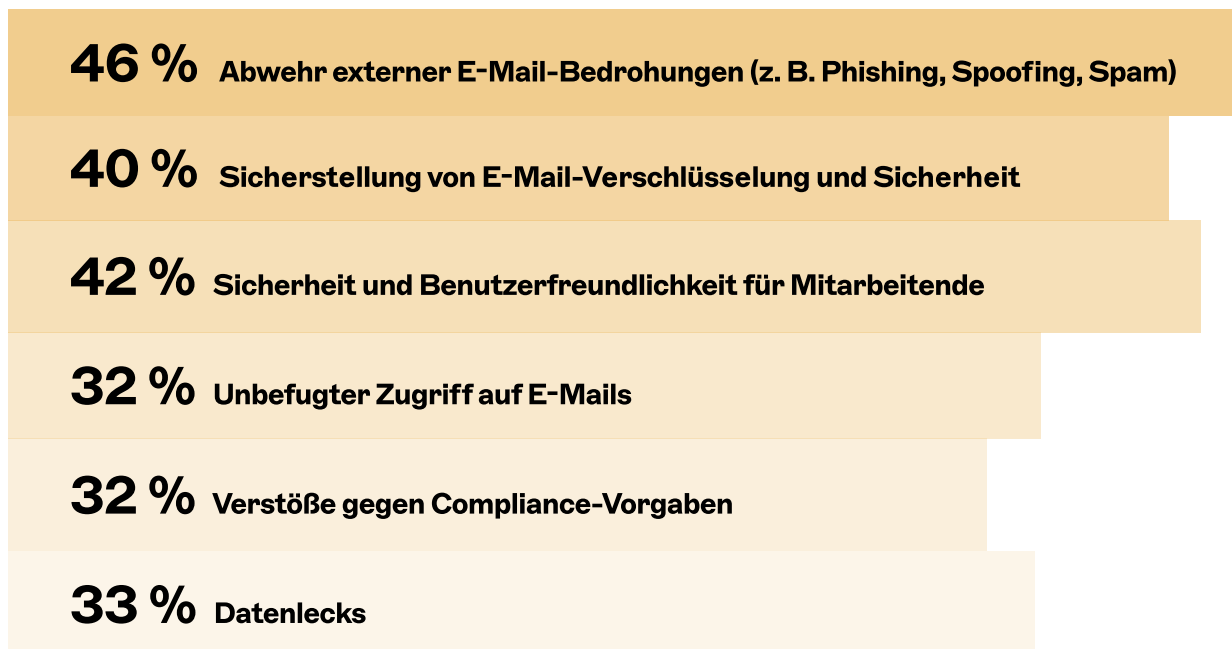
37 % Sicherheit und Benutzerfreundlichkeit für Mitarbeitende

33 % Unbefugter Zugriff auf E-Mails

29 % Verstöße gegen Compliance-Vorgaben

28 % Datenlecks

US:



AUS:



DE:

42 % Abwehr externer E-Mail-Bedrohungen (z. B. Phishing, Spoofing, Spam)

42 % Sicherstellung von E-Mail-Verschlüsselung und Sicherheit

36 % Sicherheit und Benutzerfreundlichkeit für Mitarbeitende

32 % Unbefugter Zugriff auf E-Mails

32 % Verstöße gegen Compliance-Vorgaben

25 % Datenlecks



Anteil der sicherheitsrelevanten Vorfälle, die mit E-Mails in Zusammenhang stehen – nach Branche

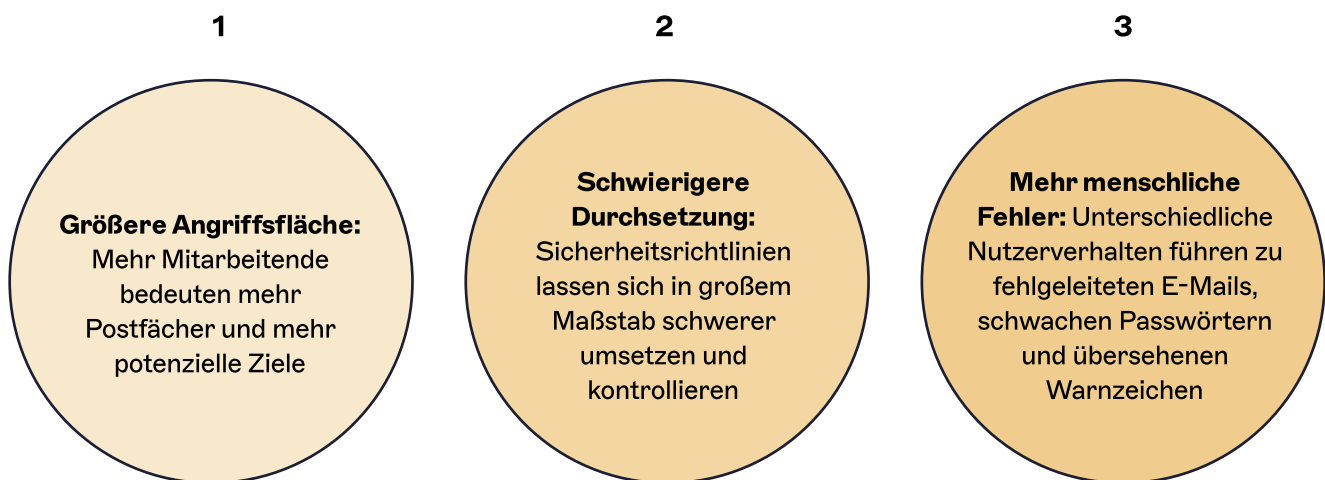
Bauwesen	→	35%
Bildung	→	40%
Finanzdienstleistungen	→	32%
Öffentlicher Sektor	→	41%
Gastgewerbe	→	38%
Gesundheitswesen	→	35%
Rechtswesen	→	34%
Fertigung	→	32%
Medien	→	30%
Gemeinnützige Organisationen	→	42%
Professionelle Dienstleistungen	→	33%
Einzelhandel / E-Commerce	→	26%
Technologie	→	29%

Branchenspezifisch zeigen sich noch deutlichere Unterschiede bei den E-Mail-bezogenen Herausforderungen.

- In den Bereichen **Medien & Unterhaltung (55 %)** sowie **Fertigung (51 %)** stehen **Phishing, Spoofing und Spam** ganz oben auf der Liste der größten Probleme.
- Im **Finanzsektor** ergibt sich ein anderes Bild: Hier rangieren **Verschlüsselung (42 %)** und **Benutzerfreundlichkeit (42 %)** gleichauf mit **Phishing (41 %)** – ein Hinweis auf den doppelten Druck, sensible Daten zu schützen, ohne den täglichen Betrieb zu behindern.
- **Non-Profit-Organisationen** heben sich deutlich ab: Nur **31 %** nennen Phishing und Spoofing als zentrale Herausforderung. Das könnte auf Unterschiede in der Sicherheitsreife, Personalstärke oder auch auf eine andere Wahrnehmung der Bedrohungslage hinweisen.

Dann ist da noch die Unternehmensgröße: In **Großunternehmen mit über 5.001 Mitarbeitenden** sehen **49 %** der IT-Verantwortlichen **Phishing und Spoofing** als größte Herausforderung. Zum Vergleich: In **mittelständischen Firmen (101–250 Mitarbeitende)** sind es **42 %**, in **Kleinstunternehmen (1–100 Mitarbeitende)** nur **41 %**.

Größere Organisationen stehen vor drei spezifischen Herausforderungen:



Das Ergebnis: Eine fragmentierte Risikolandschaft, in der ein One-Size-Fits-All-Sicherheitsmodell nicht mehr ausreicht.

Was das für IT bedeutet

Bedrohungsabwehr funktioniert nicht nach dem Gießkannenprinzip. IT-Teams müssen die spezifischen Risiken identifizieren, die für ihre Branche, Unternehmensgröße und Region am relevantesten sind und Schutzmaßnahmen entsprechend ausrichten.

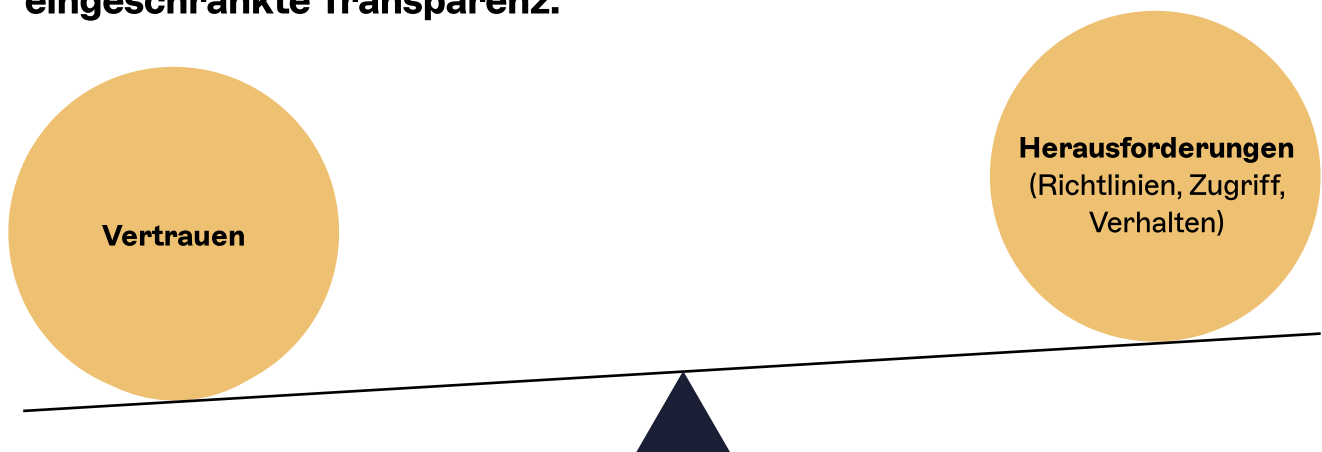
Das kann bedeuten, in großen Unternehmen stärker in **erweiterte Anti-Phishing-Tools** zu investieren – oder in Branchen wie dem **Finanz- oder Bildungswesen** den Fokus auf **Verschlüsselung** zu legen.

Breiter Schutz ist gut.

Gezielte Umsetzung ist besser.

Die meisten IT- und Geschäftsverantwortlichen geben an, dass sie sich gut aufgestellt fühlen, um regulatorische Anforderungen zu erfüllen – doch hinter diesem Vertrauen verbirgt sich eine andere Realität:

Ressourcenengpässe, komplexe Systemlandschaften und eingeschränkte Transparenz.



93 % der Befragten sagen, sie seien zuversichtlich oder sehr zuversichtlich in Bezug auf ihre Compliance-Strategie gegenüber Standards wie **DSGVO, HIPAA, SOC2** und **ISO 27001**. Aber dieses Vertrauen ist stark geprägt von äußeren Rahmenbedingungen und internen Herausforderungen, die selten offen diskutiert werden.

Einige Branchen zeigen ein überdurchschnittlich hohes Vertrauen in ihre Compliance-Fähigkeiten:

56 % Bauwesen

53 % Bildungswesen

51 % Technologiebranche

Andere hinken hinterher:

- **Non-Profit-Organisationen** und das **Gastgewerbe** kämpfen mit **hoher Personalfuktuation**, **knappen Budgets** und **veralteter Infrastruktur** – Faktoren, die die Durchsetzung von Richtlinien deutlich erschweren.
- In der **Fertigung** kommt eine zusätzliche Herausforderung hinzu: Hier muss Compliance in **physische Systeme** mit **komplexen Datenströmen** integriert werden – eine technisch und operativ anspruchsvolle Aufgabe.

Auch **geografische Unterschiede** spielen eine Rolle: IT-Verantwortliche in den **USA** zeigen das größte Vertrauen (**54 %**). Im **Vereinigten Königreich (48 %)**, in **Deutschland (43 %)** und **Australien (42 %)** liegt dieser Wert etwas niedriger – vermutlich aufgrund **strengerer nationaler Datenschutzgesetze**.

Bemerkenswert ist: **Die Wahl der E-Mail-Plattform hat kaum Einfluss auf das Sicherheitsgefühl**. Egal ob **Google Workspace**, **Microsoft 365** oder **Exchange** – die Vertrauenswerte sind nahezu identisch.

Trotzdem zeigen sich die Belastungen im Tagesgeschäft. Die größten Herausforderungen beim Compliance-Management sind:

46 % Durchsetzung von Richtlinien zur Datenaufbewahrung

45 % Verhinderung unbefugten Zugriffs

44 % Verwaltung des E-Mail-Verhaltens und der Nutzung durch Mitarbeitende

43 % Schritt halten mit sich ändernden gesetzlichen Vorgaben

Diese Herausforderungen **verstärken sich in Großunternehmen**, wo Systemlandschaften unübersichtlich werden und die Kontrolle über das Nutzerverhalten schwieriger ist. **Fast die Hälfte** der Führungskräfte in Unternehmen mit über **5.000 Mitarbeitenden** nennt das Verhalten der Nutzer als größte Sorge.

Vertrauen ohne Transparenz reicht nicht aus. Aufsichtsbehörden – und interne Stakeholder – erwarten Dokumentation, Nachvollziehbarkeit und konsequente Durchsetzung. Genau hier beginnt die eigentliche Arbeit.

Was IT jetzt tun muss

Compliance darf kein Lippenbekenntnis bleiben – sie muss systematisch verankert sein. Das bedeutet: Richtlinien automatisiert durchsetzen, Audit-Trails erfassen und manuelle Kontrollmechanismen reduzieren.

Vertrauen allein genügt nicht. IT-Verantwortliche müssen sicherstellen, dass E-Mail-Compliance **nachweisbar, systemgesteuert** und **jederzeit überprüfbar** ist.

E-Mail gehört zu den aktivsten – und gleichzeitig exponiertesten – Risikoflächen moderner Unternehmen. Sie verlangt mehr als passives Monitoring oder Vertrauen in Richtlinien. IT-Führungskräfte müssen E-Mail gezielt steuern, systematisch absichern und Compliance unter Druck nachweisen können. Das sind die wichtigsten Punkte:

Mail-Bedrohungen sind häufig – und werden oft unterschätzt.

Mehr als die Hälfte der Unternehmen gibt an, dass E-Mail für zwischen einem Viertel und der Mehrheit ihrer Sicherheitsvorfälle verantwortlich ist. Trotzdem fehlen vielen grundlegende Schutzmechanismen wie DMARC, DKIM oder SPF.

Kontext ist entscheidend.

Risikowahrnehmung und Bedrohungstypen unterscheiden sich je nach Region, Branche und Unternehmensgröße. Was in der Finanzbranche oder im verarbeitenden Gewerbe kritisch ist, hat im Bildungswesen oder bei Non-Profits möglicherweise andere Priorität. Sicherheitsstrategien müssen diese Unterschiede abbilden.

Große Unternehmen stehen vor komplexen Herausforderungen.

Mehr Postfächer, mehr Endgeräte, mehr Verhaltensvariabilität – das macht Unternehmen besonders anfällig für Phishing, fehlgeleitete E-Mails und unklare Richtlinienumsetzung.

Compliance-Vertrauen ist kein Garant für Kontrolle.

Zwar berichten die meisten Führungskräfte von einem hohen Vertrauen in ihre Compliance-Fähigkeit – doch die Durchsetzung erfolgt oft noch manuell, und Transparenzlücken bleiben bestehen, insbesondere beim Nutzerverhalten und der Datenaufbewahrung.

Nachweisbare Bereitschaft ist der neue Standard.

Vertrauen reicht nicht mehr aus. IT-Teams brauchen Systeme, die Richtlinien automatisieren, Standards durchsetzen und auditfähige Nachweise liefern. Denn wenn es zum Vorfall kommt, schützt nicht das Sicherheitsgefühl, sondern der dokumentierte Nachweis.

E-Mail-Verwaltung im großen Maßstab: Integration, Effizienz und Beschaffungsverhalten

E-Mail bleibt ein zentraler Bestandteil moderner Arbeitsabläufe – doch in vielen Unternehmen arbeitet sie noch immer isoliert vom Rest der IT-Infrastruktur. Während IT-Teams zunehmend Verantwortung für Sicherheit, Compliance und digitale Transformation übernehmen, muss sich E-Mail von einem reinen Kommunikationskanal zu einem integrierten Bestandteil des Enterprise-Tech-Stacks weiterentwickeln.

Gleichzeitig wächst die Kluft zwischen dem, was IT-Teams wirklich brauchen – Automatisierung, Interoperabilität, Effizienz – und dem, was bestehende E-Mail-Systeme tatsächlich leisten. In vielen Fällen bleibt das E-Mail-Management manuell, fragmentiert und nur begrenzt skalierbar.

Und während IT-Führungskräfte zunehmend strategische Verantwortung für eingesetzte Technologien übernehmen, verändert sich auch der Beschaffungsprozess für E-Mail-Lösungen: Weg von einfachen Funktionsvergleichen – hin zu langfristigem Architekturdenken.

In diesem Kapitel geht es darum,

- **wie veraltete Workflows Zeit kosten,**
- **wie Integrationslücken den Fortschritt behindern**
- **und warum E-Mail-Kaufentscheidungen heute eine neue strategische Tiefe erfordern.**

IT-Verantwortliche wissen genau, wo die Zeitfresser liegen – Spamfilterung, Compliance-Prüfungen, Signatur-Updates – doch diese Aufgaben werden oft noch manuell erledigt. Das Ergebnis: eine wachsende Belastung für ohnehin ausgelastete IT-Teams.

Weltweit nennen IT-Führungskräfte die größten zeitraubenden Faktoren rund um E-Mail:

37 % Reduzierung von Spam und unerwünschten E-Mails

35 % Sicherstellung von Sicherheit und Compliance

35 % Verwaltung und Aktualisierung von E-Mail-Signaturen

34 % Archivierung und Speicherverwaltung

31 % Integration von E-Mail mit anderen Tools

Diese Herausforderungen steigen mit zunehmender Komplexität: In Unternehmen mit mehr als 5.000 Mitarbeitenden sagen **43 %**, dass allein Spam einen erheblichen IT-Aufwand verursacht.

Doch bei der Automatisierung zeigt sich eine deutliche Lücke:

- Nur **29 %** haben E-Mail-Workflows mit Tools wie **Zapier** oder **Power Automate** automatisiert
- Nur **41 %** haben E-Mail in ihre **Sicherheits- und Compliance-Tools** integriert

Das ist ein kritisches Missverhältnis. Fast die Hälfte der IT-Leader wünscht sich mehr **Automatisierung und Integration** im E-Mail-Ökosystem – aber **nur wenige haben das bereits umgesetzt**.

Die Tools existieren. Was fehlt, sind **Fokus und Umsetzung**. Statt in Automatisierung zu investieren, kämpfen sich viele Teams durch alltägliche Aufgaben und lassen dabei wertvolle Zeit, Ressourcen und strategisches Potenzial ungenutzt.

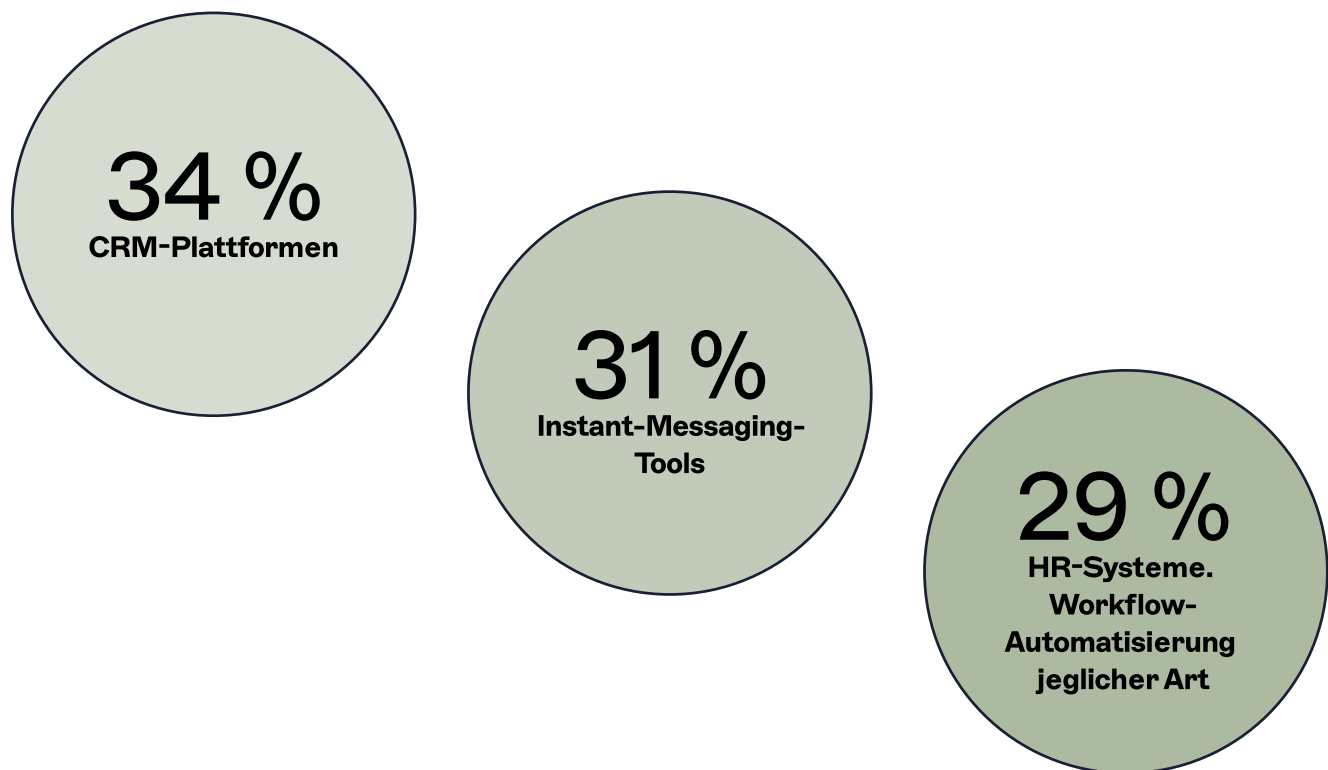
Was das für IT bedeutet

E-Mail-Management muss als System gedacht werden – nicht als Abfolge lästiger Einzelaufgaben. Ob Spamfilter, Compliance-Durchsetzung oder Signaturpflege: Diese Prozesse sind **wiederholbar und regelbasiert** – also ideal für Automatisierung geeignet. Wer in diesen Bereichen auf **Automatisierung setzt**, kann Prozesse vereinfachen, Reibungsverluste reduzieren und IT-Ressourcen freisetzen – für Projekte mit größerem strategischen Mehrwert.



E-Mail funktioniert nicht isoliert – doch in vielen Unternehmen wird sie immer noch genau so behandelt. Während Fachabteilungen neue Plattformen und Workflows einführen, bleibt E-Mail oft **vom Rest des Tech-Stacks abgekoppelt**.

Weniger als die Hälfte der IT-Verantwortlichen (**41 %**) gibt an, dass E-Mail in ihre **Sicherheits- und Compliance-Systeme** integriert ist.
Andere Integrationen liegen noch niedriger:



Und das, obwohl **48 %** der IT-Leader sagen, dass **Integration und Automatisierung** den größten Nutzen für ihre E-Mail-Systeme bringen würden.
Wenn E-Mail isoliert läuft, leiden ganze Teams:

- **Marketing** muss Signaturen manuell aktualisieren
- **HR** muss Mitarbeiteränderungen in getrennten Systemen nachverfolgen
- **Legal & Compliance** verlieren die Übersicht über wichtige Audit-Daten
- Und die **IT** wird zum Feuerwehrteam, statt proaktiv zu gestalten

Mit welchen Business-Anwendungen integriert Ihr Unternehmen E-Mails direkt?

41 % IT-Sicherheits- und Compliance-Lösungen

34 % CRM-Systeme (z. B. Salesforce, HubSpot usw.)

31 % Instant-Messaging-Tools (z. B. Slack, Microsoft Teams usw.)

31 % Kollaborationstools (z. B. Asana, Trello, Monday.com)

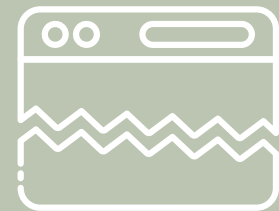
29 % HR- und Onboarding-Systeme (z. B. Workday, Bob usw.)

29 % Workflow-Automatisierungstools (z. B. Zapier, Power Automate usw.)

28 % Marketing-Automatisierungstools (z. B. Marketo, Pardot usw.)

28 % Terminbuchungstools (z. B. Calendly, MS Bookings, Chili Piper usw.)

Fehlende Integration verlangsamt nicht nur Prozesse – sie schafft Lücken in Transparenz, Durchsetzung und Verantwortlichkeit. Lücken, die Angreifer ausnutzen und Auditoren hinterfragen können.



Was das für IT bedeutet

E-Mail muss fester Bestandteil der Unternehmensarchitektur sein – nicht ein losgelöster Einzelkanal. Das bedeutet: Integration mit zentralen Systemen wie **CRM, HR, Messaging-Plattformen** und **Sicherheitstools**. **Enge Integration** verbessert die Governance, reduziert Redundanzen und stärkt die operative Widerstandsfähigkeit.

Das Ziel ist nicht, E-Mail neu zu erfinden – sondern sie besser zu machen. Indem sie **mit allem anderen zusammenarbeitet**.

Die Verantwortung für die Auswahl von E-Mail-Technologien liegt weiterhin bei der IT – doch **die Auswahlkriterien haben sich verändert**. Heute geht es weniger um **Anbieter-Reputation** oder **Funktionslisten**, sondern darum, **wie gut sich Lösungen in einen integrierten Tech-Stack einfügen**.

Die wichtigsten Entscheidungsfaktoren beim Kauf von E-Mail-Technologien sind:

42 % Sicherheits- und Compliance-Funktionen

40 % Ease of integration

38 % Automatisierung und KI-Mehrwert

37 % Skalierbarkeit und Flexibilität

Traditionelle Kriterien wie **Kosten (33 %)** und **Anbieter-Ruf (32 %)** verlieren an Bedeutung – besonders in Großunternehmen, **wo fast die Hälfte (47 %) Sicherheit** an erste Stelle setzt.

Doch der Beschaffungsprozess ist nicht reibungslos. Hürden, die IT-Teams bei Investitionen in neue Technologien ausbremsen, sind unter anderem:

43 % Bedenken bei Sicherheit und Compliance

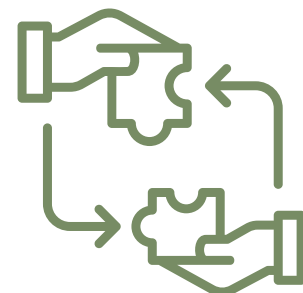
41 % Komplexität von Migration und Implementierung

41 % Verzögerungen durch interne Freigaben und Prozesse

Diese Hindernisse verlangsamten den Fortschritt – und erschweren es der IT, ihre **Transformationsziele** umzusetzen, selbst wenn der Nutzen offensichtlich ist

Warum das für IT relevant ist

E-Mail-Beschaffung sollte wie Infrastrukturplanung behandelt werden. Jedes Tool muss zur übergeordneten **Architektur- und Sicherheitsstrategie** des Unternehmens passen – nicht nur ein isoliertes Problem lösen. Die Rolle der IT verändert sich: Vom **Administrator** zum **strategischen Berater** – jemand, der Entscheidungen mitgestaltet, Integrationen bewertet und sicherstellt, dass jede Lösung ins Gesamtbild passt. Es geht nicht nur darum, Tools freizugeben. Es geht darum, **sie so zu orchestrieren**, dass sie **Skalierbarkeit, Sicherheit** und **langfristigen Nutzen** gemeinsam unterstützen.



Die Lücke zwischen IT-Prioritäten und dem, was tatsächlich optimiert wurde, wird größer.

Automatisierung, Integration und strategischer Einkauf sind die entscheidenden Hebel, um Effizienz zu steigern und echten Mehrwert zu liefern. Darauf kommt es jetzt an:

Automatisierung ist überfällig.

IT-Teams verbringen weiterhin zu viel Zeit mit wiederholbaren Aufgaben wie Spamfilterung, Compliance-Durchsetzung und Signaturpflege. Automatisierung ist kein Luxus – sie ist der nächste logische Schritt.

Integration ist kein Nice-to-have.

In den meisten Unternehmen läuft E-Mail noch immer isoliert. Ohne enge Anbindung an Systeme wie CRM, HR und Instant Messaging bleibt die IT damit beschäftigt, fragmentierte Workflows manuell zu verbinden.

Die IT verantwortet weiterhin den Einkauf – aber Strategie schlägt Preis.

Sicherheit, Integration und Skalierbarkeit sind heute entscheidender als Markenimage oder Budget. Beschaffung dreht sich nicht mehr um Features, sondern um architektonische Passgenauigkeit.

Erfolg braucht Orchestrierung.

Von der Priorisierung von Automatisierungen bis zur Abstimmung mit Fachbereichen: IT-Leader müssen sicherstellen, dass jedes Tool zur Unternehmensstrategie passt und den Stack stärkt – nicht zusätzlich verkompliziert.

E-Mail-Signaturen für Professionalität, Konsistenz und Kontrolle

E-Mail ist nicht nur ein Kommunikationsmittel – sie ist auch ein Träger der Marke.

Jede Nachricht, die Mitarbeitende versenden, spiegelt das Unternehmen wider: seine Standards, seine Konsistenz, seine Glaubwürdigkeit. Doch in den meisten Organisationen werden Signaturen noch immer stiefmütterlich behandelt: dezentral verwaltet, manuell aktualisiert und voller Inkonsistenzen.

Für IT-Verantwortliche ist das kein kosmetisches Problem, sondern ein Integrationsproblem. Signaturen befinden sich im Schnittpunkt von Infrastruktur, Governance und Professionalität – und trotzdem fehlt ihnen oft ein passendes System.

Ohne Anbindung an den Tech-Stack verursachen sie Tickets, schaffen Risiken und binden IT-Ressourcen, die anderswo dringend gebraucht werden.

Dieses Kapitel zeigt,

- **warum Signaturverwaltung noch immer im Reaktionsmodus steckt,**
- **wie fragmentierte Zuständigkeiten den Betrieb verlangsamen**
- **und wie die IT den Wandel anführen kann – durch Automatisierung, Standardisierung und Integration der Signatursteuerung in alltägliche Workflows**

IT-Verantwortliche sehen den Wert professioneller, konsistenter E-Mail-Signaturen klar: **92 %** sagen, dass **gut verwaltete Signaturen Vertrauen und Glaubwürdigkeit schaffen**. Doch der Alltag zeigt ein anderes Bild – eines voller **veralteter Prozesse, geteilter Zuständigkeiten und ständiger Formatierungsanfragen**, die IT-Ressourcen binden.

Das Kernproblem ist die Zuständigkeit: Wenn niemand die Verantwortung trägt, herrscht Chaos.

Nur **55 %** der Unternehmen geben an, dass die **IT** die Signaturverwaltung übernimmt

Der Rest verteilt die Verantwortung auf **HR (16 %)**, **Marketing (14 %)** und sogar auf **einzelne Mitarbeitende (14 %)**

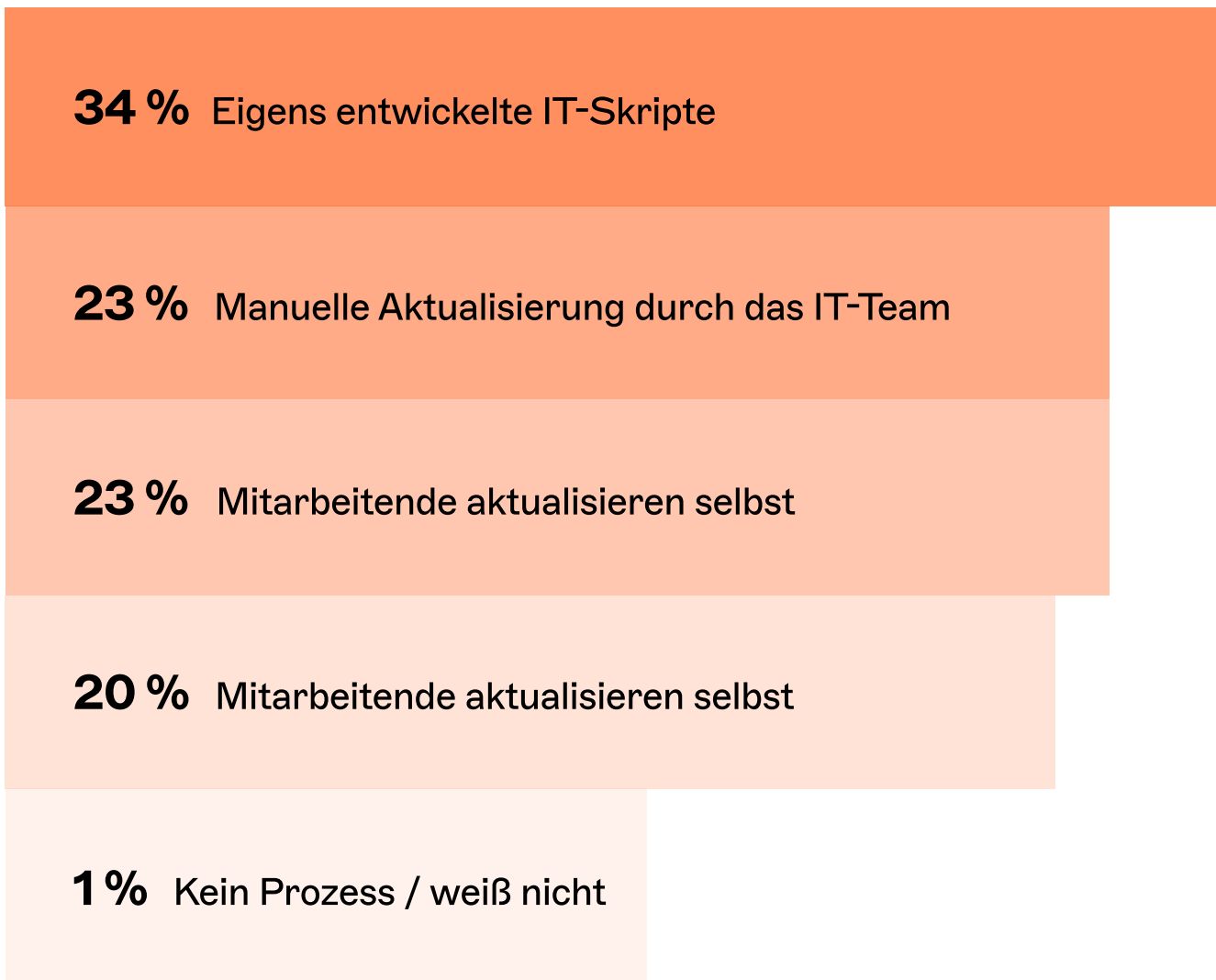
In Großunternehmen sinkt die IT-Verantwortung auf **47 %**, im öffentlichen Sektor sogar auf **34 %**

Die Art der Verwaltung spiegelt diese Fragmentierung wider. **80 %** der Unternehmen arbeiten mit **provisorischen oder manuellen Lösungen**:

- **34 %** nutzen selbst entwickelte IT-Skripte
- **23 %** aktualisieren Signaturen manuell
- **23 %** überlassen die Signaturpflege den Mitarbeitenden

Frage / Titel über dem Chart:

Wie werden E-Mail-Signaturen verwaltet?



Diese Vorgehensweisen führen zu häufigen Problemen:

- **33 %** Mitarbeitende ignorieren die Signaturreichtlinien
- **32 %** Formatierungen variieren je nach Endgerät und E-Mail-Client
- **31 %** Fehlende zentrale Steuerung und Transparenz

Trotzdem nutzen nur 20 % der Unternehmen eine dedizierte Lösung zur Signaturverwaltung.

Größte Herausforderungen bei der Verwaltung von E-Mail-Signaturen

33 % Mitarbeitende halten sich nicht an Signaturreichtlinien

32 % Uneinheitliche Formatierung (je nach Gerät und E-Mail-Client)

31 % Keine zentrale Steuerung

31 % Keine Nutzungsmöglichkeiten für Marketing und Engagement

31 % Langsamer Aktualisierungsprozess

28 % Schwache Markenführung (Brand Governance)

24 % Keine Einblicke in die Performance

3 % Keine größeren Herausforderungen

Für die IT bedeutet das: **wiederkehrende Unterbrechungen, steigende Supportaufkommen** und eine wachsende Lücke zwischen den Tools, die sie verwalten, und den professionellen Standards, die sie gewährleisten sollen.

Was IT jetzt tun muss

Um Reibungsverluste zu vermeiden und die Kontrolle zurückzugewinnen, muss **Signaturverwaltung in die Infrastrukturebene integriert werden**. Das bedeutet: **Konsistenz durch Automatisierung erzwingen – nicht durch manuelle Freigaben** – und gleichzeitig den Fachbereichen **gesteuerten Zugriff auf die Inhalte ermöglichen**. Das Ziel ist **nicht Mikromanagement**, sondern ein **skalierbares System**, das professionelle Standards sichert – **ohne zur zusätzlichen Supportlast für die IT zu werden**.



Obwohl E-Mail-Signaturen zu den **sichtbarsten Elementen externer Kommunikation** gehören, werden sie selten als Teil der **strategischen IT-Planung** behandelt. Aktualisierungen erfolgen meist erst **nachdem etwas schief läuft** – etwa bei einem Strukturwechsel, einem Sicherheitsaudit oder auf Druck anderer Abteilungen.

Die Folge: **manuelle, überhastete und oft nur temporäre Lösungen.**

Die häufigsten Auslöser für Signatur-Updates sind:

38 % Phasen starken Wachstums

38 % Sicherheits- und Compliance-Audits

36 % Umstrukturierungen im Unternehmen

31 % Fusionen und Übernahmen

30 % Interner Frust über inkonsistente Darstellung

27 % Rebranding-Prozesse

Solche reaktiven Anpassungen landen fast immer bei der **IT**, auch wenn die Inhalte aus anderen Bereichen stammen. Und weil die vorhandenen Systeme **nicht auf Skalierbarkeit ausgelegt** sind, wird eine eigentlich einfache Änderung schnell zur **mehrtägigen Aufgabe**: Vorlagen zusammensuchen, Code anpassen, Formatierungsfehler beheben, Support-Tickets beantworten.

Das kostet nicht nur Zeit – es schafft auch Risiken. Inkonsistente Signaturen können zu **veralteten Informationen, fehlenden rechtlichen Hinweisen** oder einem **unprofessionellen Außenauftritt** führen – gerade in entscheidenden Kommunikationssituationen.

Für die IT ist das ein weiteres Beispiel dafür, wie unverwaltete Infrastruktur fälschlicherweise als Designproblem wahrgenommen wird.

Was IT jetzt tun sollte

Statt auf Audits oder Rebrandings zu warten, um unter Zeitdruck Korrekturen vorzunehmen, sollte die IT eine **Lösung zur zentralen Signaturverwaltung** einführen, die **Kontrolle und Konsistenz** gewährleistet. Mit **zentral durchgesetzten Richtlinien** und **automatisierten Updates** können Fachbereiche Inhalte innerhalb klar definierter Vorgaben selbst pflegen – während die IT sicherstellt, dass **Konsistenz und Compliance** eingehalten werden. So werden E-Mail-Signaturen **von einer wiederkehrenden Störung zu einem geregelten Bestandteil des Betriebs** – und die IT gewinnt Zeit und Kapazitäten für Aufgaben mit höherem strategischen Wert.



E-Mail-Signaturen gehören zu den sichtbarsten – und zugleich am stärksten vernachlässigten – Bestandteilen der Geschäftskommunikation. Für die IT bieten sie eine klare Chance, reaktive Supportarbeit durch strategisches Systemdesign zu ersetzen. Das sind die wichtigsten Punkte:

Zuständigkeiten sind fragmentiert.

Die Signaturverwaltung liegt bei unterschiedlichen Teams, was zu Inkonsistenz führt und zusätzlichen Supportaufwand für die IT bedeutet.

Anpassungen erfolgen reaktiv.

Signaturänderungen werden meist durch Ereignisse statt durch Prozesse ausgelöst – das macht Aktualisierungen aufwendiger und langsamer als nötig.

Manuelle Methoden dominieren.

Viele Organisationen arbeiten noch mit Skripten, manuellen Anpassungen oder überlassen die Verantwortung den Mitarbeitenden, was zu unnötigem Overhead führt.

Die IT kann den Wandel steuern.

Mit zentraler Kontrolle, Automatisierung und Integration in bestehende Workflows kann die IT Konsistenz steigern, Supportanfragen reduzieren und E-Mail-Signaturen von einem Formatierungsthema zu einem strategischen Infrastrukturbaustein entwickeln.

Die Zukunft der geschäftlichen E-Mail

E-Mail verschwindet nicht – sie entwickelt sich weiter. Während KI, Automatisierung und Messaging-Tools die Kommunikation verändern, bleibt E-Mail die Basis für formelle, vertrauenswürdige und geschäftskritische Interaktionen. Für IT-Verantwortliche geht es nicht darum, ein Altsystem zu verteidigen, sondern darum, einen Kanal zu modernisieren, der nach wie vor zentrale Unternehmenswerte transportiert.

Die heutige E-Mail-Landschaft zeichnet sich nicht nur durch ihre Beständigkeit aus, sondern auch durch ihre wachsende Komplexität: Bedrohungen werden raffinierter, Erwartungen steigen, und die Systeme, die E-Mail unterstützen – von Gateways bis KI – müssen mehr leisten, in kürzerer Zeit. In diesem Kapitel geht es darum, wohin sich die geschäftliche E-Mail entwickelt – und wie IT diesen Wandel mitgestalten kann: durch Investitionen in Sicherheit, den Einsatz von KI und den Aufbau integrierter, flexibler Workflows.

Trotz aller Diskussionen über **KI, Automatisierung** und **User Experience** dominiert ein Thema übergreifend über **Rollen, Regionen** und **Branchen** hinweg: **E-Mail-Sicherheit**. Sie ist keine Nebensache – sie ist **das Fundament**, auf dem alles andere aufbaut. Während **Bedrohungen zunehmen** und **regulatorische Anforderungen steigen**, sehen IT-Verantwortliche **Sicherheit und Verschlüsselung** als den entscheidenden Faktor für die Zukunft der E-Mail.

Unabhängig von Plattform, Region oder Unternehmensgröße steht Sicherheit an erster Stelle:

47 % der IT-Leader sagen, dass **Sicherheits- und Verschlüsselungstechnologien** die geschäftliche E-Mail in den nächsten fünf Jahren maßgeblich prägen werden

Im Technologiesektor setzen **53 %** künftige Investitionen gezielt auf E-Mail-Sicherheit

51 % der Hauptentscheider sehen **Verschlüsselung** als strategische Top-Priorität

38 % wünschen sich **besseren Phishing- und Spamschutz** direkt in ihren Systemen

In den Branchen **Recht (47 %)**, **Fertigung (49 %)** und **Medien (52 %)** steht Sicherheit über allen anderen Innovationsfeldern

KI- und Kollaborationsfunktionen gewinnen an Bedeutung, doch sie verdrängen nicht die Grundlagen: E-Mail transportiert weiterhin **Verträge, Zugangsdaten, Systemwarnungen und regulatorisch relevante Inhalte**. Und mit jeder neuen Schnittstelle, jedem weiteren Endgerät und jedem zusätzlichen Drittanbieter **steigt das Risiko von Sicherheitslücken**.

Was das für IT bedeutet

E-Mail-Sicherheit ist keine Zukunftsaufgabe – sie ist eine aktuelle Notwendigkeit.

IT-Teams sollten Lösungen priorisieren, die:

- **mehrschichtigen Schutz** bieten,
- **Compliance-Richtlinien automatisiert durchsetzen**,
- und sich **über Regionen und Geschäftsbereiche hinweg skalieren** lassen.

Von **verschlüsselter Zustellung** und **Domain-Authentifizierung** bis zu

Echtzeitüberwachung und **Audit-Trails**: Die nächste Generation von E-Mail-Infrastruktur wird nicht durch ihr Design definiert – sondern durch die Frage, **wie effektiv sie das Unternehmen schützt**.

Künstliche Intelligenz im E-Mail-Kontext hat den Status des Experiments hinter sich gelassen. Was früher als Zukunftstechnologie galt, ist heute ein Standard, den moderne IT-Verantwortliche fest integriert statt nachträglich hinzugefügt erwarten.

Unabhängig von Branche, Region oder Unternehmensgröße gilt: **KI wird nicht mehr als optionales Upgrade gesehen, sondern als zentrale Komponente**, um steigende Anforderungen in den Bereichen **Automatisierung, Effizienz** und **Risikofrüherkennung** zu erfüllen.

43 % der IT-Leader nennen **KI-gesteuerte E-Mail-Automatisierung** als einen der drei wichtigsten Trends für die Zukunft der geschäftlichen E-Mail. Dieser Wert ist in Branchen mit **besonders komplexem oder sensiblen E-Mail-Management** noch höher – ein klarer Hinweis auf den Paradigmenwechsel: **KI steht nicht für Komfort, sondern für Kapazität.**

Wer denkt schon einen Schritt weiter?

52 % der Unternehmen im Technologiesektor sagen, dass **KI die Zukunft der E-Mail prägen wird**

49 % der Großunternehmen (5.001+ Mitarbeitende) erwarten **mehr KI und Automatisierung** in ihrem E-Mail-Stack

43 % der Hauptentscheider führen **KI-Automatisierung** unter ihren strategischen Top-Prioritäten

45 % im Rechtswesen und **44 %** im verarbeitenden Gewerbe sehen KI als **entscheidenden Treiber**

Das geht weit über intelligente Antworten oder **Betreffzeilenvorschläge** hinaus:

IT-Leader erwarten von KI, dass sie **Zustellung optimiert, Prioritäten erkennt, Bedrohungen identifiziert und Routineprozesse reduziert. E-Mail soll nicht nur Schritt halten – sondern vorausdenken.**

Was IT beachten sollte

KI sollte nach ihrem praktischen Nutzen bewertet werden – nicht nach Funktionslisten. Das Ziel ist klar: **Overhead reduzieren, Genauigkeit steigern und Probleme erkennen, bevor sie eskalieren.**

IT-Teams sollten Plattformen wählen, die KI gezielt einsetzen – zum Beispiel für:

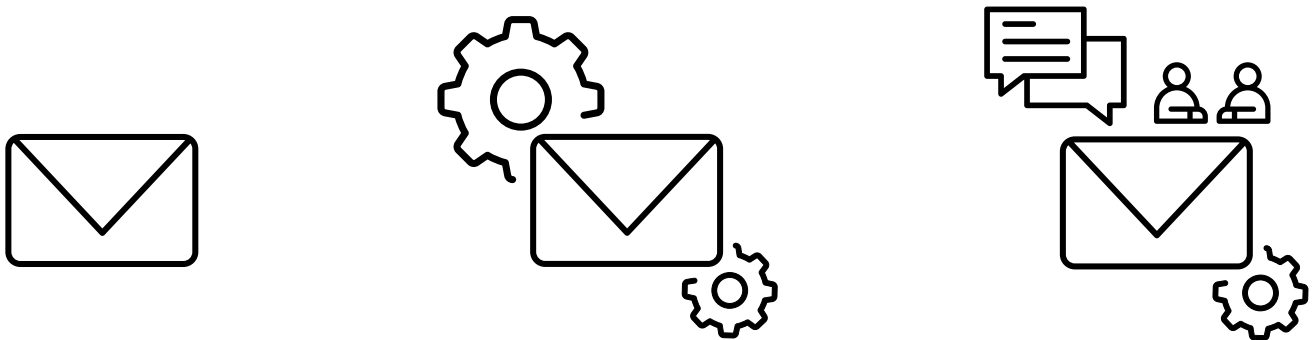
- **Echtzeit-Routing,**
- **intelligente Filterung,**
- **Verhaltensanalysen,**
- und die **Automatisierung von Routineaufgaben mit geringem Mehrwert.**

Die Zukunftsfrage lautet nicht, ob E-Mail KI nutzt – sondern wie gut. Und es ist die Aufgabe der IT, dafür zu sorgen, dass sie **effektiv liefert.**



Messaging-Plattformen gewinnen an Bedeutung, doch E-Mail bleibt unverzichtbar – besonders für **externe, formelle und auditierbare** Kommunikation. Statt ersetzt zu werden, wird E-Mail als Teil eines **verzahnten Kommunikations-Ökosystems neu positioniert**.

E-Mail entwickelt sich weiter



90 % der IT-Verantwortlichen sagen, dass E-Mail bis **2030** ein **zentrales Geschäftstool** bleiben wird – auch wenn Echtzeit-Messaging an Popularität gewinnt. Es geht nicht um „entweder/oder“, sondern um **Integration und klare Rollendefinition**.

Ein hybrides Modell entsteht:

- **E-Mail** für formelle, dokumentierte und Compliance-relevante Kommunikation
- **Messaging** für schnelle interne Zusammenarbeit und Feedback in Echtzeit

Diese Integration ist bereits im Gange:

42 % der IT-Leader erwarten eine engere **Verzahnung** von E-Mail und Kollaborationstools

41 % sehen **Personalisierung** als prägenden Faktor für die zukünftige E-Mail-Nutzung

34 % wünschen sich mehr **Individualisierung und Modularität** im E-Mail-Umfeld

E-Mail ist nicht statisch. Sie passt sich an, um neuen Erwartungen gerecht zu werden, ohne die **Professionalität** und **Nachvollziehbarkeit** zu verlieren, die sie unverzichtbar machen.

Was das für IT bedeutet

Die IT muss einen Kommunikations-Stack unterstützen, in dem **E-Mail, Chat und Kollaborationstools nahtlos zusammenarbeiten.** Das bedeutet: **Lösungen bereitstellen**, die sich übergreifend in Workflows integrieren lassen, **an Nutzerrollen anpassbar sind** und zugleich ein **hohes Maß an Professionalität und Sicherheit** gewährleisten. **Die Zukunft der E-Mail liegt nicht im Wettbewerb mit Messaging – sondern in der Ergänzung.**

E-Mail tritt in eine neue Ära ein – geprägt von intelligenteren Tools, stärkerem Schutz und strategischer Integration. Für die IT geht es nicht darum, den Status quo zu erhalten, sondern die nächste Entwicklungsstufe aktiv mitzugestalten.

Sicherheit bleibt oberste Priorität.

Mit zunehmenden Bedrohungen und sich wandelnden regulatorischen Anforderungen ist der Schutz des Posteingangs wichtiger denn je.

KI wird zur Infrastruktur.

Automatisierung, Klassifizierung und Risikofrüherkennung sind keine Zusatzfunktionen mehr, sondern Grundvoraussetzungen.

Mail entwickelt sich weiter – sie wird nicht ersetzt.

Sie bleibt zentral für die geschäftliche Kommunikation, besonders in vertrauensbasierten, regulierten und kundenorientierten Szenarien.

Die IT führt den Wandel an.

Ob sichere Plattformen oder integrierte Workflows – der Weg nach vorn ist proaktiv, nicht reaktiv. E-Mail trägt die wichtigen Botschaften und die IT sorgt dafür, dass sie sicher, konsistent und intelligent ankommen.

E-Mail verschwindet nicht – aber wie sie verwaltet, gesichert und skaliert wird, verändert sich rasant. Branchenübergreifend, weltweit und unabhängig von der Unternehmensgröße wird von IT-Verantwortlichen mehr erwartet als nur die Sicherstellung des Betriebs: Sie sollen E-Mail weiterentwickeln. Die Daten aus diesem Trendreport zeichnen ein klares Bild: Bedrohungen bleiben bestehen, Komplexität nimmt zu – aber zugleich eröffnen sich Chancen: für Automatisierung, Integration und strategisches Governance-Design. Um Schritt zu halten, muss sich die IT vom reaktiven Betrieb zur aktiven Orchestrierung entwickeln – und die Systeme gestalten, die Kommunikation, Compliance und Konsistenz unternehmensweit ermöglichen.

Und obwohl neue Plattformen entstehen, **behauptet sich E-Mail – aus gutem Grund:** Sie bleibt der Standard für alles, was zählt: **Rechtsdokumente, Kundenkommunikation, Sicherheitswarnungen, Management-Briefings. E-Mail bietet Professionalität, Nachvollziehbarkeit und Kontrolle –** Eigenschaften, die andere Tools nicht ersetzen können. **Ihre Zukunft liegt nicht im Ersatz, sondern in der Weiterentwicklung.** Empfehlungen für IT-Führungskräfte:

1. Behandeln Sie E-Mail-Sicherheit als zentrales System, nicht als Zusatzfunktion.

Da in vielen Unternehmen über die Hälfte aller Sicherheitsvorfälle mit E-Mail verbunden ist, muss IT auf mehrschichtige, proaktive Schutzmechanismen setzen: DMARC, DKIM, SPF, automatisierte Bedrohungserkennung und kontinuierliches Awareness-Training für Mitarbeitende.

2. Passen Sie Sicherheitsmaßnahmen an Ihr Risikoprofil an.

Bedrohungen unterscheiden sich je nach Branche, Region und Unternehmensgröße. Ob Phishing in der Fertigung, Verschlüsselung im Finanzwesen oder Benutzerfreundlichkeit im Non-Profit-Bereich – die IT muss ihre Sicherheitsarchitektur auf das eigene Risiko zuschneiden. One-size-fits-all führt zu blinden Flecken.

3. Automatisieren Sie ressourcenintensive Routineaufgaben.

Spamfilterung, Signaturpflege und Archivierung sind nach wie vor große Zeitfresser – vor allem in großen Unternehmen. Durch zweckorientierte Automatisierung lassen sich Supportanfragen reduzieren und IT-Kapazitäten für strategische Aufgaben freisetzen.

4. Zentralisieren Sie die Signaturverwaltung, um Konsistenz sicherzustellen.

Zersplitterte Zuständigkeiten führen zu inkonsistenten Botschaften und hohem Supportaufwand. Mit einer zentralen Lösung kann die IT klare Richtlinien setzen, während Fachabteilungen Inhalte innerhalb definierter Vorgaben selbst verwalten – ohne manuelle Skripte oder Workarounds.

5. Machen Sie Ihr E-Mail-Ökosystem zukunftssicher – mit KI und Integration.

Fast die Hälfte der IT-Leader sagt, dass KI und Automatisierung die E-Mail-Zukunft prägen werden. Gleichzeitig sehen **90 %** E-Mail als kritisches Geschäftstool bis mindestens 2030. Die IT sollte Tools nicht nur nach Funktionen bewerten, sondern nach ihrer Fähigkeit zur Anpassung an hybride Kommunikationsmodelle, intelligente Workflows und skalierbare Governance.

E-Mail ist gemacht für die Kommunikation, die zählt – und ihre Weiterentwicklung beginnt bei der IT. Sie zu sichern, zu automatisieren und strategisch zu steuern ist kein technisches Upgrade. Es ist der Weg, wie Unternehmen geschützt, verbunden und zukunftsfähig bleiben.

Über Exclaimer

E-Mail ist gemacht für die Kommunikation, die zählt – und Exclaimer hilft IT-Teams, sie entsprechend zu steuern.

Exclaimer ist der führende Anbieter für die zentrale Verwaltung von **E-Mail-Signaturen** in **Microsoft- und Google-Umgebungen**. Die skalierbare Cloud-Plattform ermöglicht es Unternehmen, E-Mail-Signaturen zentral zu verwalten und zu automatisieren – und so **Compliance sicherzustellen, Effizienz zu steigern und ein konsistentes Markenbild** über alle Nachrichten hinweg zu gewährleisten.

Speziell für IT-Teams entwickelt, vereinfacht Exclaimer die Administration, indem manuelle Updates entfallen, Sicherheitsrisiken reduziert werden und die volle Kontrolle über die geschäftliche E-Mail-Kommunikation erhalten bleibt. Dank leistungsstarker Automatisierungs- und Integrationsfunktionen modernisieren IT-Abteilungen damit einen kritischen Teil ihres Kommunikations-Stacks – ohne zusätzliche Komplexität.

Kernfunktionen:

- **Zentrale Verwaltung** über Geräte, Plattformen und Nutzer hinweg
- **Skalierbare Automatisierung** für Formatierung, rollenbasierte Updates und Richtliniendurchsetzung
- **Integrierte Compliance-Funktionen** zur Unterstützung von Audit-Fähigkeit und Governance
- **Nahtlose Integration** mit Microsoft 365, Google Workspace und weiteren geschäftskritischen Tools

Exclaimer verarbeitet jährlich über **20 Milliarden E-Mail-Signaturen** von **9 Millionen E-Mail-Konten** in **70.000 Organisationen** – darunter **Sony, Mattel, Bank of America, NBC, die kanadische Regierung, die BBC und die Academy Awards**.

Mehr Informationen unter www.exclaimer.com Folgen Sie uns auf Facebook, LinkedIn und X (ehemals Twitter). Presseanfragen an: press@exclaimer.com

Demo vereinbaren

Trendreport
geschäftliche
E-Mails 2025:
Infrastruktur, Risiken
und die nächste
Chance für IT