Spoofing – unterschätzte Gefahr?

Der Einsatzgrad von DMARC in Deutschland und die Folgen erfolgreicher Spoofing-Angriffe für Unternehmen und ihre Marken

statista

mimecast

Inhaltsverzeichnis

Methoden der Datendiebe – Was ist Spoofing?

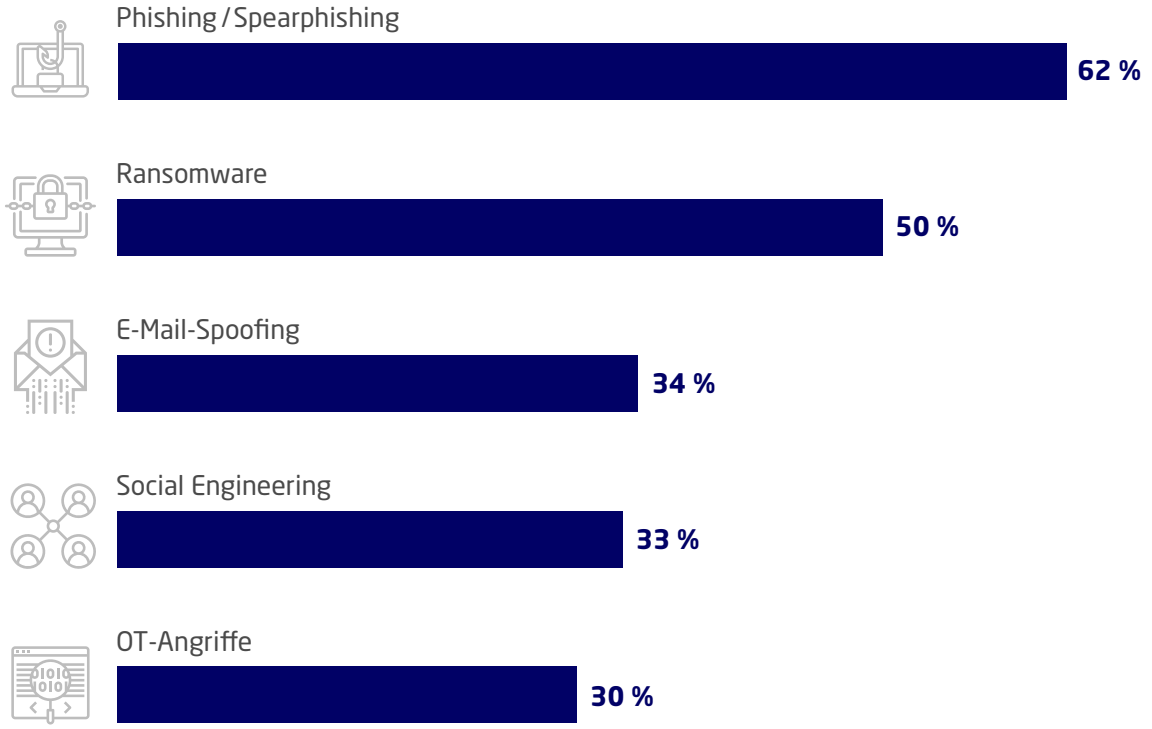
Identitätsmissbrauch vorbeugen und die Kontrolle über E-Mails und Domains behalten

Datenmissbrauch, Passwortdiebstahl, Malware – Unternehmen stehen mehr denn je im Fadenkreuz von Cyberkriminellen, die sensible Daten abgreifen oder schädliche Aktionen ausführen wollen. Fachleute zählen Spoofing zu den gefährlichsten Methoden der Datendiebe. Allgemein geläufig ist der Begriff bislang aber nicht. Wie funktioniert Spoofing und wie wird dagegen vorgegangen? Ein Beispiel:
Eine Person wird per E-Mail auf eine Bankseite geleitet und aufgefordert, ihre Anmeldedaten einzugeben. Sie folgt der Anweisung – ohne zu bemerken, dass sie Opfer eines Angriffs ist.
Ein Betrüger hat die E-Mail verschickt und eine gefälschte Webseite erstellt, die der echten täuschend ähnlich ist.

Spoofing, also das Vortäuschen einer seriösen Identität durch E-Mail- und Domain-Missbrauch, zählt nur jeder dritte IT-Entscheider zu den aktuell größten Cybergefahren – obwohl es oft schwer zu erkennen und für Kriminelle entsprechend erfolgsversprechend ist. Gelingt der Betrug, sind Vertrauensverluste von Kunden wahrscheinlich, die fatale Auswirkungen auf den Unternehmenserfolg haben können. Spezifische IT-Lösungen, insbesondere der E-Mail-Authentifizierungsstandard DMARC, können dies verhindern, wenn sie weitreichend implementiert werden.

Wie sensibilisiert sind deutsche Unternehmen für Spoofing? Wie verbreitet ist der Einsatz von DMARC? Dieses Whitepaper liefert Antworten.

Die Top 5 der größten Cybergefahren aus Sicht von IT-Entscheidern[1]

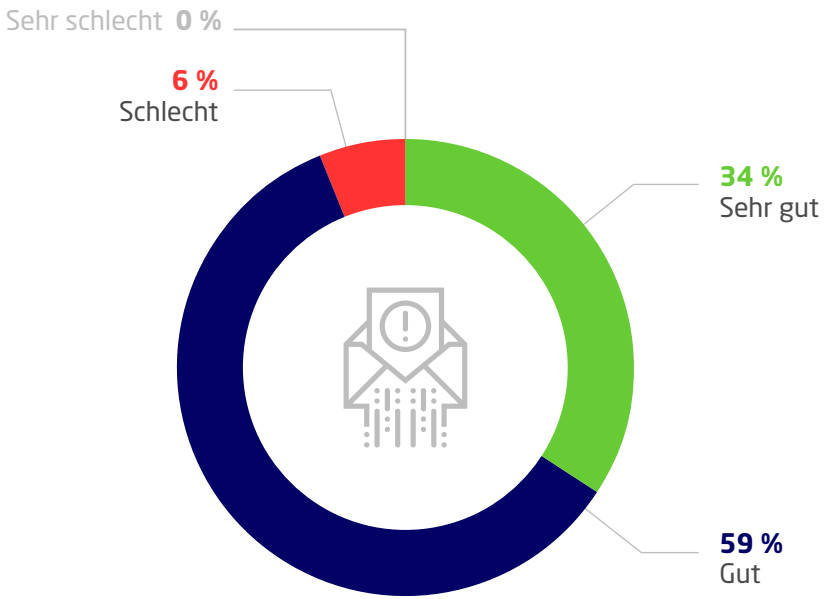


[1] Mehrfachnennungen möglich.
Quelle: Online-Befragung von Statista im Auftrag von Mimecast (2022)

Maßnahmen zum Schutz vor Spoofing

DMARC ist weit verbreitet – Fake-Webseiten werden trotzdem oft manuell recherchiert

Wie gut Unternehmen laut IT-Entscheidern gegen E-Mail-Spoofing geschützt sind



Wir haben 201 IT-Entscheider gefragt: IT-Lösungen, die gefälschte Webseiten regelmäßig aufspüren und melden, setzen nur 55 % der Unternehmen ein. Nahezu jedes zweite Unternehmen sucht regelmäßig zusätzlich oder sogar ausschließlich manuell nach Fake-Webseiten, um Domainmissbrauch zu bekämpfen und die eigene Marke zu schützen. Solche Recherchen sind in der Regel mit erheblichem Zeitaufwand verbunden und unterstreichen die Notwendigkeit, die die entsprechenden Unternehmen im Kampf gegen Domain-Spoofing sehen.

Den Schutz ihres Unternehmens gegen E-Mail-Spoofing bewertet eine überwältigende Mehrheit als gut oder sehr gut. In Unternehmen mit mehr als 10.000 Mitarbeitern gilt dies sogar ausnahmslos. Die Entscheider fühlen sich also sicher – nur die wenigsten bewerten den Schutz ihres Unternehmens als schlecht oder sehr schlecht. Etwas höher sind die Bedenken lediglich im Einzelhandel: Hier fühlt sich jeder fünfte IT-Entscheider schlecht gegen E-Mail-Spoofing geschützt.

Den DMARC-Standard nutzen etwa sieben von zehn Unternehmen, in Unternehmen mit 500 bis 999 und in solchen mit 10.000 und mehr Mitarbeitern ist DMARC am weitesten verbreitet.
Die Implementierung erfolgte insgesamt etwas häufiger intern als durch eine externe Lösung.

Welche Motive liegen dem Einsatz von DMARC zugrunde?

Quelle: Online-Befragung von Statista im Auftrag von Mimecast (2022)

Pull statt Push – Gründe für DMARC-Lösungen

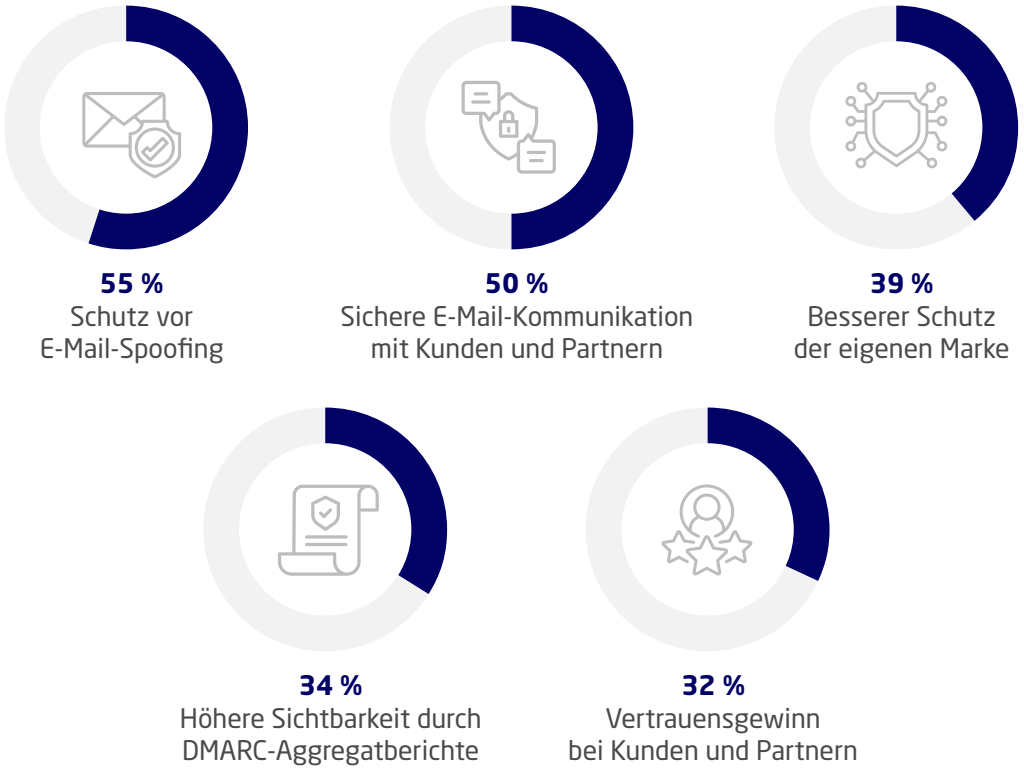
Über sichere E-Mail-Kommunikation zu Markenschutz und -vertrauen

Die Eigenperspektive der Unternehmen dominiert die Anwendungsentscheidung: Etwa zwei Drittel veranlassten interne Gründe zur Nutzung von DMARC. Dies gilt insbesondere für große Unternehmen. Nur in kleineren Unternehmen war der DMARC-Einsatz häufiger auch extern, z. B. durch Kunden, Partner oder Berater, motiviert. Innerhalb der Unternehmen heißt es: Spoofing-Abwehr ist Teamsport! Die Mehrheit der befragten IT-Entscheider sieht bei der Frage nach Schutzmaßnahmen eine Mitverantwortlichkeit anderer Bereiche, wie der Rechtsabteilung, der Kundenbetreuung oder des Marketings. Schließlich gilt auch bei einem erfolgreichen Cyber-Angriff: Mitgefangen, mitgehangen – Reputations- und Vertrauensverluste werden alle Abteilungen eines Unternehmens zu spüren bekommen.

Die Vorteile von DMARC-Aggregatberichten werden vergleichsweise selten gesehen – obwohl sie ein zentrales Feature von DMARC-Lösungen darstellen. Die Berichte ermöglichen eine Rückverfolgung von E-Mails, die im Namen des Unternehmens versandt wurden, und legen damit kriminelle Machenschaften offen, auf die das IT-Sicherheitspersonal nun einfacher und schneller reagieren kann. Für die befragten Führungskräfte ist DMARC v. a. ein Mittel zur Bekämpfung von E-Mail-Spoofing. Auf der Metaebene soll dies aber nicht nur die Kommunikation mit Kunden und Partnern, sondern auch die Marke selbst und das Markenvertrauen der Kunden schützen.

Was gilt dagegen für Unternehmen, die DMARC bislang nicht nutzen? Unterschätzen ihre IT-Entscheider das Spoofing-Risiko?

Die wichtigsten Vorteile beim Einsatz von DMARC-Lösungen[1]



[1] Mehrfachnennungen möglich.
Quelle: Online-Befragung von Statista im Auftrag von Mimecast (2022)

Unterschätzte Gefahr

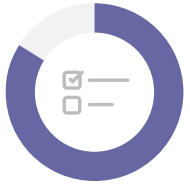
Unternehmen ohne DMARC priorisieren andere IT-Risiken – DMARC-Einsatz ist aber vielfach in Planung

Gründe, warum Unternehmen keine DMARC-Lösung einsetzen[1]

61 %
Andere IT-Sicherheitslösungen haben Priorität.

27 %
Die bekannten DMARC-Lösungen sind zu teuer.

20 %
Gefahr von E-Mail-Spoofing wird als gering erachtet.



84 %
aller Unternehmen ohne DMARC-Lösung planen eine Anschaffung.

30 %
aller Unternehmen ohne DMARC-Lösung planen eine Anschaffung in den nächsten 12 Monaten.

In Unternehmen, die DMARC nicht nutzen, wird die Gefahr von E-Mail- und Domain-Spoofing tatsächlich geringer eingeschätzt als in DMARC-nutzenden Unternehmen. Eine große Mehrheit der Entscheider sieht sich auch ohne DMARC-Lösung gut oder sogar sehr gut gegen Spoofing geschützt und priorisiert die Umsetzung von anderen IT-Sicherheitslösungen, etwa einem Viertel erscheinen zudem die Anschaffungskosten zu hoch. Bei einem Spoofing-Angriff können dies folgenschwere Fehleinschätzungen sein. Auch wenn 20 % der Befragten die Gefahr von E-Mail-Spoofing als gering erachten, würde im Ernstfall eine Vielzahl von Kunden das Markenvertrauen verlieren und sich der Konkurrenz zuwenden. Imageschäden und Umsatzeinbußen wären dann kaum abzuwenden.

Ein grundlegendes Bewusstsein über die Wichtigkeit und Wirksamkeit von DMARC scheint seitens der befragten IT-Entscheider dennoch zu bestehen: 84 % der IT-Entscheider in Unternehmen ohne DMARC-Lösung geben an, dass ein zukünftiger Einsatz geplant ist, fast jeder Dritte will bereits in den nächsten zwölf Monaten eine DMARC-Lösung implementieren. Besonders hoch wird die Dringlichkeit im höheren Mittelstand gesehen: In Unternehmen mit 1.000 bis 4.999 Mitarbeitern plant jeder zweite IT-Entscheider mit einer entsprechend zeitnahen Umsetzung. Auch branchenabhängig werden das Spoofing-Risiko und mögliche Folgen unterschiedlich beurteilt.

[1] Mehrfachnennungen möglich.
Quelle: Online-Befragung von Statista im Auftrag von Mimecast (2022)

Nutzung von DMARC-Lösungen im Branchenvergleich

Einzelhandel bei DMARC-Nutzung vorn, Automobilbranche Schlusslicht

Im Einzelhandel zählt jeder zweite IT-Entscheider E-Mail-Spoofing zu den aktuell größten Cybergefahren. In Bank- und Finanzdienstunternehmen sowie der Automobilindustrie sind es dagegen nur etwa jeder Dritte und im Health Care Bereich sogar nur jeder Fünfte. Im Einsatz von DMARC-Lösungen spiegelt sich dieser Unterschied teilweise wider.

Im Einzelhandel stehen gleich zwei große Sorgen im Fokus: Über die Hälfte der Entscheider befürchtet, dass Kunden infolge von Spoofing Opfer von Consumer-Phishing werden und das Markenvertrauen verlieren. Vertrauensverluste sind auch in der Automobilindustrie und im Health Care Bereich die größte Sorge. Banken und Finanzdienstleister befürchten dagegen vor allem Passwortdiebstähle. Unser einleitendes Beispiel hat verdeutlicht, wie einfach die Zugangsdaten ihrer Kunden durch Spoofing abgegriffen werden können.

Ausgewählte Branchen im Vergleich

Cybergefahren nach Branche[1]

Automobil und Fahrzeugbau

50 % Phishing / Spearphishing

42 % Ransomware, Social Engineering

Einzelhandel[2]

63 % Ransomware

50 % Phishing/Spearphishing, E-Mail-Spoofing, Social Engineering

Banken und Finanzdienstleistungen

86 % Phishing / Spearphishing

71 % Ransomware

43 % Social Engineering

Health Care[3]

60 % Phishing / Spearphishing

53 % Ransomware

20 % E-Mail-Spoofing, Domain-Spoofing, OT-Angriffe

Anteil der Unternehmen, die eine DMARC-Lösung nutzen

[1] Mehrfachnennungen möglich.
[2] inkl. Handwerk/einzelhandelsnahe Dienstleistungen, ohne Bekleidung
[3] z. B. Pharmazie, Krankenkassen, Krankenhäuser, Medizintechnik
Quelle: Online-Befragung von Statista im Auftrag von Mimecast (2022)

Handlungsmöglichkeiten für Unternehmen

Der Schutz vor Spoofing ist nicht nur eine Angelegenheit der IT-Abteilung

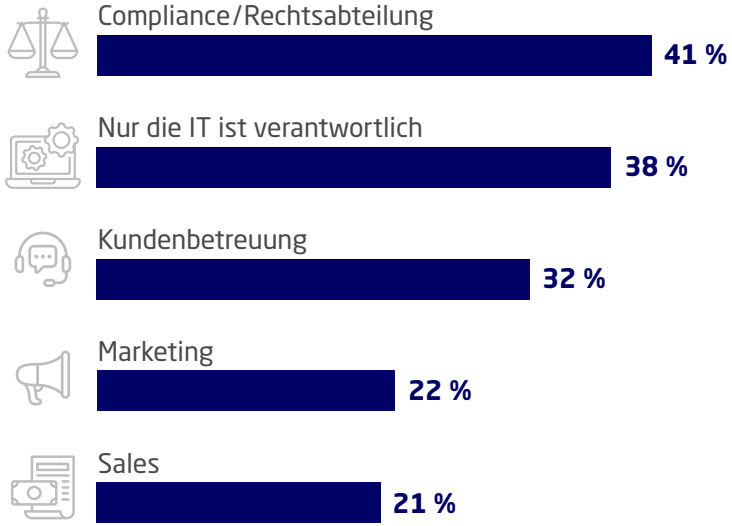
Von Cybersicherheit profitiert das gesamte Unternehmen – in vielen Unternehmen liegt die Verantwortung für den Schutz vor E-Mail- und Domain-Spoofing aber allein bei der IT-Abteilung. Der damit verbundene Markenschutz ist dagegen eine Aufgabe, zu der alle Abteilungen beitragen müssen. In diesem Sinne sieht die Mehrheit der befragten IT-Entscheider eine Mitverantwortlichkeit anderer Bereiche ihres Unternehmens, die ebenfalls unter den Folgen von Spoofing leiden, und erhoffen sich insbesondere Unterstützung der Rechtsabteilung, aber auch der Kundenbetreuung, des Marketings und des Vertriebs.

Fakt ist: Ein Unternehmen sollte als Ganzes zusammenarbeiten, um Identitätsmissbrauch zu verhindern! DMARC ist eine bewährte Lösung – eine erfolgreiche Implementierung kann den mit Fake-Webseiten und E-Mails verbundenen Arbeitsaufwand der ohnehin oft stark belasteten IT drastisch reduzieren. Eine klare Kommunikation über den Nutzen ist entscheidend, um alle Abteilungen von einem Einsatz zu überzeugen.

Nur etwa ein Drittel der Befragten zählt Spoofing zu den aktuell größten Cybergefahren. Noch alarmierender ist, dass sich fast alle gut oder sogar sehr gut gegen E-Mail-Spoofing geschützt fühlen – obwohl mehr als ein Viertel derjenigen, die sich (sehr) gut geschützt fühlen, noch keine DMARC-Lösung verwendet. Dass dies schwerwiegende Folgen nach sich ziehen kann, ist auch diesen IT-Entscheidern durchaus bewusst: Mehr als die Hälfte befürchtet Vertrauensverluste der Marke, mehr als ein Drittel ist besorgt, dass Kunden infolge von Spoofing Opfer eines Passwortdiebstahls werden. Dennoch priorisieren sie bislang mehrheitlich andere IT-Sicherheitslösungen. Großunternehmen setzen im Kampf gegen Spoofing aktuell am häufigsten auf DMARC-Lösungen – in kleinen und mittleren Unternehmen besteht noch Nachholbedarf!

Welche Abteilungen beim Thema Spoofing Mitverantwortung tragen[1]

62 %
der IT-Entscheider denken, dass beim Thema Spoofing andere Abteilungen mitverantwortlich sind.



[1] Mehrfachnennungen möglich.
Quelle: Online-Befragung von Statista im Auftrag von Mimecast (2022)

Methodik der Studie

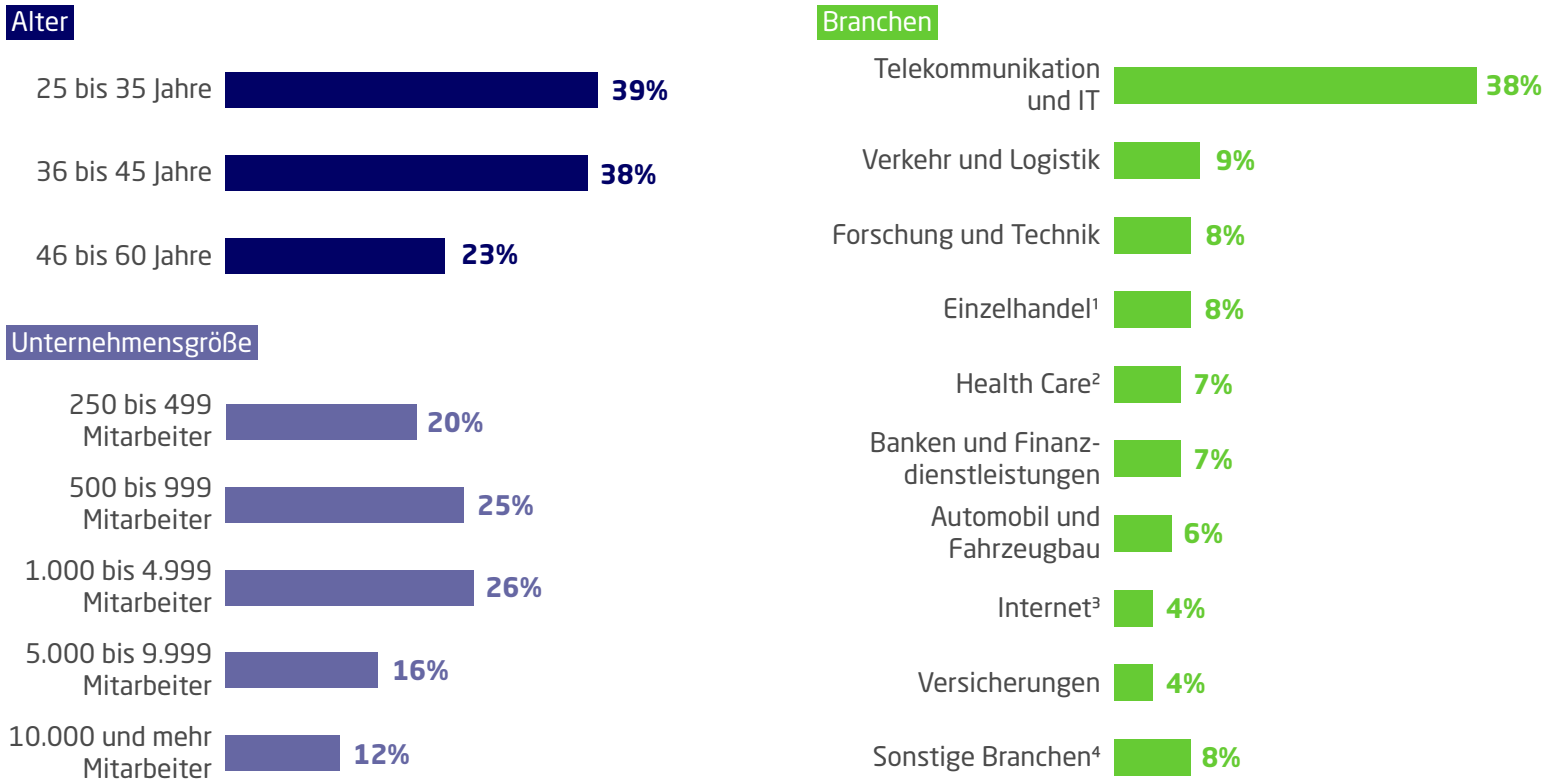
Umfrage zur Nutzung von DMARC-Lösungen

Im Auftrag vom Mimecast führte das Marktforschungsinstitut Statista im Februar 2022 eine deutschlandweite Umfrage durch. Insgesamt wurden 201 IT-Entscheider von Unternehmen ab 250 Mitarbeitern aus 13 Branchen befragt.

Ziel war es, zu verstehen, wie hoch die Gefahr von E-Mail-Spoofing und Domain-Spoofing von Führungskräften in Deutschland eingeschätzt wird und welche Schutzmaßnahmen in welchem Umfang bereits ergriffen werden.

Diese Studie soll außerdem aufzeigen, aus welchen Gründen Unternehmen DMARC-Lösungen einsetzen und wie sicher sie sich damit fühlen. Die Ergebnisse wurden dafür nach Branche und Unternehmensgröße ausgewertet.

Eckdaten zur Umfrage



¹ inkl. Handwerk/einzelhandelsnahe Dienstleistungen, ohne Bekleidung; ² z. B. Pharmazie, Krankenkassen, Krankenhäuser, Medizintechnik; ³ z. B. Infrastruktur, Portale, E-Commerce;
⁴ Dienstleistungen (Personal, Immobilien, Call-Center), Kundenberatung und -projekte, Agenturen, Kanzleien, Bekleidung, Schuhe, Sportausstattung (Herstellung und Handel) und Medien
Quelle: Online-Befragung von Statista im Auftrag von Mimecast (2022)

Impressum

Mimecast Germany GmbH
Kistlerhofstraße 172, 81379 München

Bernd Hohlweg, Director Marketing DACH
Telefon: +49 89 904 200 800
E-Mail: info@mimecast.com

Weiterführende Links:
www.mimecast.com/de/
www.mimecast.com/de/produkte/dmarc-analyzer/
www.mimecast.com/de/produkte/brand-exploit-protect/

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy.
From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.

mimecast