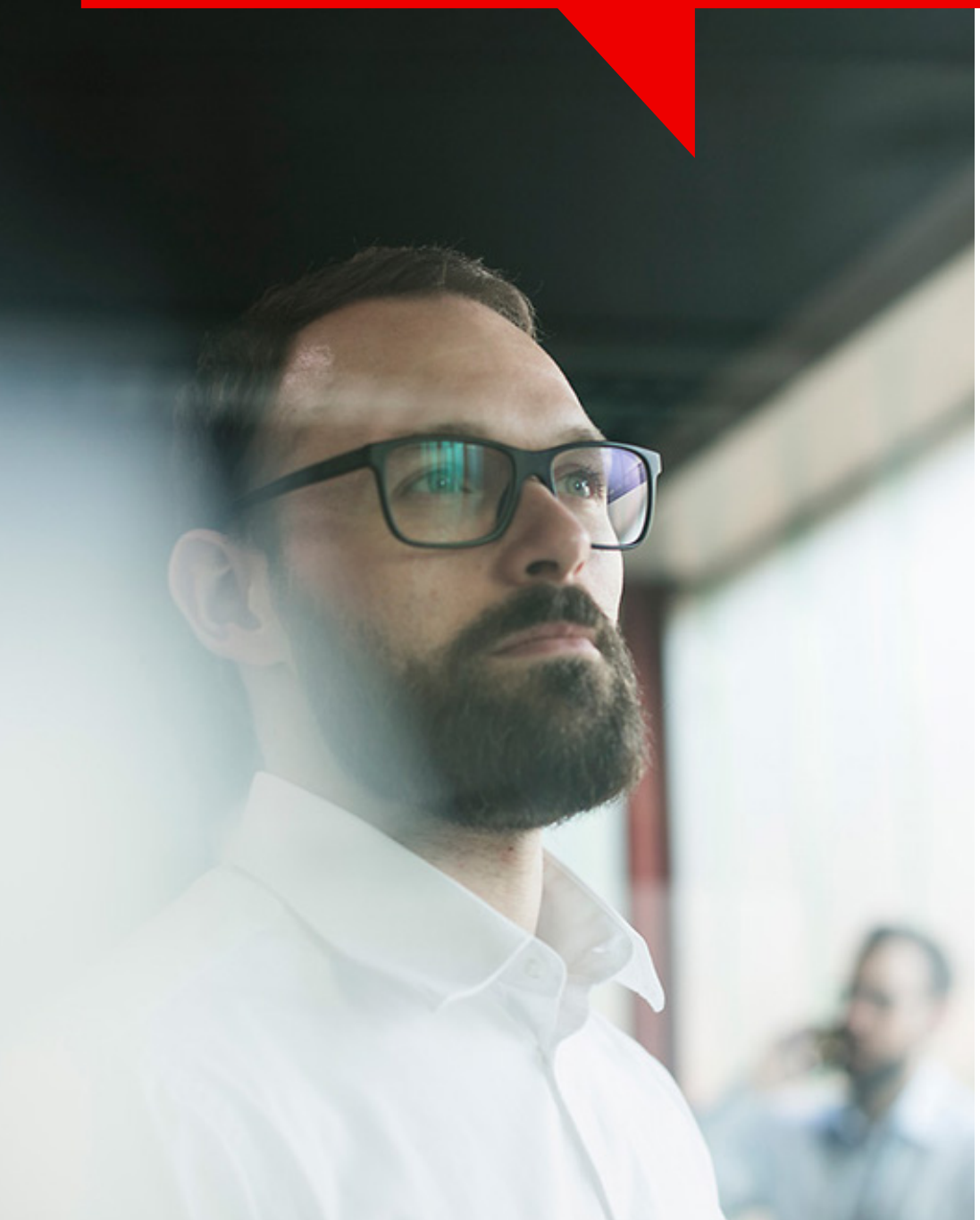
E-Mail: Gefühlt ist alles unter Kontrolle

Wie „funktionierende“ Systeme rechtliche, operative und strategische Abhängigkeiten verschleiern

Enterprise E-Mail Report 2026 — Souveränität



retarus

Inhaltsverzeichnis

Executive Summary

Für die Mehrheit der Unternehmen bleibt E-Mail ein wesentliches Element des täglichen Betriebsablaufs. Bestellungen, Rechnungen, Verträge, Benachrichtigungen: Tausende von Dateien reisen auf unsichtbaren Routen innerhalb und außerhalb der Organisation. Doch was dem Blick entgeht, entzieht sich auch der Kontrolle. Und genau hier entsteht das Risiko.

Eine aktuelle Umfrage von Researchscape im Auftrag von Retarus in Deutschland, Frankreich und Spanien zeigt, dass 80 % der Unternehmen glauben, ihre E-Mail-Ströme weitgehend unter Kontrolle zu haben [Hinweis: Sofern nicht anders angegeben, geben die Zahlen den Durschnitt über alle drei befragten Länder an]. Dennoch sind 45 % von außereuropäischen Anbietern abhängig, und 56 % befürchten, dass ihre Daten extraterritorialen Gesetzen wie dem US-amerikanischen CLOUD Act unterliegen. Diese Diskrepanz unterstreicht: Viele Unternehmen verwechseln Funktionieren mit Kontrollieren.

Tatsächlich wird die Kontrolle über E-Mail-Flüsse oft anhand sichtbarer Faktoren beurteilt: der Kontinuität des Datenaustauschs, der Stabilität der Systeme und dem Ausbleiben schwerwiegender Incidents. Dies ist jedoch nur die Spitze des Eisbergs und sagt leider nur wenig über den geltenden Rechtsrahmen, die Abhängigkeit von Anbietern außerhalb der Europäischen Union, ausreichende Datentransparenz oder die Einhaltung von Meldepflichten aus.

Angesichts regulatorischer Anforderungen wie NIS2 oder DORA reicht es nicht mehr aus, reine Sicherheitsmaßnahmen einzurichten. Unternehmen müssen nun auch deren Wirksamkeit nachweisen, die Umsetzung nachverfolgen und die Ergebnisse sorgfältig dokumentieren. Die Kontrolle geht damit über die Beherrschung der Infrastruktur hinaus. Laut der Umfrage halten 92 % der Unternehmen ein umfassendes und verwertbares Reporting für unverzichtbar. Souveränität ist keine ideologische Debatte mehr: 89 % der Befragten betrachten sie als strategisch wichtig, für 94 % ist sie ein entscheidendes Kriterium bei der Auswahl von Dienstleistern.

Sicherheit allein genügt nicht mehr. Man muss darüber hinaus handeln, Nachweise erbringen und die Kontrolle zurückgewinnen können. Dafür sind operative Aspekte entscheidend:

61 % der befragten Unternehmen geben an, ihre Richtlinien eigenständig umsetzen zu können.

61 %

Nur 49 % sagen aus, ihre Konten verwalten oder migrieren zu können, ohne von ihrem Dienstleister abhängig zu sein.

49 %

Diese Zahlen spiegeln eine konkrete Realität wider: Unternehmen sind nur bedingt unabhängig handlungsfähig. Das gilt sowohl für die Änderung von Einstellungen als auch für die Anpassung von Datenflüssen, um die Kontrolle über E-Mail zurückzugewinnen.

Der Grund ist einfach: Die Systemarchitekturen sind viel komplexer als früher. Die Daten fließen nicht mehr in einem einzigen System, sondern durch eine Vielzahl von Schichten: Cloud-Plattformen, Business-Applikationen, interne Tools, Dienste von Drittanbietern. Jeder einzelne Baustein für sich genommen funktioniert. Das Ganze wird jedoch schwieriger zu durchschauen, zu steuern und zu skalieren. Genau hier liegt die eigentliche Herausforderung. Eine Umgebung kann im Alltag stabil erscheinen und sich dennoch als starr erweisen, sobald sie angepasst, auditiert oder in ihrer Funktionsweise nachvollziehbar gemacht werden muss. Was oberflächlich beherrscht wirkt, hält einer realen Prüfung fast nie stand.

Kontrolle über E-Mail bedeutet heutzutage die Fähigkeit, Abläufe zu steuern, zu überprüfen und weiterzuentwickeln, ohne übermäßig von Dritten abhängig zu sein.

02

Datenflüsse lenken: Weg von der technischen Illusion

Die Kontrolle der Datenflüsse im Praxistest

Lange Zeit wurde Kontrolle vor allem an der technischen Stabilität gemessen: Solange die Datenflüsse funktionierten, klassische Filteralgorithmen ausreichten und Zwischenfälle selten waren, galt das System als unter Kontrolle. Eine technisch stabile Umgebung kann heutzutage jedoch andere Schwachstellen verbergen: unsichtbare Abhängigkeiten, rechtliche Zwänge oder mangelnde Reaktionsfähigkeit, sobald ein Eingreifen erforderlich ist.

Diese Diskrepanz in der Wahrnehmung ist kein Mangel an Wachsamkeit, sondern der Konzeption der Architekturen geschuldet. E-Mails durchlaufen eine Abfolge von Schichten in hybriden, übergreifenden Umgebungen: Cloud, Fachanwendungen, Sicherheitsbausteine, interne Tools, historisch gewachsene Sicherheitssysteme. Jeder Baustein für sich ist funktionsfähig. Das Ganze wird jedoch intransparenter, starrer und schwieriger in den Griff zu bekommen.

Die Kontrolle lässt sich nicht mehr allein anhand der Intuition beurteilen. Die Erwartungen der Unternehmen bestätigen dies:

92 %

halten es für wesentlich oder sehr wichtig, über ein umfassendes und verwertbares Reporting zu verfügen.

88 %

halten es für unerlässlich oder sehr wichtig, den E-Mail-Traffic über eigene Regeln aktiv zu steuern.

88 %

möchten ihre Dienste schrittweise bei einem europäischen Dienstleister bereitstellen können.

Ein System, das nur auf den ersten Blick funktionsfähig erscheint, genügt also nicht mehr. Man muss es auch kontrollieren und weiterentwickeln können.

Die Kontrolle spielt sich dabei auf drei Ebenen ab.

01 Rechtliche Kontrolle

Die erste wichtige Frage lautet: Welche Regeln gelten tatsächlich für Daten und Datenströme? Es reicht nicht mehr aus, die Daten in Europa zu hosten, um vollständig geschützt zu sein. Entscheidend sind der rechtliche Rahmen und Datenhoheit, dem der Anbieter unterliegt, sowie die Bedingungen, unter denen Dritte auf die Daten zugreifen können. Mit anderen Worten: Inwieweit bleiben die Daten geschützt – und unter welchen Umständen sind sie es nicht mehr?

02 Operative Kontrolle

Die zweite Frage, die man sich stellen muss, lautet: Wer lenkt die Datenströme? Wer legt die Regeln fest? Wer kann sie unabhängig von Dritten ändern? In fragmentierten Umgebungen liegt dies selten in einer Hand. Die Kontrolle ist verwässert, manchmal geteilt und oft eingeschränkt. Das Problem hierbei ist weniger die Verteilung selbst, sondern vielmehr ihre Auswirkungen. Wenn es ums Handeln geht, dauert alles länger, es entstehen Abhängigkeiten und der Handlungsspielraum schrumpft.

03 Aussagekräftiges Reporting

Die dritte wesentliche Frage lautet: Welche Daten stehen zur Verfügung? Sind sie schnell auswertbar? Geben sie präzise Antworten auf Fragen im Zusammenhang mit einem Audit, der Compliance oder einer Untersuchung? Transparenz hat nur dann einen Wert, wenn sie zuverlässige, verwertbare und gerichtsfeste Informationen liefert.

03

Die Souveränität wechselt die Seiten: vom Rechtlichen zum Strategischen

Souveränität wird zu einer operativen Herausforderung

Das Schlagwort „Souveränität“ hat seinen Charakter verändert in Richtung eines Handlungsspielraums, den es zu bewahren gilt. Souveränität spielt nun bei konkreten Abwägungen eine Rolle: Wahl des Dienstleisters, akzeptables Maß an Abhängigkeit, rechtliches Risiko, Vertragsbedingungen, Support sowie die Möglichkeit, gegebenenfalls den Anbieter zu wechseln.

Die Zahlen der Umfrage bestätigen dies:

94 %

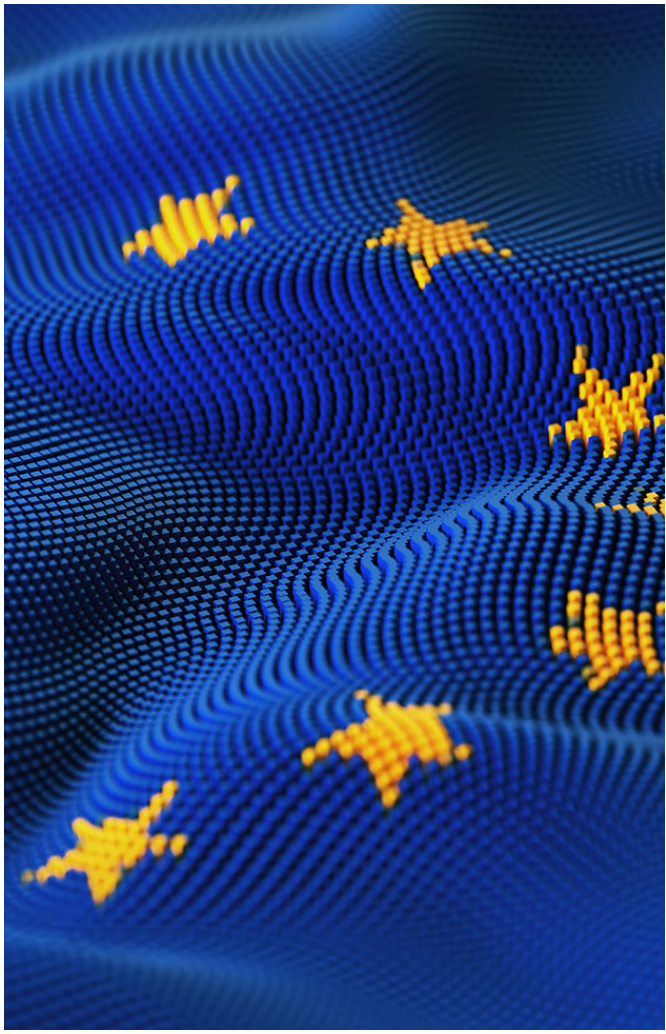
der Unternehmen geben an, dass Souveränität eine Schlüsselrolle bei der Auswahl von Dienstleistern spielt.

89 %

betrachten sie als strategische Priorität.

88 %

halten es für unerlässlich, dass ihr Dienstleister seinen rechtlichen Sitz in Europa hat.



Souveränität ist kein Buzzword mehr. Sie wird zunehmend zum strategischen Thema auf C-Level.

Erstens verschärft sich der regulatorische Rahmen: Mit NIS2 reicht es nicht mehr aus, die E-Mail-Infrastruktur technisch zu sichern. Unternehmen müssen ihre Entscheidungen begründen, ihre Praktiken nachverfolgen und ihre Maßnahmen kontinuierlich dokumentieren. Sprich man muss die Konformität im Falle eines Audits belegen können

Zweitens mischt der geopolitische Kontext die rechtlichen Karten neu. Das Risiko, unter extraterritoriale Gesetze zu fallen, ist sehr real. In Europa vorgehaltene Daten allein reichen nicht mehr aus, um sich sicher zu fühlen. Unternehmen wollen wissen, welche Regeln tatsächlich gelten – und welche Risiken bestehen, die Kontrolle über ihre Daten zu verlieren oder gar Opfer von Spionage zu werden.

Schließlich holt die operative Realität das theoretische Architektur-Setup immer häufiger ein. Je mehr Schichten sich auftürmen, desto größer werden die Abhängigkeiten. Schwer zu erreichende Dienstleister, starre Verträge, Fernsupport von außerhalb der EU: All dies sind Einschränkungen, die in ihrer Summe den Handlungsspielraum einschränken.

Souveränität wird zu einem konkreten Thema. Sie beschränkt sich nicht auf den Standort der Daten. Sie bezieht sich auf alles, was die tatsächliche Kontrolle über die Datenströme bedingt: die Unterwerfung unter ausländische Rechtsordnungen, der Spielraum bei Vertragsverhandlungen, die Abhängigkeit vom Dienstleister, die Qualität des Supports, die Fähigkeit, die Architektur weiterzuentwickeln, und letztendlich die Möglichkeit, mit echten Rückübertragungsklauseln wieder die Kontrolle zu übernehmen.

Dieser Paradigmenwechsel hat konkrete Auswirkungen für die Praxis:

Er bestimmt die architektonischen Entscheidungen, wobei modularere und weniger geschlossene Modelle bevorzugt werden.

Er gestaltet die Beziehung zu Dienstleistern neu, wobei den Vertragsbedingungen und der Reversibilität erhöhte Aufmerksamkeit geschenkt wird.

Schließlich beeinflusst er Investitionsentscheidungen, indem er Kriterien einführt, die über die reine technische Leistung hinausgehen.

Souveränität wird somit zu einem eigenständigen Entscheidungskriterium.

04

Nur Hosting in Europa reicht nicht mehr

Souveränität entscheidet sich nicht allein beim Hosting

Noch immer hält sich hartnäckig das Vorurteil, es reiche aus, seine Daten in Europa zu hosten, um die Kontrolle zu haben. Die Zahlen der Umfrage zeichnen hier ein ambivalentes Bild:

56 %

der Unternehmen halten es für wahrscheinlich, dass US-Gesetze den Zugriff auf ihre E-Mail-Daten erzwingen könnten.

45 %

nutzen trotzdem weiterhin Lösungen, die außerhalb Europas gehostet werden.

In Deutschland ist das Problembewusstsein bei diesem heiklen Thema übrigens signifikant höher als in Spanien und Frankreich, obwohl ausgerechnet französische Anwender aktuell noch deutlich mehr ihrer E-Mail-Services außerhalb Europas hosten.

Das Problem ist erkannt, die Gefahr aber mitnichten gebannt.

01 Der Mythos „in Europa gehostet“

Die weit verbreitete Annahme lautet: Wenn Daten in Europa gespeichert sind, sind sie automatisch geschützt. Die Realität ist jedoch viel komplizierter. Der Standort allein bestimmt nämlich nicht den geltenden Rechtsrahmen. So kann ein Anbieter durchaus Infrastrukturen in Europa betreiben und dennoch extraterritorialen Verpflichtungen unterliegen. Unternehmen wird diese Problematik zunehmend bewusst. Sie wird indes nach wie vor unterschätzt, und das reine Standort-Argument beeinflusst noch immer strategische Entscheidungen.

02 Das eigentliche Thema: die Gerichtsbarkeit

Die eigentliche Frage lautet: Welchen Vorschriften unterliegt der Dienstleister tatsächlich? Wer kann Zugriff auf die Daten beantragen? In welchem rechtlichen Rahmen? Mit welchen Auskunftspflichten? Es sind die konkreten Antworten auf diese Fragen, die das tatsächliche Schutzniveau bestimmen. Die rechtliche Kontrolle hängt nicht nur davon ab, wo die Daten gespeichert sind, sondern von den Gesetzen und Regularien, denen der Dienstleister unterliegt.

03 Garantien, die sich in der Praxis bewähren müssen

77 % der Organisationen geben an, über zertifizierte und überprüfbare vertragliche Garantien bezüglich des Speicherorts ihrer Daten, der Zugangsbedingungen und des geltenden Rechtsrahmens zu verfügen.

77 %

22 % räumen jedoch ein, dass diese Garantien nur teilweise greifen.

22 %

05

Die Kontrolle ist operativ stärker fragmentiert als es scheint

Mehr Schichten, weniger Kontrolle

In großen Organisationen sind E-Mail-Datenströme nicht linear. Sie durchlaufen ein immer dichter werdendes Netzwerk aus Standorten, Deployment-Modellen, Applikationen und Geräten. Je komplexer die Architektur, desto schwieriger wird es, die Kontrolle zu behalten.

Hier droht eine Schein-Kontrolle. Solange die E-Mail-Nachrichten fließen, gilt das System als unter Kontrolle. Ein ungestörter Datenfluss ist jedoch nicht zwangsläufig auch ein kontrollierter. Die Zahlen der Umfrage bestätigen dies:

Kurz gesagt: Es gibt zwar Autonomie, aber die stößt schnell an ihre Grenzen.

Das Problem ist erkannt, aber noch immer nicht gelöst.

01 Die Architektur ist immer komplexer als gedacht

In der Praxis nutzen eine Vielzahl von Systemen bevorzugt den Kommunikationskanal E-Mail: Cloud, ERP, CRM, interne Tools, Sicherheitslösungen, Archive, Altsysteme und zahlreiche Dienstleister. Diese Komplexität wächst mit der Zeit durch Projekte und Integrationen stetig an. Dazu kommen heute verstärkt automatisierte Datenströme aus Geschäftsanwendungen, die die Zahl der Schnittstellen und Abhängigkeiten nochmals vervielfachen.

Unternehmen unterschätzen gern die Anzahl der Anwendungen, die E-Mails versenden, und das Phänomen der „Schatten-IT“. Projekte zeigen fast immer dasselbe: mehr Datenströme, mehr Abhängigkeiten, mehr blinde Flecken als erwartet. Fusionen und Übernahmen verstärken diese Problematik noch. Jede Abteilung bringt ihre eigenen Tools, Regeln und Ausnahmen mit. Die Architektur wächst, ohne sich jedoch zwangsläufig zu vereinfachen.

02 Diffuse, aber sehr reale Abhängigkeiten

In diesem Umfeld geht die Kontrolle nicht verloren, sie zerfasert. Einige Komponenten werden intern verwaltet, andere stammen von Dienstleistern oder Drittanbietern. Doch hinter der scheinbaren Stabilität versteckt sich mitunter eine sehr konkrete Abhängigkeit. Diese tritt erst zutage, wenn es darauf ankommt: Unternehmen müssen eine Regel durchsetzen, einen Prozess anpassen, einen Bereich migrieren oder eine Ausnahme verwalten. Das dauert dann länger als erwartet, ist mit mehr Einschränkungen verbunden und hängt manchmal von Dritten ab.

03 Sehr konkrete Auswirkungen auf den Betrieb

Die Fragmentierung beschränkt sich nicht auf die IT. Sie hat sehr konkrete Auswirkungen aufs Business: längere Bearbeitungszeiten, verspätete Rechnungen, blockierte Bestellungen oder ein ausgebremster Kundensupport. Dazu kommt die Zeit, die die Teams für Überprüfungen, Nachfassaktionen und Korrekturen aufwenden müssen. Für sich genommen erscheint jedes dieser Ärgernisse geringfügig. In der Summe verursachen sie jedoch ständige Reibungsverluste mit entsprechenden und häufig versteckten Betriebskosten.

06

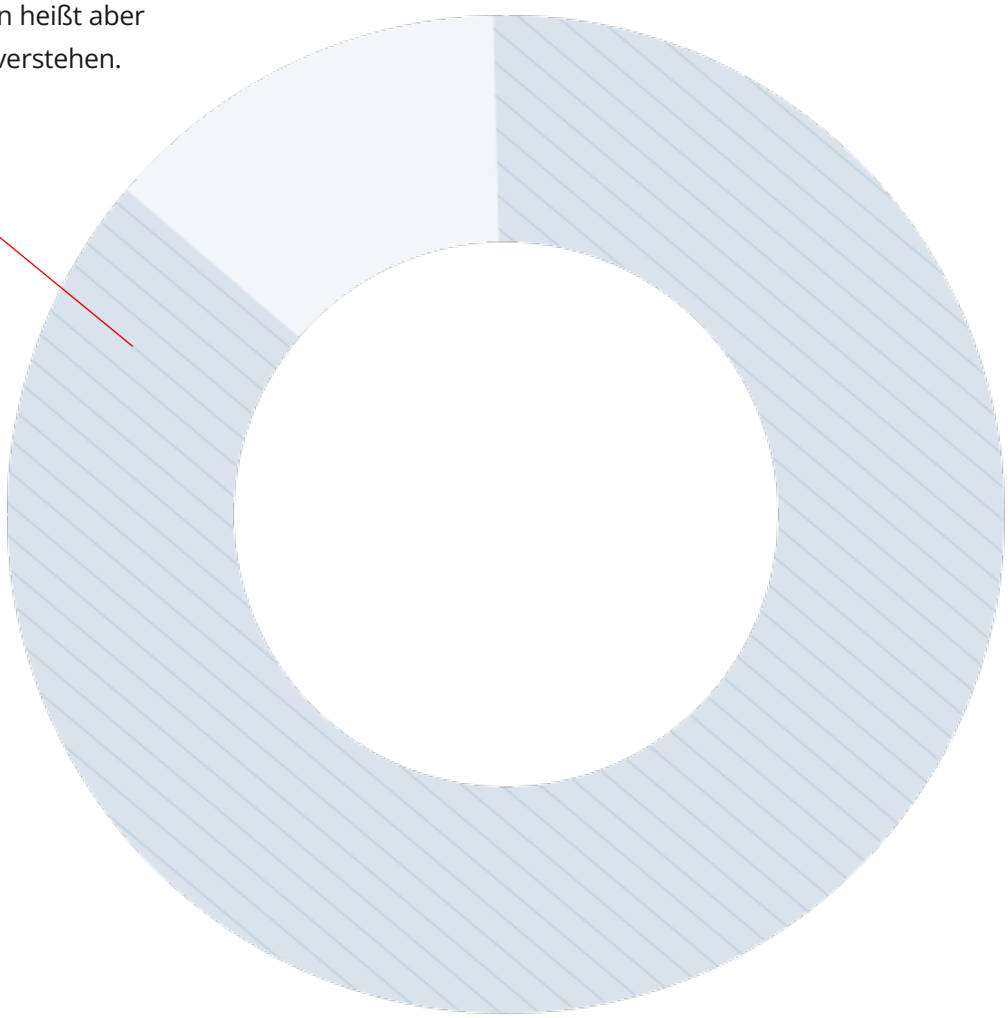
Transparenz, Berichterstattung, Nachweis: Stresstest für die Kontrolle

Sichtbarkeit informiert. Nachweise schaffen Vertrauen. Rückverfolgbarkeit schützt.

Transparenz schafft Klarheit. Nachweise geben Sicherheit. Rückverfolgbarkeit schützt. Dashboards, Kennzahlen und Indikatoren sind mittlerweile gesetzt.

92 %

der Unternehmen halten ein umfassendes und transparentes Berichtswesen für wesentlich oder sehr wichtig. Sehen heißt aber noch längst nicht auch verstehen.



01 Die Abläufe sichtbar zu machen reicht nicht mehr aus

Auch wenn die meisten Unternehmen heute glauben, ihre E-Mail-Flows anhand von Daten über versendete Volumina, Zustellraten, erkannte Vorfälle und Sicherheitswarnungen verfolgen zu können, ist dies in Wahrheit oftmals nur eingeschränkt möglich. Die Kennzahlen geben einen Überblick und ermöglichen es, Anomalien oder einen Anstieg des Datenverkehrs schnell zu erkennen. Doch ein Problem zu erkennen, heißt aber nicht, es auch zu lösen. Man muss überdies genau nachvollziehen können, was wann und auf welcher Ebene passiert ist – idealerweise für jede einzelne. Genau hier liegt der Unterschied zwischen dem bloßen Feststellen eines Vorfalls und der Fähigkeit, ihn zu erklären.

02 Die eigentliche Herausforderung: die Nachweisbarkeit

Der regulatorische Druck hinsichtlich der Compliance nimmt zu. NIS2, interne Kontrollen, Kundenaudits: Anfragen nach Datenzugriff werden immer häufiger. 52 % der Unternehmen geben an, dass sie drei- bis fünfmal pro Jahr auf ihre Daten zugreifen oder diese prüfen mussten.

In solchen Situationen lautet die Frage: Kann man schnell auf die Daten zugreifen, sie extrahieren, die Abläufe rekonstruieren, sie in ihren Kontext einordnen und verwertbare Erkenntnisse liefern? Ohne schnellen Zugriff, ohne klare Rückverfolgbarkeit und ohne die Möglichkeit, genau zu dokumentieren, was passiert ist, gibt es keine Transparenz.

03 Der Moment der Wahrheit: das Audit

Auf dem Papier existieren Kontroll- und Audit-Instrumente.

Allerdings geben nur

41 %

der Organisationen an, spontan ein Audit absolvieren zu können.

In den übrigen Fällen ist eine aufwendige Vorbereitung erforderlich: Daten müssen abgeglichen, Abläufe rekonstruiert und Informationen überprüft werden, um den Verpflichtungen nachkommen zu können. Konkret bedeutet dies, dass unter Termindruck kostbare Ressourcen darauf verwendet werden, eine E-Mail wiederzufinden, ihren Weg nachzuvollziehen und einen Vorfall zu erklären. Transparenz ist wertlos, wenn sie nicht zu verwertbaren Beweisen führt.

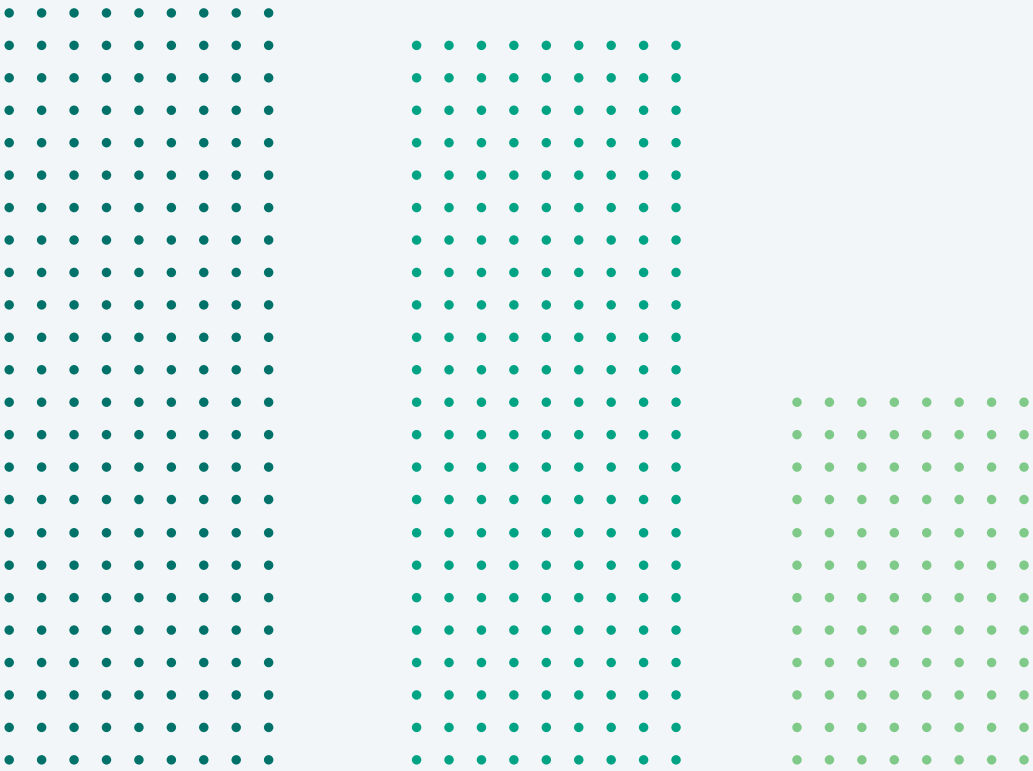
07

Lokaler Support: konkreter Ausdruck der Souveränität

Support wird zu einer Frage der Souveränität

Der Support ist nicht mehr nur ein einfaches Kriterium für die Servicequalität. Er wirkt sich direkt auf die Fähigkeit aus, einen Incident zu bewältigen, einen Prozess anzupassen oder eine schnelle Entscheidung zu treffen.

Die Umfragedaten sprechen dazu eine eindeutige Sprache:



84 %

der Unternehmen halten einen lokalen Support für unerlässlich oder sehr wichtig.

83 %

erwarten einen erreichbaren und reaktionsschnellen Dienstleister

46 %

und fast 46 % geben an, dass dieses Kriterium bei der Entscheidung für einen Anbieterwechsel eine Rolle spielen kann.

Für viele Unternehmen entscheidet sich die Souveränität auch genau hier, also in der Fähigkeit, schnell mit jemandem zu sprechen, der etwas tun kann und im wahrsten Sinne des Wortes die eigene Sprache spricht.

01 Wenn alles von der Reaktionszeit abhängt

Die Reaktionsfähigkeit wird erst dann sichtbar, wenn etwas schiefgeht. Solange alles reibungslos läuft, tritt sie in den Hintergrund. Doch sobald ein Prozess ins Stocken gerät, eine Konfiguration angepasst werden muss oder ein Zwischenfall eintritt, ist die Fähigkeit, einzugreifen, von entscheidender Bedeutung.

Wie lange dauert es in solchen Situationen, bis die Lage erfasst, eine Entscheidung getroffen und Abhilfe geschaffen ist? Wenn mehrere Hierarchieebenen, Teams oder Zeitzonen in eine Maßnahme involviert sind, verlängern sich die Wartezeiten. Die Auswirkungen sind nicht zu unterschätzen.

02 Im Falle eines Falles: alles eine Frage der Koordination

Störungen sind eher die Regel als die Ausnahme. Sie können auf jeder Ebene auftreten: Sicherheit, E-Mail, Geschäftsanwendungen, Dienste von Drittanbietern. Um die Ursache eines Problems zu identifizieren, muss man sich in diesem Labyrinth schnell zurechtfinden. Das Eingreifen wird zu einer Koordinationsaufgabe. Je mehr Zwischenstufen es gibt, desto langsamer die Lösung. Die entscheidende Frage lautet: Wer kann eingreifen, und wie schnell kann die Reaktion erfolgen?

03 Was im kritischen Moment wirklich zählt

Unternehmen erwarten von ihrem Dienstleister handfeste Lösungen:

- Sich an jemanden wenden zu können, der sich mit dem Thema auskennt.
- Eine Antwort zu erhalten, die schnell umsetzbar ist.
- Ein Hin und Her zu vermeiden, das die Lösung verzögert.

Werden diese Erwartungen erfüllt, lässt sich ein Vorfall eindämmen und die Kontinuität der Abläufe bleibt erhalten.

Lokaler Support ist kein Bonus-Feature. Er verhindert vielmehr, dass aus einem banalen Vorfall ein kostspieliges Problem wird.

08

Modularität oder Abhängigkeit: die falsche Freiheit von E-Mail Architekturen

Modularität garantiert keine Unabhängigkeit

Unternehmen wollen nicht immer alle Systeme auf einmal ersetzen. Sie möchten eventuell schrittweise vorgehen, entsprechend ihren Prioritäten und (budgetären) Möglichkeiten, ohne dabei die Kontrolle über ihre Umgebung zu verlieren. Die Umfragedaten bestätigen dies:

71 %

der Befragten halten es für einfach, Teile ihrer E-Mail Security zu ändern oder hinzuzufügen.

49 %

geben an, dass Unabhängigkeit oder Modularität ihre Entscheidung für einen Anbieterwechsel direkt beeinflusst.

88 %

halten es für wesentlich oder sehr wichtig, E-Mail-Dienste sukzessive bei europäischen Anbietern betreiben zu können.

76 %

der Unternehmen beschreiben ihre Umgebung als modular.

Modularität bedeutet jedoch nicht automatisch Unabhängigkeit. Die eigentliche Frage ist: Gibt Ihnen diese Modularität wirklich Freiheit – oder nur die Illusion davon?

01 Schritt für Schritt vorangehen, ohne alles umzukrempeln

Architekturen entwickeln sich heute schrittweise weiter. Bausteine werden hinzugefügt, Dienste aktiviert und neue Anwendungen angebunden. Diese Weiterentwicklungen müssen ohne Komplettaustausch oder irreversible Verpflichtung möglich sein. So ist eine Koexistenz mit bestehenden Systemen möglich, ebenso wie die schrittweise Integration neuer Dienste und die Anpassung an betriebliche Vorgaben und Möglichkeiten.

02 Modularität darf die Abhängigkeit nicht verstärken

Nicht alle Formen der Modularität sind gleichwertig. Bausteine hinzuzufügen ist eine Sache. Sie aber ersetzen, neu konfigurieren oder davon loskommen zu können, ist eine andere. Hier liegt der eigentliche Unterschied zwischen echter Flexibilität und einer nur vorgetäuschten.

03 Das wahre Risiko: ein vorgegebener Kurs

Vendor Lock-in entsteht nicht sofort mit der Vertragsunterzeichnung. Er kann sich auch mit der Zeit durch erzwungene Kompromisse, die gegenseitige Abhängigkeit der Bausteine, die Komplexität einer Migration sowie hohe Ausstiegskosten erst entwickeln.

Ab einer bestimmten Vertragsdauer und einem bestimmten Grad des Engagements wird der Kurs nicht mehr selbst bestimmt, sondern diktiert. Oft wird er durch technische Entwicklungen vorgegeben. Flexibilität hat nur dann einen Wert, wenn sie umkehrbar ist. Nur unter dieser Voraussetzung wird Modularität zu einem Kontrollinstrument und nicht zu einem Faktor der Abhängigkeit.

Modularität ohne Umkehrbarkeit ist verkappter Lock-in.

09

Warum Unternehmen ihren Anbieter wirklich wechseln

Die Wahl eines Dienstleisters wird zu einer Frage der Kontrolle.

Unternehmen werfen ihre E-Mail-Strategie nicht einfach für eine zusätzliche Funktion über den Haufen. Sie versuchen vielmehr, die Kontrolle zurückzugewinnen. Hier sind die wichtigsten Kriterien, die bei der Entscheidung eine Rolle spielen.

01 Souveränität und Rechtsprechung

Souveränität ist ein zentrales Kriterium. 94 % der Unternehmen geben an, dass sie die Wahl des Anbieters stark beeinflusst.

02 Expertise und lokaler Support

Die operative Nähe wird zu einem entscheidenden Faktor: 84 % der Unternehmen betrachten den lokalen Support als entscheidend oder sehr wichtig.

03 Transparenz, Reporting, Compliance, Nachweisfähigkeit

Bei Entscheidungen gewinnt die Fähigkeit, Abläufe zu verfolgen, zu verstehen und zu dokumentieren, zunehmend an Bedeutung.

65 %

der Unternehmen geben an, dass Compliance-Anforderungen oder der Zugang zu Audits ihre Entscheidung beeinflussen, den Dienstleister zu wechseln.

04 Modularität, Unabhängigkeit und Umkehrbarkeit

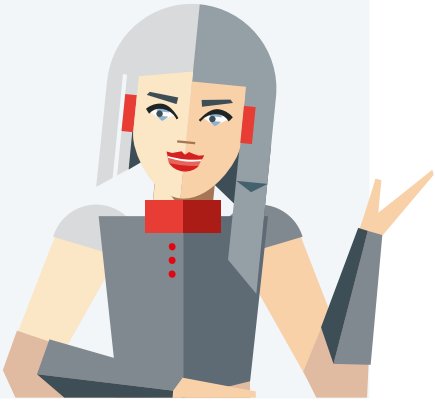
Flexibilität wird zu einem strategischen Kriterium:

49 %

der Unternehmen geben an, dass Modularität oder Unabhängigkeit vom Dienstleister ihre Entscheidung beeinflussen.

88 %

halten es zudem für wesentlich oder sehr wichtig, die Dienste schrittweise bei einem europäischen Anbieter integrieren zu können.



Unternehmen suchen nicht möglichst viele Optionen, sondern möchten sich weiterentwickeln können, ohne durch eine Architektur oder eine Lieferantenbeziehung festgelegt zu sein.

05 Eine implizite Hierarchie der Prioritäten

Bestimmte Kriterien treten bei der Auswahl einer Lösung deutlicher hervor. Reaktionsfähigkeit und Kontinuität unter lokaler Kontrolle sowie die regelgesteuerte Umsetzung von Richtlinien gehören zu den am höchsten bewerteten Kriterien (Durchschnittswert um 2,2). Die Priorität liegt also darauf, einen zuverlässigen, steuerbaren und langfristig konsistenten Betrieb zu gewährleisten.

Übrigens gibt es bei den Argumenten für den Umstieg auf eine souveräne E-Mail-Lösung interessante länderspezifische Unterschiede: Deutsche Anwender sind eher preissensitiv, legen aber weniger Wert auf lokalen Support und lokale Expertise. In Spanien ist es genau umgekehrt.

10

Benchmark: Haben Sie Ihre Datenflüsse unter Kontrolle?

In den meisten Organisationen funktionieren die E-Mail-Workflows im Großen und Ganzen. Die Nachrichten fließen, Störungen bleiben die Ausnahme und daran gewöhnen sich die Teams. Erst wenn sie eingreifen müssen, wird alles langsamer, undurchsichtiger und komplizierter.

Die Reibungspunkte bleiben oft diffus. Sie stellen zwar nicht den Gesamtbetrieb in Frage, summieren sich aber: verlorene Zeit, verzögerte Entscheidungen, falsch identifizierte Abhängigkeiten.

Meistens werden diese Friktionen erst mit Abstand sichtbar. Zum Beispiel, wenn man den eigenen Kontrollgrad mit dem von Organisationen gleicher Größe und aus derselben Branche vergleicht.

Dazu haben wir für Sie einen Benchmark programmiert, mit dem Sie den Kontrollgrad Ihrer Organisation bewerten und einordnen können. Das Tool finden Sie auf der Retarus-Website:

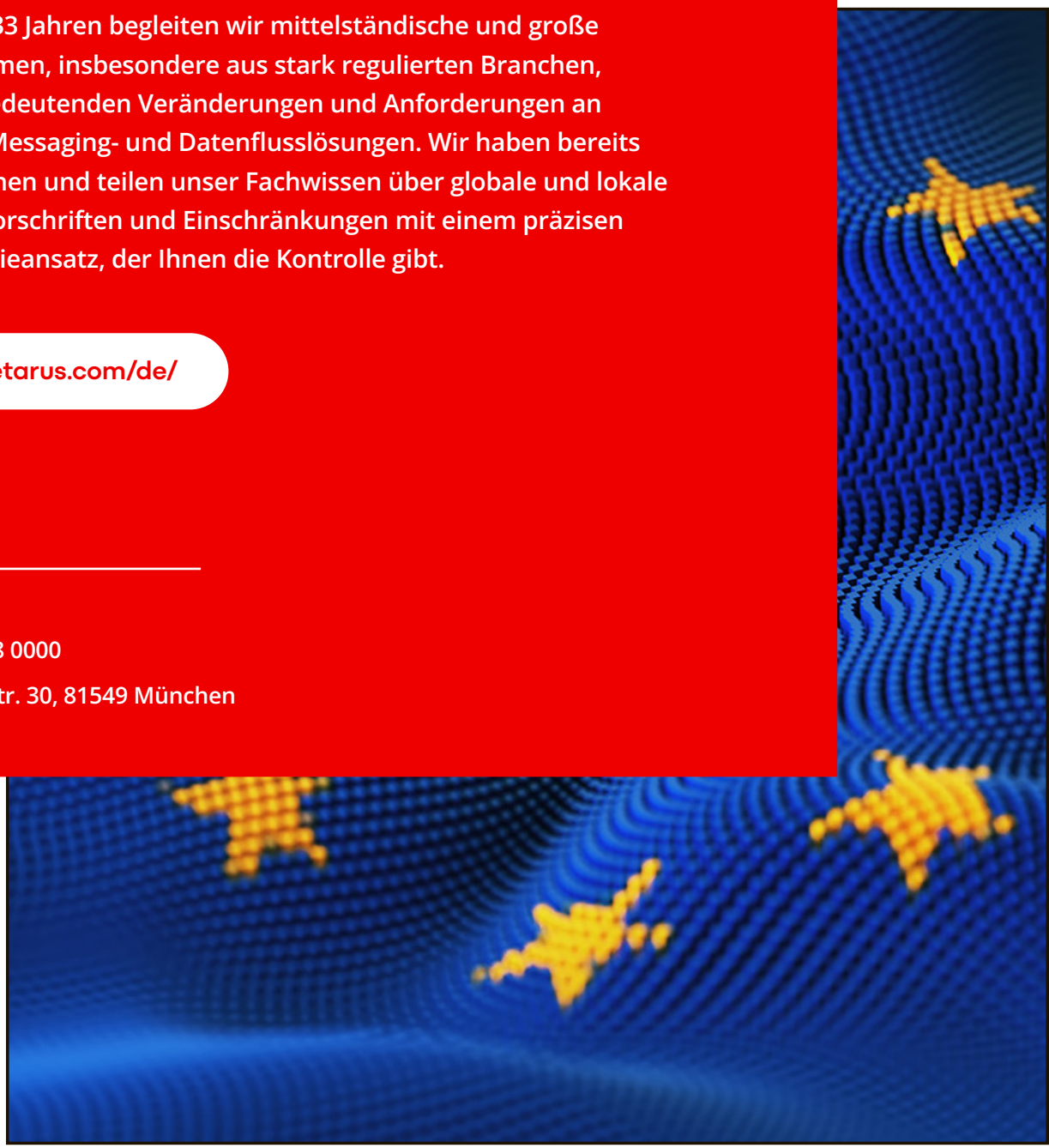
Jetzt Benchmark starten

Für Unternehmen ist jetzt der richtige Zeitpunkt gekommen, um wieder die Kontrolle über die kritischen Bausteine ihrer E-Mail-Infrastruktur zu übernehmen, Abhängigkeiten zu reduzieren und mit Partnern zu arbeiten, die sowohl rechtliche Transparenz als auch operative Kontrolle und Nachweisfähigkeit bieten. Genau das macht Retarus.

Retarus ist ein weltweit führender Anbieter für sichere Kommunikation.

Seit über 33 Jahren begleiten wir mittelständische und große Unternehmen, insbesondere aus stark regulierten Branchen, bei den bedeutenden Veränderungen und Anforderungen an kritische Messaging- und Datenflusslösungen. Wir haben bereits alles gesehen und teilen unser Fachwissen über globale und lokale Märkte, Vorschriften und Einschränkungen mit einem präzisen Technologieansatz, der Ihnen die Kontrolle gibt.

www.retarus.com/de/



+49 89 5528 0000

Aschauer Str. 30, 81549 München

retarus