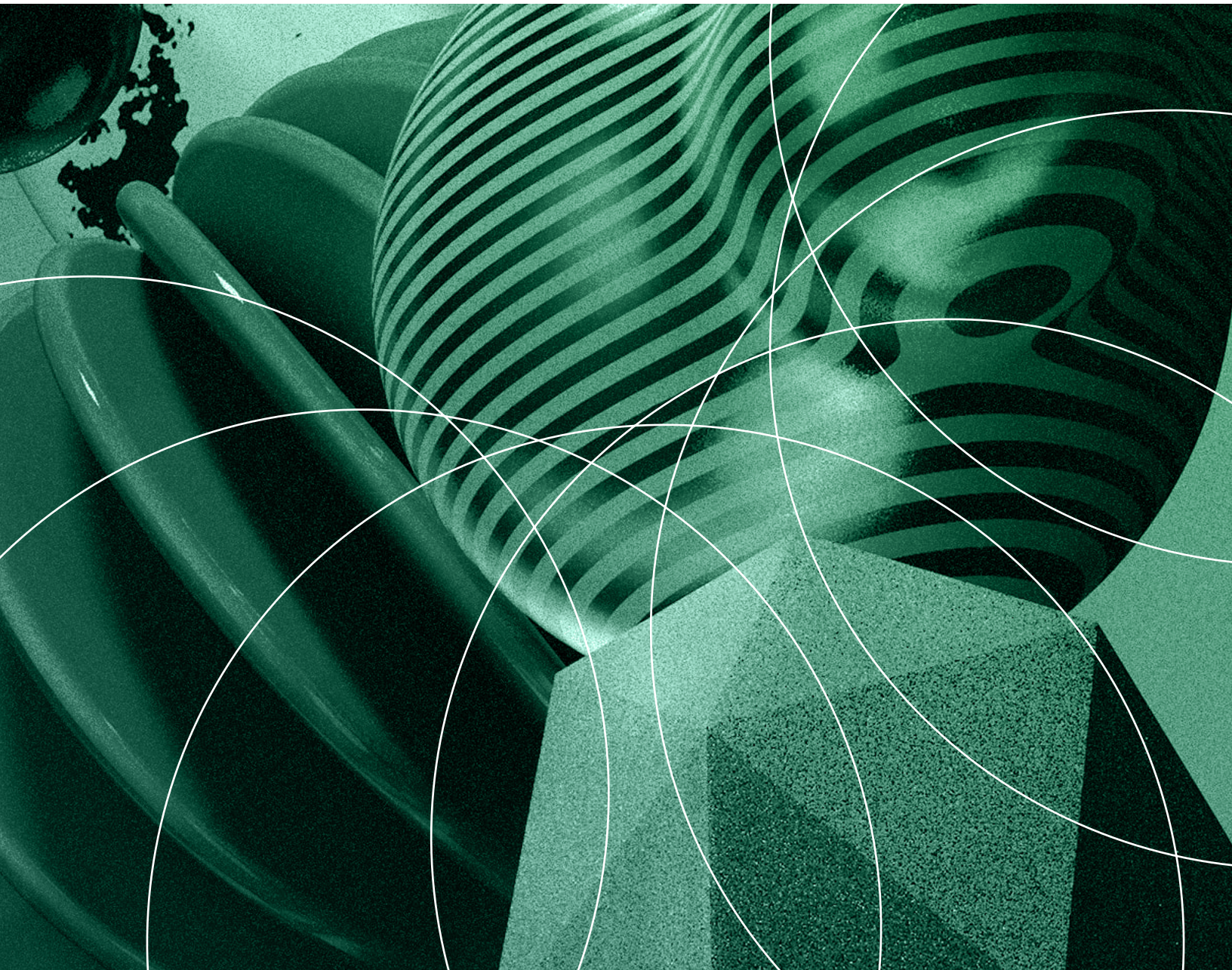
FORRESTER®

Die Zukunft der sicheren Kommunikation

Digitale Souveränität, Ende-zu-Ende Verschlüsselung und Interoperabilität werden die interne und externe Kommunikation am Arbeitsplatz revolutionieren.

EIN STRATEGIEPAPIER VON FORRESTER CONSULTING IM AUFTRAG VON ELEMENT, SEPTEMBER 2023



Inhaltsverzeichnis

Projektteam:

Sophia Christakis,

Market Impact Consultant

Alex Martini,

Associate Market Impact Consultant

Studienbeiträge:

Forrester-Forschungsgruppe Security & Risk

INFORMATIONEN ZU FORRESTER CONSULTING

Forrester bietet unabhängige, objektive und auf Forschungsergebnisse gestützte Beratungsdienstleistungen und unterstützt Führungskräfte so bei ihrer erfolgreichen Arbeit. In kundenspezifischen Studien arbeiten die erfahrenen Berater von Forrester gemeinsam mit Führungskräften daran, deren spezifische Prioritäten umzusetzen. Dabei kommt ein spezielles Kooperationsmodell zum Einsatz, das eine nachhaltige Wirkung sicherstellt. Weitere Informationen finden Sie auf unserer Website unter forrester.com/consulting.

Zusammenfassung

In den schnelllebigen digitalen Arbeitsumgebungen unserer Zeit sind die Kommunikationstechnologien eines Unternehmens (z. B. Messaging/Chat, Telefon- und Videokonferenzen) zentral für das Überbrücken der Distanz zwischen den Beschäftigten, Kollegen, Kunden und Partnern. Allerdings stellen die Führungskräfte fest, dass herkömmliche Kommunikationsansätze angesichts zunehmender Sicherheitsbedrohungen, Compliance-Anforderungen, Interoperabilitätsprobleme und der Notwendigkeit zusätzlicher Kontrollmechanismen oft nicht mehr ausreichen.

Im Frühjahr 2023 beauftragte Element Forrester Consulting mit einer Untersuchung des Mehrwerts, den Führungskräfte im Hinblick auf die Lösung dieser Probleme sicheren Kommunikationsplattformen beimessen. Forrester führte zu diesem Thema eine Onlinebefragung von 217 Führungskräften aus aller Welt durch, die für Behörden und in den Bereichen Gesundheitswesen, Energie/Versorgung und Transport/Logistik tätig und für die kommunikationstechnischen Entscheidungen ihrer jeweiligen Unternehmen zuständig sind. Die Studie hat ergeben, dass ein großer und weiter wachsender Bedarf an sicherer Kommunikation besteht, um Echtzeitverbindungen innerhalb und außerhalb des Unternehmens zu verbessern, ohne dass dadurch Sicherheits- und Compliance-Ziele beeinträchtigt werden.

Wichtigste Erkenntnisse

Führungskräfte schenken der Kommunikation mit Partnern besondere Aufmerksamkeit. Die Möglichkeit, sich Kompetenzen externer Partner zunutze zu machen, ist heute von entscheidender Bedeutung.[1] Allerdings wirft die externe Kommunikation Sicherheitsbedenken auf, und das Fehlen gemeinsamer technischer Standards führt zu Kompatibilitätsproblemen. Aus diesem Grund nennen 63 % der Führungskräfte den Schutz der Kommunikation entlang der Lieferkette als oberste Priorität für die nahe Zukunft.

Fehlende Kontrolle behindert häufig den Erfolg. Führungskräfte aus dem Technologiebereich müssen die Sicherheit und Zuverlässigkeit der Echtzeitkommunikation optimieren, stehen aber vor Herausforderungen. Nicht genehmigte Anwendungen, unflexible Systeme und fehlende Interoperabilität der verschiedenen Tools sind an der Tagesordnung. Unzureichende Eigenschaften für digitale Souveränität haben zur Folge, dass Führungskräfte nur begrenzte Kontrolle über die Kommunikationsdaten haben, was die Einhaltung von Daten-Governance-Anforderungen erschwert. Vielfach werden auch mehrere verschiedene Kommunikations-Apps eingesetzt, aber aufgrund der Abhängigkeit von den großen Anbietern bestehen noch immer Konzentrationsrisiken.

Eine sichere Kommunikationsplattform ermöglicht neue Arbeitsweisen und ganz konkrete Anwendungsfälle. Dedizierte Plattformen sind geeignet, die Lücke zwischen bestehenden Lösungen und dem Bedarf an mehr Unterstützung für unterschiedliche Mitarbeitertypen und Szenarien zu schließen. Führungskräfte sind besonders an Plattformen interessiert, die Hochverfügbarkeit, Ende-zu-Ende Verschlüsselung, hohe Zuverlässigkeit sowie Funktionen für digitale Souveränität und der Kommunikation im dezentralen Verbund unterstützen. Auch vertritt eine Mehrheit der Führungskräfte die Meinung, dass eine Plattform, die diese und weitere wertstiftende Funktionen bietet, ihnen sinnvolle Verbesserungen in den Bereichen Sicherheit, Benutzerfreundlichkeit, Compliance und Produktivität ermöglichen würde.

Echtzeitkommunikation als Grundlage für Geschäftsabläufe

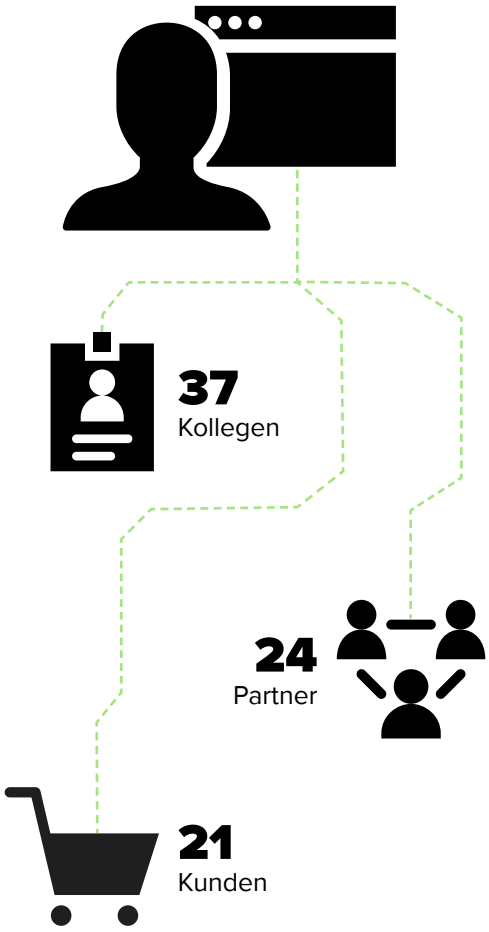
Die in einem Unternehmen eingesetzten Kommunikations-Tools sind zentral für die tägliche Zusammenarbeit der Mitarbeiter mit internen und externen Stakeholdern. Häufig werden auch personenbezogene Kundendaten, Einblicke in Geschäftsabläufe, vertrauliche Dokumente oder andere hochsensible Daten übertragen.[2] Daher ist es für Unternehmen heute wesentlich, dass derartige Tools unter allen Umständen ohne Unterbrechungen, Verzögerungen oder Risiken funktionieren. In der modernen vernetzten Welt, in der systemische Risiken, Compliance-Anforderungen, Sicherheitsbedrohungen und Benutzererwartungen ständig zunehmen, ist es jedoch noch komplizierter.[3]

75 % der Führungskräfte geben an, dass Zuverlässigkeit und Sicherheit der Kommunikation in ihrer Organisation entscheidend für das Vertrauen in ihre Services ist. Viele von ihnen sind allerdings besorgt um die Sicherheit und Zuverlässigkeit der internen und externen Kommunikation. In Verlauf einer ganz normalen Woche kommuniziert jeder Mitarbeiter über einschlägige Tools mit vielen Kollegen, Kunden und Partnern (Abbildung 1).[4] Veränderungen in den Arbeitsmustern der Beschäftigten, bei den Kundenerwartungen und in den Abläufen der Wertschöpfungsketten erhöhen die Komplexität solcher Interaktionen und stellen zunehmend neue Anforderungen an die Tools. So haben 74 % der Führungskräfte die Erfahrung gemacht, dass der Schutz der internen Kommunikation infolge der Zunahme hybrider Arbeitsmethoden eine Herausforderung darstellt, und 66 % haben festgestellt, dass die Kunden mehr Transparenz und bessere Kontrolle über die von ihnen geteilten Informationen erwarten.

ABBILDUNG 1

Mitarbeiterkommunikation über ein weites Netzwerk

Durchschnittliche Anzahl von Personen, mit denen jeder Mitarbeiter in einer normalen Arbeitswoche kommuniziert:



Basis: 217 Entscheidungsträger für Kommunikationstechnologie weltweit
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

BRÜCHE IN DER KOMMUNIKATION MIT EXTERNEN PARTNERN FÜHREN ZU BEHELFSLÖSUNGEN

56 % der Befragten geben an, dass ihr Unternehmen Teil einer größeren Wertschöpfungskette mehrerer Partner ist, die kooperieren, um wichtige Leistungen für Kunden zu erbringen. Aus diesem Grund ist eine schnelle, sichere und effektive Kommunikation zwischen diesen Partnern unverzichtbar. Die Mitarbeiter nutzen eine Reihe traditioneller Tools für den Kontakt mit den Partnern, wobei etwa 88 % der Befragten angaben, häufig oder sehr häufig über E-Mail zu kommunizieren. Dass gerade E-Mail so beliebt ist, überrascht nicht, denn E-Mail basiert auf einem allgemeinen Standard und ist somit ein gemeinsamer Nenner zwischen den Organisationen.

Zwar haben E-Mail und weitere häufig genutzte Tools wie etwa Anwendungen für Audio- und Videokonferenzen ihre Berechtigung, unterliegen aber bei der gemeinsamen Nutzung mit Partnern oft auch Einschränkungen in Bezug auf Kompatibilität, Benutzerfreundlichkeit und/oder Sicherheit. Die meisten Befragten sind sich einig, dass solche Lösungen für eine sichere und zuverlässige Echtzeitkommunikation in diesem Kontext nicht besonders gut geeignet sind (Abbildung 2). So wird die Sicherheit von E-Mails beispielsweise durch die fehlende Ende-zu-Ende Verschlüsselung beeinträchtigt. Die Befragten erwähnen ferner Risiken durch Viren, die sich leicht über E-Mail-Anhänge und Links verbreiten können, und das Fehlen von Möglichkeiten zur Echtzeitinteraktion.

Isolierte Kommunikationsplattformen, zeitliche Verzögerungen und Reibungsverluste bei der Zusammenarbeit sind angesichts der Marktgegebenheiten und der Erwartungen der Kunden heute nicht mehr akzeptabel. Mitarbeiter, die intern wie auch privat die Nutzung nahtloser Kommunikationsmittel ohne Wartezeiten gewohnt sind, greifen unter Umständen auf Messaging-Apps aus dem Verbraucherbereich zurück, wenn die im Unternehmen eingesetzten Tools den anstehenden Aufgaben nicht gewachsen sind. Tatsächlich geben 52 % der Führungskräfte an, dass ihre Mitarbeiter für die Kommunikation mit Partnern häufig nicht genehmigte Echtzeit-Chat-Apps verwenden. Diese nicht genehmigten Tools bergen eine Reihe schwerwiegender Risiken: Compliance-Verstöße, Mithören durch Dritte, Datenverlust oder -offenlegung, fehlende Kontrollmöglichkeiten für die Administration und auch Reputationsprobleme.[5]

> Nicht genehmigte Apps unterwandern das Unternehmen, wenn die zugelassenen Tools den Aufgaben nicht gewachsen sind.

ABBILDUNG 2

Herkömmliche Tools sind für eine sichere und zuverlässige Partnerkommunikation nicht mehr ausreichend

(Dargestellt werden die Werte für „nicht sehr gut geeignet“.)

Offizielle oder Arbeits-E-Mail **66 %**

„Viren verbreiten sich leicht über E-Mail-Anhänge oder Links.“
– Manager im Gesundheitswesen, USA

„Weniger Kollaborationsfunktionen.“
– Bereichsleiter bei einem Transport- und Logistikunternehmen, Frankreich

„Echtzeitinteraktion ist schlicht nicht möglich.“
– Bereichsleiter bei einer nationalen Verteidigungs-/Sicherheitsbehörde, USA

Offizielle Tools für die Sprachkommunikation **76 %**

„Erschweren eine Rationalisierung von Arbeitsabläufen oder die Automatisierung bestimmter Prozesse.“
– Manager bei einem Energieerzeuger, USA

„Weniger Spielraum für Dokumentation.“
– Vorstand bei einem Transport- und Logistikunternehmen, Vereinigtes Königreich

„Der Zugriff ist ortsabhängig mitunter nicht möglich.“
– Leiter bei einer regionalen Behörde, Deutschland

Offizielle Videokonferenz-Tools **79 %**

„Die Kommunikation ist nicht reibungslos, und es kommt vermehrt zu Ausfallzeiten.“
– Leiter bei einer Gesundheitseinrichtung, Kanada

„Schwierigkeiten bei technischer Kompatibilität und Kollaboration.“
– Bereichsleiter bei einer nationalen Verteidigungs-/Sicherheitsbehörde, Vereinigtes Königreich

„Die Weitergabe sensibler Informationen birgt ein großes Risiko.“
– Bereichsleiter bei einer nationalen Verteidigungs-/Sicherheitsbehörde, Frankreich

Basis: 217 Entscheidungsträger für Kommunikationstechnologie weltweit
Hinweis: Aufgeführt sind drei am häufigsten genannten Antworten.
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

DIE BEDEUTUNG EINER SICHEREN UND ZUVERLÄSSIGEN PARTNERKOMMUNIKATION NIMMT ZU

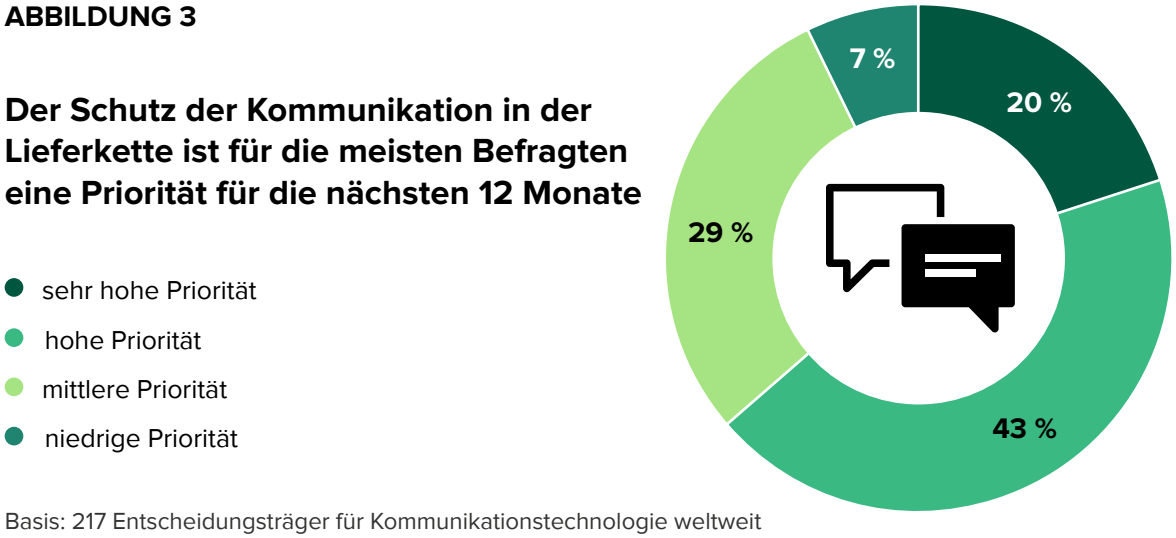
53 % der Führungskräfte erwarten, dass die Anzahl der Partner in ihrer Lieferkette in den kommenden zwei bis drei Jahren zunehmen wird. Mit der immer stärkeren Abhängigkeit von Partnern steigt jedoch auch die Bedeutung einer sicheren Partnerkommunikation. 63 % der Führungskräfte sagen daher auch, dass der Schutz der Kommunikation entlang ihrer Lieferketten im kommenden Jahr eine hohe oder entscheidende Priorität für ihr Unternehmen darstellen wird (Abbildung 3).

77 %

sagen, dass Sicherheitsschwachstellen in Tools für die Kommunikation mit Partnern ein erhebliches Risiko für ihr Unternehmen darstellen.

ABBILDUNG 3

Der Schutz der Kommunikation in der Lieferkette ist für die meisten Befragten eine Priorität für die nächsten 12 Monate



Basis: 217 Entscheidungsträger für Kommunikationstechnologie weltweit
Hinweis: Aufgrund von Rundungen ergibt die Summe der Prozentsätze möglicherweise nicht 100 %.
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

Bestehende Kommunikationsansätze zeigen Funktionsmängel auf und bergen Risiken

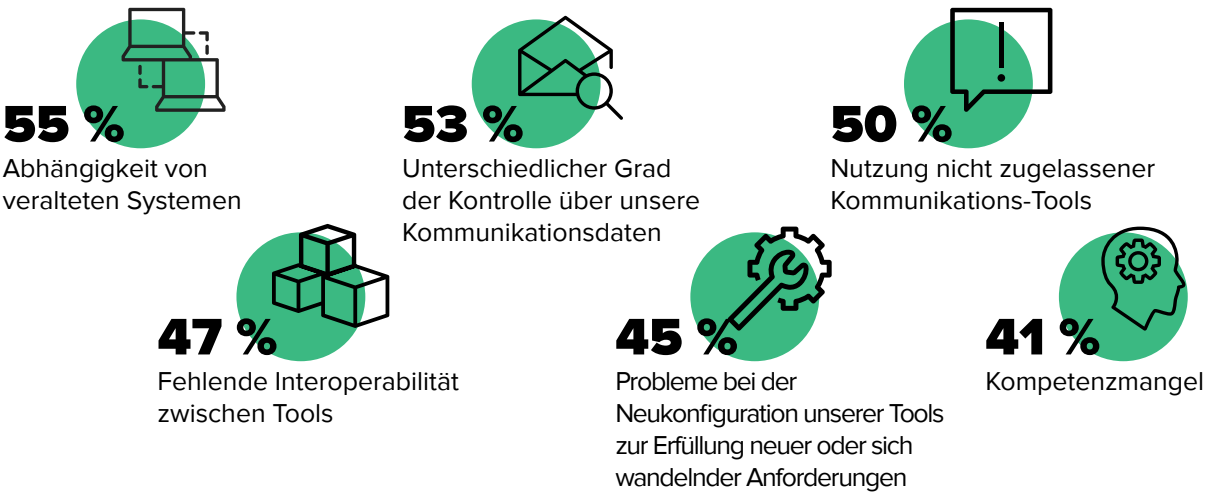
Neben der Verwendung nicht genehmigter Kommunikations-Tools, was 50 % der Befragten als wesentliche Herausforderung bezeichnen, stehen die Führungskräfte auf dem Weg zur Verbesserung von Sicherheit und Zuverlässigkeit der Echtzeitkommunikation vor einer Reihe weiterer Hindernisse (Abbildung 4).

Hierzu gehören vor allem veraltete oder anderweitig unflexible Systeme, die sich nicht ohne Weiteres an neue oder sich wandelnde Anforderungen anpassen lassen. Ein weiterer Aspekt ist der unterschiedliche Grad der Kontrolle über die Kommunikationsdaten, der von den verfügbaren Konfigurationseinstellungen und Optionen für das Daten-Hosting und den Möglichkeiten für digitale Souveränität abhängig ist. Mangelnde Interoperabilität zwischen den Tools bedeutet, dass die meisten Anwendungen nicht miteinander kommunizieren können. So entstehen Kommunikationssilos und die Notwendigkeit, häufig zwischen Anwendungen und Kontexten zu wechseln, was Konzentration und Produktivität der Mitarbeiter beeinträchtigt.

> Da die Zahl der von den Beschäftigten benötigten Apps weiter zunimmt, wird die Interoperabilität noch wichtiger, um Kontextwechsel und Zeitverluste zu vermeiden.[6]

ABBILDUNG 4

Erhebliche Hindernisse für die Optimierung von Sicherheit und Zuverlässigkeit der Echtzeitkommunikation



Basis: 217 Entscheidungsträger für Kommunikationstechnologie weltweit
Hinweis: Dargestellt sind die 6 am häufigsten genannten Antworten.
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

Im Schnitt arbeiten die befragten Führungskräfte mit fünf separaten Kommunikations-Apps, bei 21 % sind es sogar sieben oder mehr. Während sich Führungskräfte mit einer Fülle von Kommunikations-Tools auseinandersetzen müssen, besteht für ihre Unternehmen nach wie vor ein Konzentrationsrisiko. Seit Anfang 2020 weichen eigenständige Apps für Chats, Videokonferenzen oder Dokumentenfreigabe zunehmend Komplettpaketen großer Anbieter, da sich Unternehmen aufgrund der flächendeckenden Einführung des Homeoffice dazu gezwungen sahen, auf New-Work-Arbeitsweisen umzustellen.[7] Es ist kennzeichnend für die Abhängigkeit von diesen Big-Tech-Firmen, dass 85 % der Befragten angeben, dass allein durch eine Störung bei einem einzigen ihrer großen Kommunikationstechnologieanbieter ein erhebliches Risiko für ihr Unternehmen entstünde.

KOMMUNIKATION, DIE „GERADE SICHER GENUG“ IST, REICHT NICHT AUS

Unternehmen müssen prüfen, wie gut ihre Kommunikationstechnologien verschiedenen Szenarien und Stresstests standhalten. Selbst genehmigte Apps stellen in bestimmten Anwendungsfällen ein Risiko dar.[8] Ein Beispiel dafür ist die Incident Response, also die Reaktion auf sicherheitsrelevante Vorfälle: 75 % der Entscheidungsträger befürchten bei einem Cyberangriff eine Kompromittierung ihrer Kommunikationstechnologien, die dazu führen könnte, dass Angreifer die Echtzeitkommunikation von Mitarbeitern und Einsatzkräften mithören. Auch fehlen bei herkömmlichen Tools bestimmte Kontrollmöglichkeiten, wie z. B. Funktionen für eine stärker differenzierte Zugriffssteuerung bei der externen Kooperation oder beim Datenschutz.[9]

Nach eigenen Angaben befürchten 65 % der Entscheidungsträger bei kommunikationsrelevanten Sicherheitsverstößen erhebliche Kosten direkter (z. B. Bußgelder, Umsatzeinbußen aufgrund von Systemausfällen) wie auch indirekter Art (etwa Produktivitätsverluste bei den Mitarbeitern). Dabei sprechen die meisten von ihnen aus eigener Erfahrung: 66 % der Befragten stammen aus Unternehmen, die in den letzten drei Jahren von einem kommunikationsspezifischen Sicherheitsverstoß oder einer Kompromittierung betroffen waren, wobei 25 % von ihnen in diesem Zeitraum sogar mehrere Vorfälle zu verzeichnen hatten. Solche Vorfälle haben verschiedene negative Auswirkungen, etwa zusätzliche Sicherheits- und Revisionsanforderungen, behördliche Untersuchungen und Produktivitätseinbußen. Zu den häufigsten Folgen gehört dabei der Vertrauensverlust bei Kunden (an erster Stelle) und Partnern (an vierter Stelle).

72 %

sagen, dass disruptive Ereignisse ihnen die strategische Wichtigkeit ihrer Kommunikationstechnologien vor Augen geführt haben.

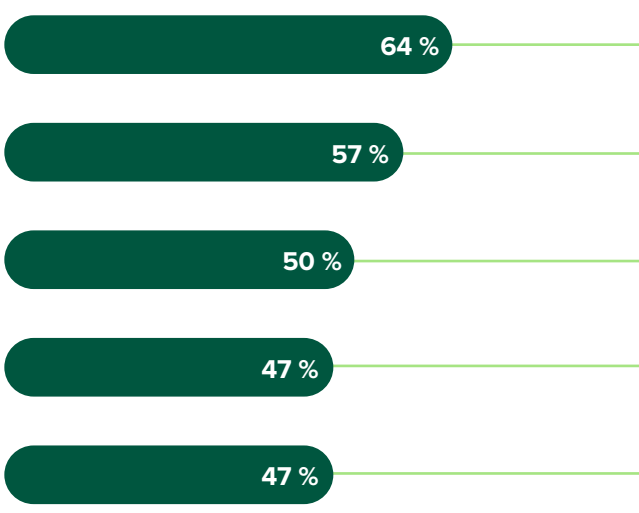
Zukunftsfähige Organisationen nutzen sichere Kommunikationsplattformen

Entscheidungsträger prognostizieren, dass sich die Kommunikation innerhalb und außerhalb der Unternehmen weiterentwickeln muss, um noch sicherer, nahtloser und robuster zu werden (Abbildung 5). Zur Vorbereitung darauf müssen Behörden und Unternehmen zukunftsfähig werden. Eine wesentliche Komponente der Zukunftsfähigkeit fußt auf dem Ökosystem: Es müssen Kompetenzen entwickelt werden, um den im internen und externen Ökosystem des Unternehmens vorhandenen Mehrwert umfassend zu nutzen.[10]

Die Optimierung der Kommunikation zwischen allen Akteuren bringt Unternehmen dieser Vision einen Schritt näher und eröffnet Möglichkeiten für mehr Zusammenarbeit und Innovation. Sicherheit und Zuverlässigkeit müssen jedoch weiterhin im Vordergrund stehen, um zu verhindern, dass aus diesen Chancen Bedrohungen werden. Die Befragten sind der Meinung, dass Bemühungen zur Verbesserung von Sicherheit und Zuverlässigkeit der Echtzeitkommunikation insgesamt zu einer erheblichen Verringerung der regulatorischen (78 %), Sicherheits- (75 %), Betriebs- (70 %) und Reputationsrisiken (68 %) führen würden.

ABBILDUNG 5

Interne und externe Kommunikation werden sich in Zukunft verändern



Basis: 217 Entscheidungsträger für Kommunikationstechnologie weltweit
Hinweis: Dargestellt sind die 5 am häufigsten genannten Antworten.
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

DEDIZIERTE PLATTFORMEN BIETEN UMFASSENDE SICHERHEIT

In bestimmten Szenarien (z. B. bei der Reaktion auf einen Datensicherheitsvorfall oder beim Ausfall kritischer Infrastrukturen) und für bestimmte Benutzer (z. B. Mitarbeiter mit Kundenkontakt, leitende Angestellte) gelten ganz spezifische Kommunikationsanforderungen, die mehr Sorgfalt erfordern. Hier spielen alternative Plattformen, die sichere Kommunikation ermöglichen, eine entscheidende Rolle, da beispielsweie Kommunikationskanäle wie die folgenden bereitgestellt werden können:

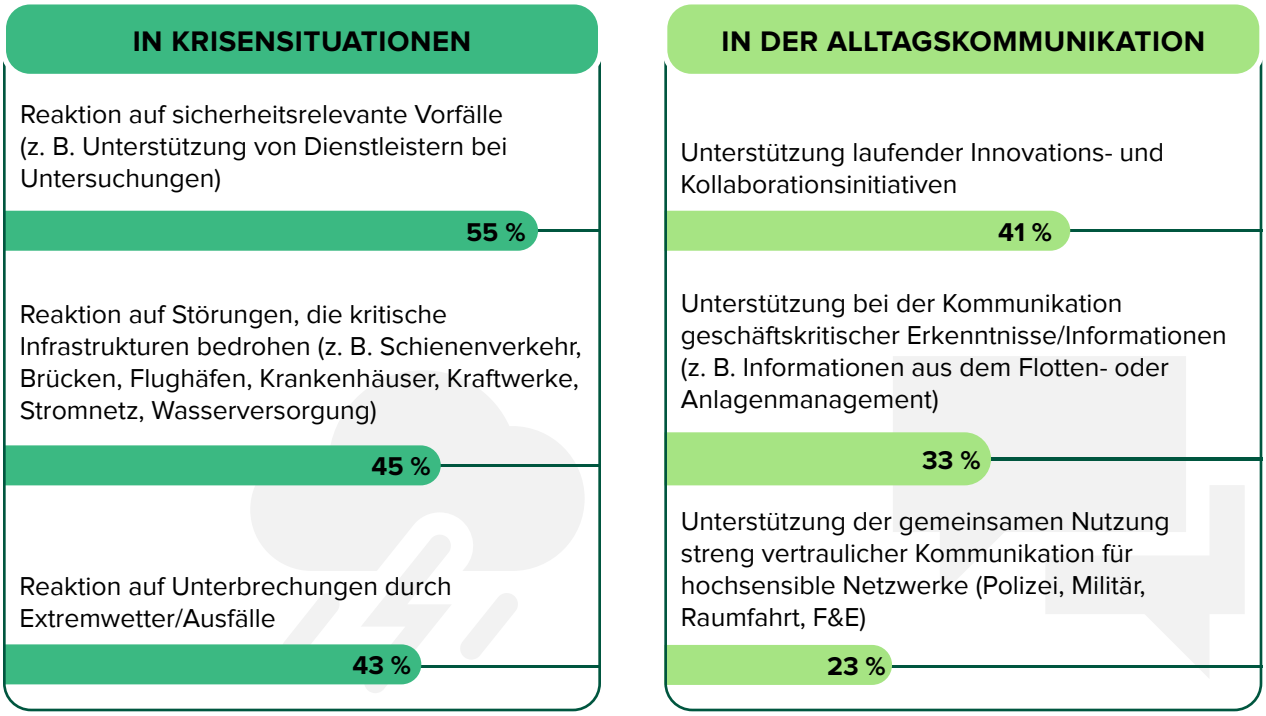
- **Out-of-Band Kommunikation** Als Out-of-Band Kommunikationskanäle werden Kanäle bezeichnet, die von der primären Kommunikationsinfrastruktur des Unternehmens getrennt sind. Solche Kanäle sind besonders nützlich in Situationen, in denen die Geschäftskontinuität aufrecht gehalten werden muss (z. B. wenn die Hauptserver des Unternehmens ausfallen), bei Gesprächen von Führungskräften über sensible Themen (beispielsweise Personalbeschaffung, Boni, Fusionen/Übernahmen) und bei der Reaktion auf Vorfälle (wenn etwa ein Cyberangriff die primären Kanäle beeinträchtigt oder bereits kompromittiert hat).
- **Air-Gap-Kommunikation.** Bei Air-Gap-Kommunikationskanälen handelt es sich um hochsichere Netze, die physisch von anderen Netzwerken und Systemen getrennt sind. Solche Kanäle werden von Behörden, Nachrichtendiensten und wichtigen staatlichen Einrichtungen zur Übertragung streng geheimer Informationen in hochsensiblen Umgebungen eingesetzt. Sie eignen sich außerdem für hochgradig regulierte Branchen (etwa Wertpapierbörsen) und Industriesteuerungsumgebungen (z. B. kritische Systeme, beispielsweise in kerntechnischen Anlagen oder der Luftfahrt), die aus Sicherheits- und Datenschutzgründen eine solche Trennung erfordern.

52 % der Führungskräfte geben an, dass in ihren Unternehmen für eine Vielzahl von Szenarien ein großer oder erheblicher Bedarf an Echtzeitkommunikation in solchen sicheren (z. B. Air-Gap-, isolierten oder hochsensiblen) Umgebungen besteht. Zudem erwarten die meisten von ihnen eine Steigerung dieses Bedarfs (Abbildung 6).

> **64 %**
>
> gehen davon aus, dass die Notwendigkeit, Partnern Zugang zu Air-Gap- oder isolierten Umgebungen zu gewähren, in ihren Unternehmen in den kommenden zwei bis drei Jahren steigen wird.

ABBILDUNG 6

Geschützte Echtzeitkommunikation wird in Krisen- und Alltagsszenarien benötigt



Basis: 212 Entscheidungsträger für Kommunikationstechnologie weltweit aus Unternehmen, die Echtzeitkommunikation in gesicherten Umgebungen benötigen
Hinweis: Dargestellt sind die am häufigsten genannten Antworten.
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

FÜHRUNGSKRÄFTE SUCHEN NACH PLATTFORMFUNKTIONEN, DIE DIFFERENZIERTEN MEHRWERT BIETEN

77 % der Führungskräfte sind der Meinung, dass das Marktumfeld von ihnen verlangt, beim Schutz ihrer Kommunikation stets auf dem aktuellen Stand zu bleiben. Im Falle sicherer Kommunikationsplattformen bedeutet dies, dass Lösungen Vorrang eingeräumt wird, die Folgendes bieten (Abbildung 7):

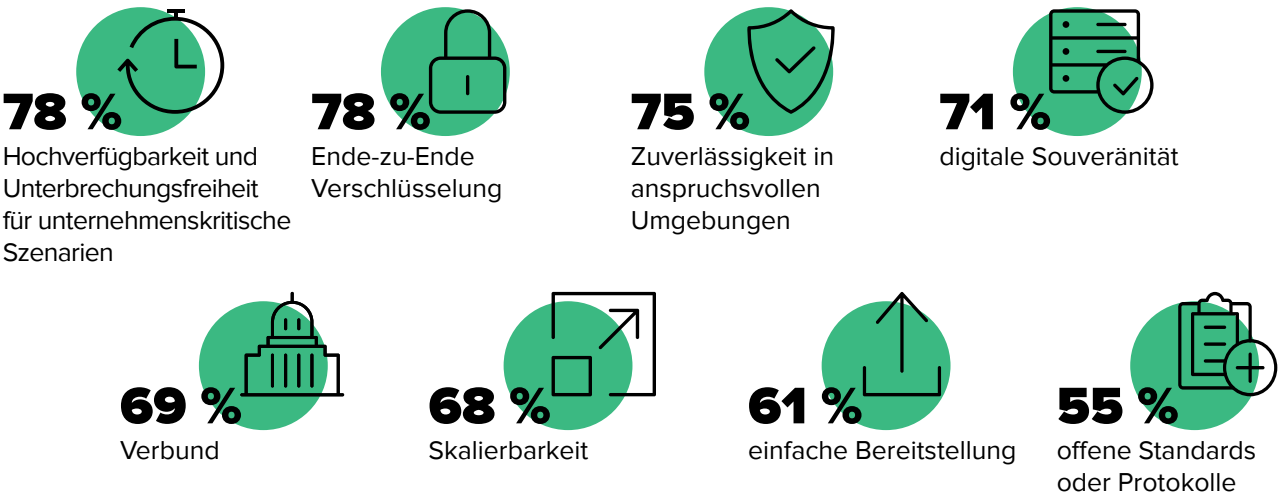
- Hochverfügbarkeit und Unterbrechungsfreiheit für unternehmenskritische Szenarien, insbesondere im Bereich der kritischen Infrastruktur. Im Gesundheitswesen steht diese Anforderung bei den meistgewünschten Fähigkeiten an dritter Stelle, bei Behörden und Energieversorgern sogar ganz oben auf der Liste.

- Ende-zu-Ende Verschlüsselung zum Schutz der Daten: Noch nicht einmal der Technologieanbieter und die Plattform selbst dürfen den Inhalt der Kommunikation einsehen können. Die Daten werden dabei vor der Übertragung am Endpunkt verschlüsselt. Diese Maßnahme soll Datensicherheit, Datenschutz und Schutz vor Datenmanipulation gewährleisten. Nur der Absender und der Empfänger haben Zugang zu den Daten.
- Zuverlässigkeit auch unter schwierigen Bedingungen – z. B. in Regionen mit geringer Bandbreite oder schlechter Konnektivität –, um die betriebliche und geschäftliche Resilienz des Unternehmens zu unterstützen
- Digitale Souveränität durch Funktionen, die Eigentümerschaft an und Kontrolle über Kommunikationsdaten bieten, sodass sie der Governance-Struktur des Unternehmens unterliegen. Dies schließt etwa auch ein, wo und auf welche Weise die Daten gehostet und kontrolliert werden.
- Bildung von Verbunden, um getrennte Kommunikationstechnologien zusammenzuführen und eine einfache Konnektivität zwischen separaten Organisationen innerhalb der Lieferkette oder einer übergeordneten Organisation zu ermöglichen.

ABBILDUNG 7

Zentrale Fähigkeiten werden zur Optimierung der Echtzeitkommunikation gebraucht

(Dargestellt werden Antworten für „Erheblicher Nutzen“ und „Transformativer Nutzen“.)



Basis: 217 Entscheidungsträger für Kommunikationstechnologie weltweit
Hinweis: Dargestellt sind 8 Antworten.
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

77 % der Führungskräfte geben an, dass ihre Unternehmen Probleme haben, den Datenschutz und die Kontrolle der über Kommunikationstechnologien ausgetauschten Daten zu gewährleisten. Angesichts dieses Hindernisses und der Notwendigkeit, regulatorische und unternehmensinterne Vorgaben bei Governance und Datenkontrolle zu meistern, wird klar, warum die Führungskräfte der digitalen Souveränität einen so hohen Wert beimessen. Neben der Stärkung des Sicherheitsniveaus ihrer Unternehmen werden als weitere wesentliche Vorteile der digitalen Souveränität weniger Abhängigkeit von einem bestimmten Anbieter (weil etwa die Daten des Unternehmens nicht auf Systemen eines proprietären Anbieters gespeichert sind) und geringere Risiken genannt, die per se durch die Inanspruchnahme externer Anbieter oder Tools entstehen.

> **64 %**
>
> verbinden die Möglichkeiten für digitale Souveränität mit einer Verbesserung des Sicherheitsniveaus ihrer Unternehmen.

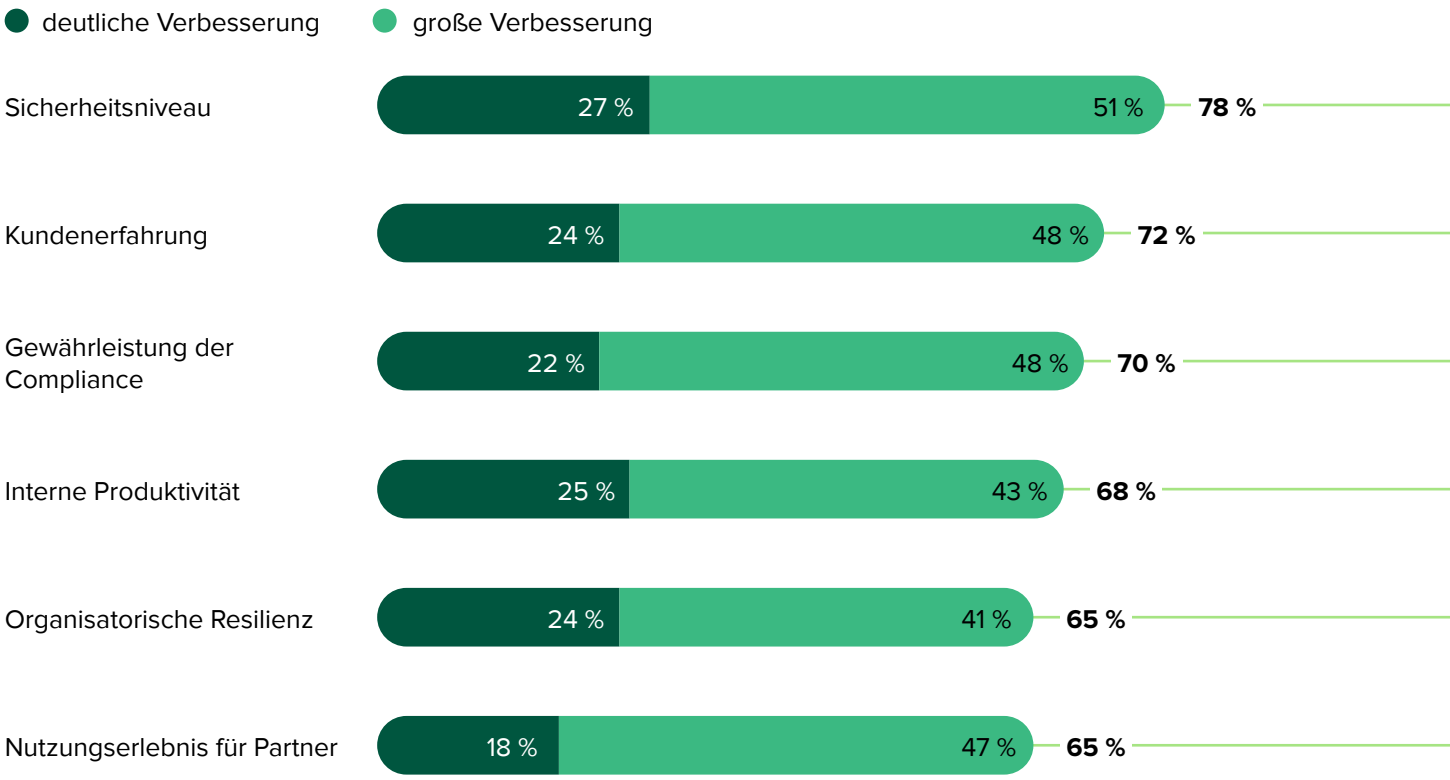
Führungskräfte werden bei der Bewertung sicherer Kommunikationsplattformen wahrscheinlich mehrere weitere Faktoren berücksichtigen. Hierzu gehört etwa die Unterstützung offener Standards. Offene Standards helfen bei der Lösung von Interoperabilitätsproblemen, denn sie stellen formalisierte Protokolle bereit, die von mehreren Akteuren akzeptiert werden (ähnlich wie die bei E-Mails eingesetzten gemeinsamen Standards) und eine stärkere Vernetzung zwischen einem Unternehmen und seinen Branchenökosystemen ermöglichen. Zudem verringern sie die Abhängigkeit des Unternehmens von einem einzelnen Anbieter und ermöglichen vielmehr die Nutzung unterschiedlichster Produkte einer beliebigen Zahl von Anbietern, wodurch Innovation im gesamten Ökosystem gefördert wird.

SICHERE KOMMUNIKATIONSPLATTFORMEN VERBESSERN DIE SICHERHEIT UND DAS BENUTZERERLEBNIS

Weniger als 45 % der befragten Führungskräfte gaben an, dass die aktuellen Tools ihrer Unternehmen auch nur eine dieser zentralen Fähigkeiten sehr gut unterstützen. Allerdings vertreten sie die Ansicht, dass der Zugang zu einer sicheren Kommunikationsplattform mit solchen Funktionen einen erheblichen Nutzen mit sich bringen würde. Zu den Vorteilen, die sie sich davon versprechen, gehören spürbare Verbesserungen beim Sicherheitsniveau, beim Nutzungserlebnis für Kunden und Partner, bei der Compliance (z. B. Datenaufbewahrung, Datenschutz) und bei der Produktivität (Abbildung 8).

ABBILDUNG 8

Sichere Kommunikationsplattformen, die marktführende Funktionen bieten, steigern den Nutzen



Basis: 217 Entscheidungsträger für Kommunikationstechnologie weltweit
Hinweis: Dargestellt werden die Auswirkungen, die sich die Befragten von der Einführung einer sicheren Kommunikationsplattform mit den zuvor als wertschöpfend eingestuften Funktionen (z. B. Hochverfügbarkeit, Ende-zu-Ende Verschlüsselung, Zuverlässigkeit, digitale Souveränität, Verbund) versprechen.
Quelle: Studie von Forrester Consulting im Auftrag von Element, Mai 2023

Empfehlungen

Aus der von Forrester durchgeführten ausführlichen Befragung von über 200 Technologieentscheidern zur sicheren Kommunikation ergaben sich fünf wichtige Empfehlungen:

Benutzerfreundlichkeit ist nicht verhandelbar.

Wenn Beschäftigte und Partner den Wert einer Lösung nicht erkennen, dann werden sie sie auch nicht nutzen. Bei der Festlegung von Anforderungen und gewünschten Funktionen für sichere Kommunikationstechnologien durch die Unternehmen spielt die Benutzerfreundlichkeit eine zentrale Rolle. Angesichts der großen Zahl verfügbarer nicht genehmigter Optionen werden die Mitarbeiter nutzen, was ihnen beim Erledigen ihrer Aufgaben am besten dient.

Schützen Sie die Kommunikationsdaten Ihres Unternehmens durch flexible Hosting-Optionen und Ende-zu-Ende Verschlüsselung, um echte digitale Souveränität zu erzielen.

Zu den Kontroll- und Sicherheitsfunktionen, die eine stärkere Differenzierung ermöglichen, gehören BYOK („Bring Your Own Key“) für die Verschlüsselung, Kryptoagilität und Anbietertransparenz mit SBOM-Berichten („Software Bill of Materials“). Robuste Sicherheitsfunktionen können auch bei der Einhaltung verschiedener Sicherheits- und Datenschutzanforderungen eine große Hilfe sein, da sie Ihnen die Kontrolle über die Daten Ihres Unternehmens ermöglichen.

Achten Sie auf zusätzliche Funktionen zur Erfüllung von Compliance-Anforderungen, die über Sicherheit und Datenschutz hinausgehen.

Je nachdem, welche Compliance-Anforderungen Sie konkret zu erfüllen versuchen – wie z. B. branchenspezifische Vorschriften oder vertragliche Anforderungen Ihrer Geschäftspartner –, reichen die reinen Sicherheitsfunktionen möglicherweise nicht aus. Beispielsweise könnten Sie bestimmte Anforderungen an die Löschung oder Aufbewahrung von Daten haben.

Beseitigen Sie Ausfall- und Cybersicherheitsrisiken, die von zentralisierten Lösungen ausgehen.

Kommunikation ist das Rückgrat des Geschäftsbetriebs, und sichere Kommunikation ist sowohl für die tägliche Kommunikation als auch in Krisenzeiten wichtig. Hybrides Arbeiten wird abhängig davon zu- oder abnehmen, wie sich Unternehmen an eine Vielzahl von externen Faktoren anpassen müssen – seien es extreme Wetterbedingungen oder wettbewerbsorientierte Einstellungspraktiken. Systemische Risikoereignisse, Störungen und Ausfälle sowie Probleme bei kritischen Infrastrukturen tragen ebenfalls zu einem höheren Bedarf an betrieblicher und geschäftlicher Resilienz bei. Diese Tools müssen dort funktionieren, wo Ihre Mitarbeiter und Partner sie brauchen.

Integrieren Sie Interoperabilität in die Kommunikationslösung Ihres Unternehmens, um regulatorische Vorgaben ebenso gerecht zu werden wie sich wandelnden Anforderungen.

Die Verwendung offener Standards für die Interoperabilität ermöglicht es den Benutzern einer Plattform, mit jenen einer anderen Plattform zu kommunizieren. In der EU schreibt das im Mai 2022 verabschiedete Gesetz über digitale Märkte (GDM) die Interoperabilität von Messaging-Plattformen vor. Solche Plattformen haben bis März 2024 Zeit, die Vorgaben zu erfüllen.[11] Das MLS-Protokoll (Messaging Layer Security) – ein interoperabler Standard, der seit Jahren von der Internet Engineering Task Force (IETF) entwickelt wird – ist im Juli 2023 als RFC veröffentlicht worden.[12] Weitere offene Standards sind Web Real-Time Communication (WebRTC), das Session Initiation Protocol (SIP), das Extensible Messaging and Presence Protocol (XMPP) und Matrix. Für Messaging-Plattformen wird Interoperabilität schon bald obligatorisch sein, um zukunftsfähige Organisationen zu unterstützen.

Anhang A: Methodik

Für die vorliegende Studie führte Forrester eine Online-Befragung unter 217 Entscheidungsträgern aus Zentral- und Regionalbehörden sowie den Bereichen Energie/Versorgung, Gesundheitswesen und Transport/Logistik in Nordamerika und Europa durch, um den aktuellen und künftigen Bedarf an Kommunikationstechnologie zu bewerten. Die Fragen an die Teilnehmenden befassten sich mit der Häufigkeit, mit der Mitarbeiter verschiedene Kommunikations-Tools nutzen, um die Herausforderungen bei der Optimierung von Sicherheit, Zuverlässigkeit und Benutzererfahrung bei diesen Interaktionen sowie um den Nutzen, den eine sichere Kommunikationsplattform bieten kann, die häufige Herausforderungen beseitigt und die Wertschöpfung steigert. Die Teilnehmenden erhielten ein kleines Dankeschön für ihre aufgewendete Zeit. Die Studie wurde im Mai 2023 begonnen und abgeschlossen.

Anhang B: Demografische Daten

LAND	
USA	**32** %
Kanada	**19** %
Vereinigtes Königreich	**18** %
Deutschland	**16** %
Frankreich	**15** %

BRANCHE	
Bundes-/Zentralregierung	**30** %
Energie und Versorgung	**21** %
Gesundheitswesen	**20** %
Landes-/Regionalregierung	**16** %
Transport und Logistik	**13** %

ABTEILUNG	
IT	**55** %
Sicherheit	**30** %
Compliance/Risikomanagement	**16** %

ANZAHL DER MITARBEITER	
2.500 bis 4.999	**11** %
5.000 bis 9.999	**65** %
10.000 bis 19.999	**18** %
20.000 oder mehr	**7** %

POSITION	
Vorstand	**7** %
Vice President	**15** %
Bereichsleiter	**30** %
Manager	**47** %

Hinweis: Aufgrund von Rundungen ergibt die Summe der Prozentsätze möglicherweise nicht 100 %.

Anhang C: Schlussbemerkungen

[1] Quelle: „The Future Fit Practices Strategy“, Forrester Research, Inc., 23. September 2022.

[2] Quelle: „Now Tech: Secure Communications, Q2 2022“, Forrester Research, Inc., 2. Mai 2022.

[3] „Erfahrung“ bezieht sich in diesem Zusammenhang darauf, wie eine Person (sei es ein Kunde, ein Mitarbeiter oder ein Partner) ihre Interaktionen mit einem Unternehmen wahrnimmt. Der Begriff der Mitarbeitererfahrung („Employee Experience“) beschreibt etwa die Wahrnehmung der Mitarbeiter in Bezug auf die Interaktion mit ihrem Arbeitgeber. Dies schließt auch die Wahrnehmung von Technologien ein, die den Mitarbeitern für ihre tägliche Arbeit zur Verfügung stehen.

[4] Für die Zwecke dieser Studie bezieht sich der Begriff „Kunde“ auf Personen oder Gruppen, denen die Organisation Dienstleistungen oder Waren bereitstellt (z. B. Bürger, Patienten, Klienten).

[5] Quelle: „Now Tech: Secure Communications, Q2 2022“, Forrester Research, Inc., 2. Mai 2022.

[6] Quelle: „Make Digital Employee Experience The Centerpiece Of Your Digital Workplace Strategy“, Forrester Research, Inc. 15. November 2022.

[7] Quelle: „The Forrester Tech Tide™: Enterprise Collaboration Technologies, Q3 2022“, Forrester Research, Inc., 19. September 2022.

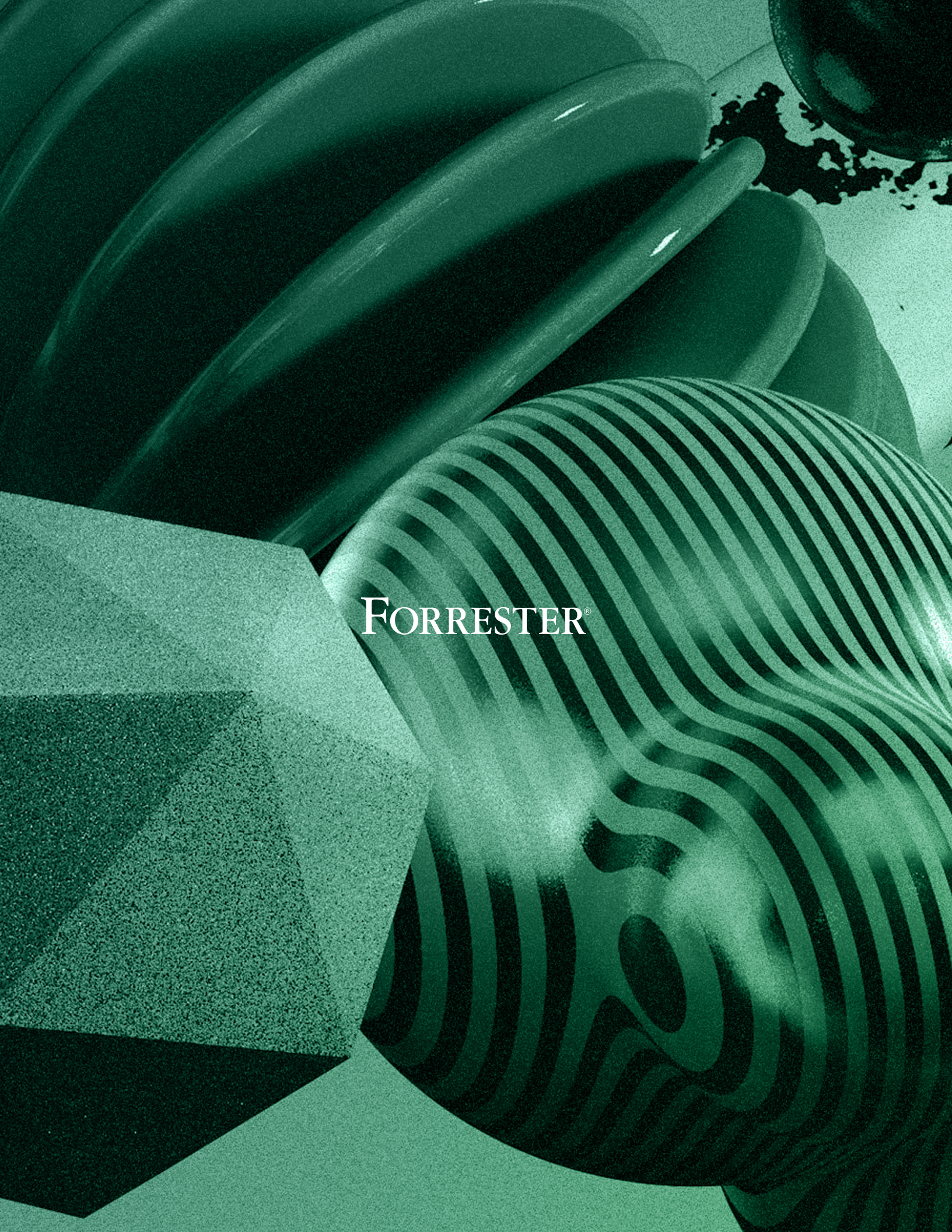
[8] Quelle: „Now Tech: Secure Communications, Q2 2022“, Forrester Research, Inc., 2. Mai 2022.

[9] ebd.

[10] Quelle: „The Future Fit Practices Strategy“, Forrester Research, Inc., 23. September 2022.

[11] Quelle: „Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force“, Pressemitteilung der Europäischen Kommission, 31. Oktober 2022.

[12] Quelle: „New MLS protocol provides groups better and more efficient security at Internet scale“, Internet Engineering Task Force, 19. Juli 2023.


FORRESTER®