E-BOOK

DMARC als Schlüssel für die E-Mail-Zustellbarkeit

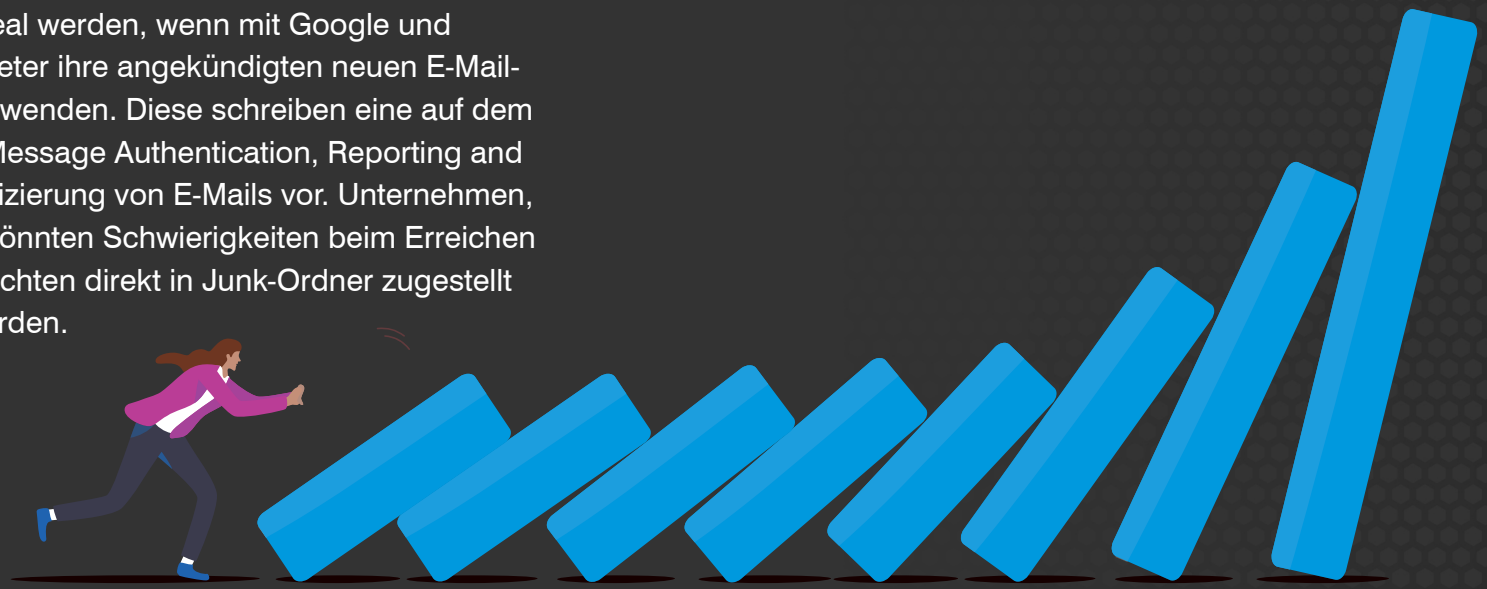
Warum E-Mail-Authentifizierung für das Erreichen von Interessenten, den Kontakt mit Kunden und den Schutz Ihrer Marke heute unverzichtbar ist

proofpoint.

Einleitung: Der Tag X für DMARC

Was wäre, wenn Ihre Kunden keine E-Mails mehr von Ihrem Unternehmen erhalten würden? Plötzlich stünde Ihr schnellster und effektivster Marketing-Kanal nicht mehr zur Verfügung. Kunden könnten nicht mehr ihre Identität verifizieren oder ihre Kennwörter zurücksetzen. Und Sie könnten keinen Kundendienst mehr bieten.

Dieses Szenario könnte bald sehr real werden, wenn mit Google und Yahoo zwei der größten E-Mail-Anbieter ihre angekündigten neuen E-Mail-Authentifizierungsanforderungen anwenden. Diese schreiben eine auf dem Standard DMARC (Domain-based Message Authentication, Reporting and Conformance) basierende Authentifizierung von E-Mails vor. Unternehmen, die diese Vorgabe nicht einhalten, könnten Schwierigkeiten beim Erreichen ihrer Kunden bekommen, da Nachrichten direkt in Junk-Ordner zugestellt oder direkt abgelehnt (blockiert) werden.



Das Ziel

In der heutigen Zeit gehört E-Mail zu den am häufigsten genutzten und effektivsten Kommunikationskanälen. Damit verbunden sind jedoch auch zahlreiche Herausforderungen und Bedrohungen, da Cyberkriminelle diesen Kanal für Phishing, Spoofing und Spam-Angriffe missbrauchen.

Wenn die Internetgiganten Gmail und Yahoo Mail von Versendern mit einem Versandvolumen von mehr als 5.000 E-Mails pro Tag die Implementierung von DMARC verlangen, schützen sie damit ihre Anwender vor schädlichen E-Mails, die vertrauenswürdige Absender oder Domains missbrauchen. Dabei geht es auch um betrügerische BEC-Angriffe (Business Email Compromise), die bei Unternehmen jedes Jahr Kosten in Milliardenhöhe verursachen. Mit dieser Initiative hoffen Gmail und Yahoo zudem, branchenweit bessere E-Mail-Prozesse und -Standards anzuregen. Dazu gehören einfache Möglichkeiten, sich aus E-Mail-Listen auszutragen, sowie der Versand von weniger E-Mails, um unterhalb des Spam-Schwellenwerts zu bleiben.

All diese Maßnahmen sollen die Zahl unerwünschter und betrügerischer E-Mails reduzieren, die die Postfächer von Anwendern verstopfen und das Vertrauen in E-Mails beeinträchtigen.

Die Herausforderung

Die korrekte Einrichtung von DMARC ist jedoch keine einfache Aufgabe. Dazu müssen die DNS-Datensätze (Domain Name System) sorgfältig konfiguriert und überwacht, die Identifikatoren für Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) abgestimmt, die verschiedenen DMARC-Richtlinien getestet und DMARC-Berichte analysiert werden.

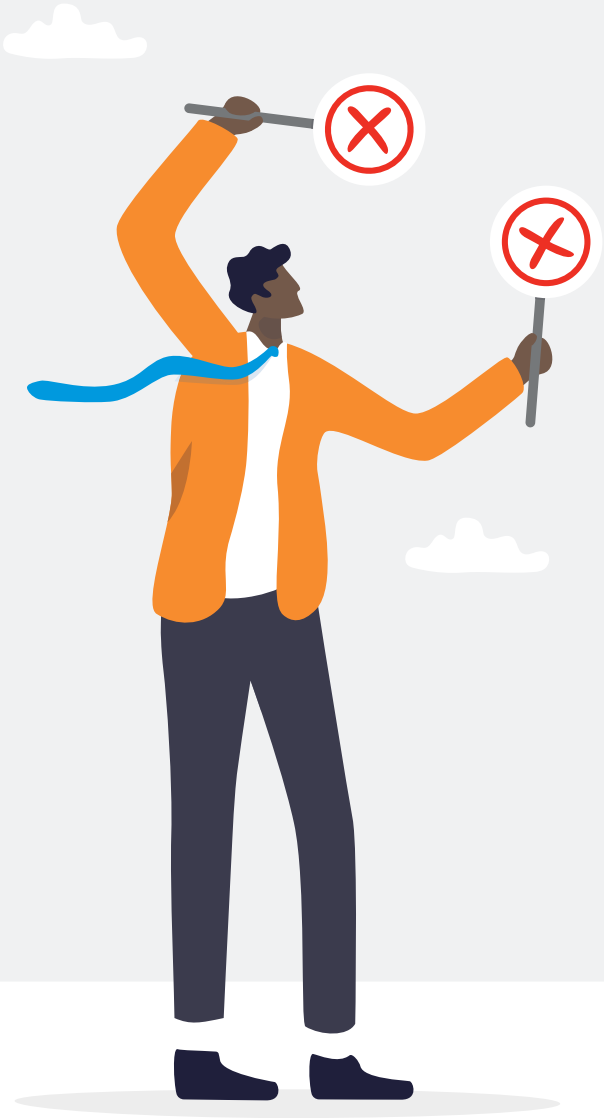
Andernfalls könnten legitime E-Mails blockiert oder als Spam eingestuft werden, wodurch die Zustellbarkeit und die Leistung beeinträchtigt werden. Deshalb müssen Unternehmen, die von E-Mail-Kommunikation abhängig sind, die Vorteile und Herausforderungen von DMARC verstehen und wissen, wie sie den Standard vor dem Inkrafttreten der neuen Anforderungen ordnungsgemäß implementieren können.

In diesem E-Book erfahren Sie, wie DMARC funktioniert und welche Auswirkungen DMARC auf die Zustellbarkeit von E-Mails hat. Außerdem erhalten Sie Hinweise zu empfohlenen Vorgehensweisen und zu Schritten, mit denen Sie optimale DMARC-Ergebnisse erzielen können.

ABSCHNITT 1

E-Mails sind für Unternehmen geschäftskritisch

In der heutigen schnelllebigen Welt sind E-Mails zum Lebenselixier der modernen Wirtschaft geworden. Die Aussage, dass der reibungslose Ablauf moderner Unternehmen von ihnen abhängt, ist noch eine Untertreibung. Fakt ist: E-Mails werden in fast allen Bereichen täglich millionenfach eingesetzt – von Marketing-Strategien bis zum Kundendienst.



Ein unverzichtbares Marketing-Tool

Marketing-Teams setzen bei der Kommunikation ihrer Kampagnen stark auf E-Mails, um Angebote, Neuigkeiten und Content an potenzielle und bestehende Kunden zu senden und so Interaktionen mit der Marke sowie die Umsatzzahlen zu fördern.

Ein Kanal für Transaktionskommunikation

Für Kunden ist es wichtig, per E-Mail Kennwörter zurücksetzen oder einmalige Zugangscodes erhalten zu können. Ohne diese Transaktions-E-Mails könnten sie nicht auf Services zugreifen oder mit Ihrem Unternehmen ins Geschäft kommen.

Ein wichtiges Tool für den Kundendienst

Das Anwendererlebnis nach einem Kauf wird mit Bestellbestätigungen, digitalen Kaufbelegen und Follow-up-Umfragen erheblich verbessert. Dafür werden E-Mails verwendet. Und diese E-Mails werden nicht nur erwartet, sondern gelten als grundlegender Kundendienst.

Und heute eines der häufigsten Ziele

Ohne vertrauenswürdige E-Mails kommen viele Geschäftsabläufe zum Erliegen. Leider sind E-Mails heute auch ein primäres Ziel von Cyberkriminellen, die Ihre Domain missbrauchen und das Vertrauen Ihrer Anwender ausnutzen wollen.

ABSCHNITT 2

Warum DMARC?

Eine der häufigsten und gleichzeitig kostspieligsten Formen von E-Mail-Betrug ist Business Email Compromise (BEC). (Bei diesen Angriffen ahmen Betrüger mithilfe gefälschter oder Doppelgänger-E-Mail-Adressen vertrauenswürdige Absender nach.) Laut FBI haben BEC-Angriffe auf Unternehmen von 2013 bis 2022 Kosten in Höhe von 51 Milliarden US-Dollar verursacht.[1] Zudem haben Untersuchungen von Proofpoint ergeben, dass 2022 mehr als 75 % aller Unternehmen mindestens einen BEC-Versuch verzeichnet haben.[2]

Da E-Mail-Betrug zu einer stark wachsenden Bedrohung wurde, einigten sich 20 Unternehmen (darunter Google, Yahoo, Microsoft und Facebook) im Jahr 2012 gemeinsam auf den DMARC-Standard. Dieses offene E-Mail-Authentifizierungsprotokoll ermöglicht den Domain-basierten Schutz von E-Mails. Es baut auf den bestehenden Standards SPF und DKIM auf, mit denen die Identität des Absenders und die Integrität der E-Mail-Nachricht verifiziert werden können.

1 FBI: „Business Email Compromise: The 50 $ Billion Scam“ (Business Email Compromise: Der 50-Milliarden-Dollar-Betrug), Juni 2023.
2 Proofpoint: „State of the Phish“, März 2023.

51 Mrd. US-Dollar

kostete BEC-Betrug Unternehmen von 2013 bis 2022.

Mehr als 75 %

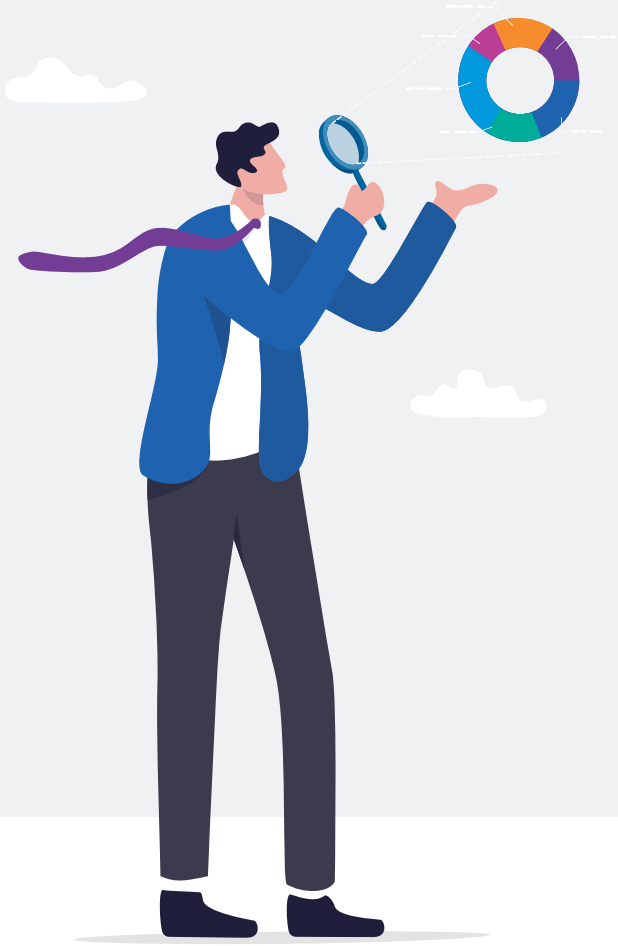
aller Unternehmen verzeichneten im Jahr 2022 mindestens einen BEC-Versuch.

Dies sind die wichtigsten Funktionen und Vorteile von SPF, DKIM und DMARC:

	Beschreibung	Vorteil
SPF	Ein DNS-Datensatz, mit dem festgelegt wird, welche IP-Adressen berechtigt sind, E-Mails von einer Domain zu senden.	Verhindert die nicht autorisierte Nutzung einer Domain durch Spammer oder Betrüger.
DKIM	Eine digitale Signatur im E-Mail-Header, mit der nachgewiesen wird, dass die Nachricht vom Domain-Inhaber gesendet und während der Übertragung nicht manipuliert wurde.	Gewährleistet die Authentizität und Integrität der E-Mail-Nachricht.
DMARC	Ein DNS-Datensatz, der definiert, wie Ergebnisse von SPF- und DKIM-Prüfungen interpretiert werden sollen und wie vorgegangen werden soll, wenn eine E-Mail die Authentifizierungsprüfungen nicht besteht.	Ermöglicht Domain-Inhabern die Überwachung und Kontrolle der Domain-Nutzung für die E-Mail-Kommunikation.

Das DMARC-Protokoll ist die erste und einzige weit verbreitete Technologie, bei der der in E-Mail-Clients angezeigte Absender (die From-Zeile im Header) geprüft wird. Dadurch können sich die Anwender darauf verlassen, dass er vertrauenswürdig ist. Durch die Verwendung von DMARC können Domain-Inhaber verhindern, dass ihre Domains für Phishing- oder Spoofing-Angriffe gegen Kunden, Mitarbeiter und Partner missbraucht werden können.

Die Implementierung war bisher jedoch ein langsamer und wenig geradliniger Prozess. Um die Einführung von DMARC zu beschleunigen und die E-Mail-Sicherheit zu verbessern, gaben Google und Yahoo Ende 2023 bekannt, dass E-Mails blockiert oder direkt in den Junk-Ordner von Anwendern zugestellt werden können, wenn sie bestimmte SPF-, DKIM- und DMARC-Standards nicht einhalten. Die Standards werden besonders strikt bei Versendern angewendet, die pro Tag mehr als 5.000 E-Mails an Gmail- und Yahoo Mail-Adressen senden.



Zusätzlich zu diesen marktbasierten Anreizen gibt es auch neue Vorschriften, die den Druck zur Implementierung von DMARC erhöhen. PCI DSS v4.0 schreibt ab Anfang 2025 Phishing-Schutzmaßnahmen vor. Das bedeutet, dass Unternehmensaudits möglicherweise nicht bestanden werden, wenn DMARC nicht implementiert ist.

Regionale Gesetze erhöhen die Bedeutung von DMARC-Compliance zusätzlich. So wird in Japan mit den Unified Standards for Cyber Security Measures for Government Agencies zum Beispiel festgelegt, dass alle staatlichen Stellen ab Juli 2024 eine DMARC-Richtlinie zur E-Mail-Ablehnung oder -Isolierung einrichten müssen. Gleichzeitig drängen japanische Behörden alle Kreditkartenunternehmen, ab Februar 2024 eine solche Richtlinie einzurichten.

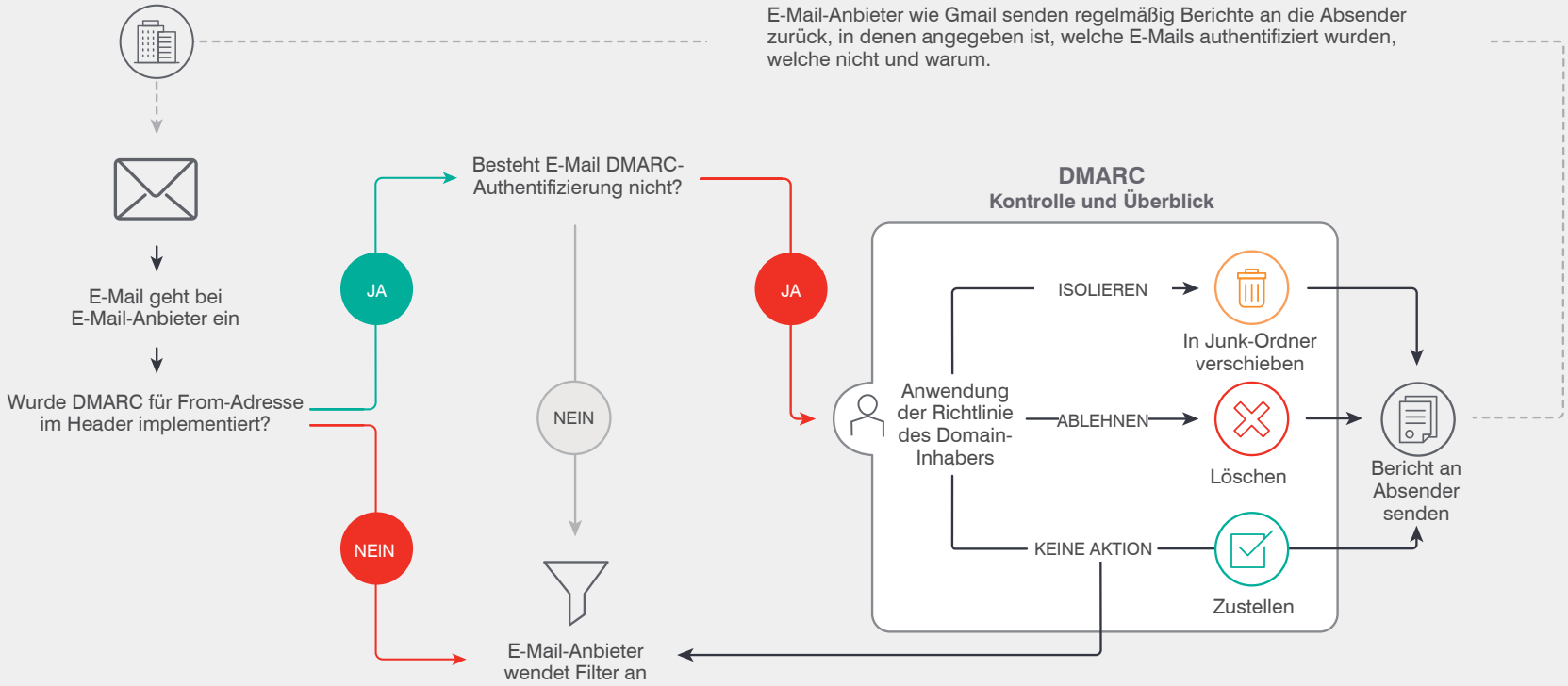
Funktionsweise von DMARC

Alle Unternehmen, die E-Mail als zentralen Kommunikationskanal verwenden, müssen DMARC verstehen und wissen, wie dieser Standard ordnungsgemäß implementiert wird.

DMARC authentifiziert legitime E-Mails für ihre Versand-Domains, indem geprüft wird, ob die E-Mail-Nachricht die zwei bestehenden Standards SPF und DKIM besteht.

SPF verifiziert, dass die E-Mail-Nachricht von einer IP-Adresse gesendet wurde, die vom Domain-Inhaber autorisiert wurde. DKIM verifiziert, dass die E-Mail-Nachricht über eine gültige digitale Signatur verfügt, die mit dem öffentlichen Schlüssel des Domain-Inhabers übereinstimmt.

Wenn eine dieser Prüfungen fehlschlägt, wird die E-Mail-Nachricht als nicht authentifiziert und damit als potenziell betrügerisch eingestuft.


E-Mail-Anbieter wie Gmail senden regelmäßig Berichte an die Absender zurück, in denen angegeben ist, welche E-Mails authentifiziert wurden, welche nicht und warum.
E-Mail geht bei E-Mail-Anbieter ein
Wurde DMARC für From-Adresse im Header implementiert?
JA
NEIN
Besteht E-Mail DMARC-Authentifizierung nicht?
JA
NEIN
E-Mail-Anbieter wendet Filter an
DMARC
Kontrolle und Überblick
Anwendung der Richtlinie des Domain-Inhabers
ISOLIEREN
In Junk-Ordner verschieben
ABLEHNEN
Löschen
KEINE AKTION
Zustellen
Bericht an Absender senden

Mit einer expliziten Richtlinieneinstellung weist DMARC die E-Mail-Anbieter an, wie mit Nachrichten umzugehen ist, die die Authentifizierung nicht bestehen. Diese Nachrichten können entweder in einen Junk-Ordner verschoben oder direkt abgelehnt werden. Die Richtlinieneinstellung bietet drei Optionen:

- **None (Keine Aktion):** Bei nicht authentifizierten Nachrichten werden keine Aktionen durchgeführt. Der Domain-Inhaber kann weiterhin Berichte darüber erhalten, wie die eigene Domain bei E-Mails verwendet wird.
- **Quarantine (Isolieren):** Nicht authentifizierte Nachrichten werden als Spam eingestuft und an einen Junk-Ordner verschoben. Die Empfänger können sich Spam-Nachrichten ansehen, tun es aber selten.
- **Reject (Ablehnen):** Nicht authentifizierte Nachrichten werden blockiert und als nicht zustellbar an den Absender zurückgesendet (Bounce-E-Mail). Der Empfänger bekommt diese Nachricht gar nicht erst zu sehen.

ABSCHNITT 3

Die Vorteile von DMARC

Für Unternehmen, die E-Mail als zentralen Kommunikationskanal verwenden, bietet DMARC zahlreiche Vorteile. Nachfolgend werden einige davon erläutert.

Bessere Zustellbarkeit und stärkere Nutzung von E-Mails

Da DMARC gewährleistet, dass nur legitime und authentifizierte E-Mails von Ihrer Domain den Posteingang der Empfänger erreichen, sinkt die Wahrscheinlichkeit, dass Ihre E-Mails als Spam eingestuft oder von E-Mail-Anbietern herausgefiltert werden. Dadurch verbessert sich die Reputation und Leistung Ihrer E-Mails erheblich. Außerdem erhöht sich die Wahrscheinlichkeit, dass Ihre E-Mails geöffnet und gelesen werden und dass Ihre Zielgruppe darauf reagiert.

Dieser Vorteil ist für Transaktions-E-Mails besonders wichtig, da er gewährleistet, dass Ihre Geschäftsabläufe nicht durch E-Mails gestört werden, die nicht oder mit nur geringer Priorität übertragen werden.

Schutz für Mitarbeiter, Geschäftspartner, Kunden und Marken

DMARC ermöglicht die Blockierung einer ganzen Klasse betrügerischer E-Mails, bevor diese in den Postfächern Ihrer Mitarbeiter, Partner und Kunden eingehen. Dadurch werden Phishing- und Spoofing-Angriffe verhindert, die Ihre Domain nutzen, um E-Mail-Empfänger zu täuschen oder Schaden zu verursachen. Auf diese Weise erhöht DMARC nicht nur das Vertrauen in Ihre Marke und die Loyalität, sondern reduziert zudem das Risiko von Datenschutzverletzungen, finanziellen Verlusten und anderen rechtlichen Problemen.

Einblick in die E-Mail-Bedrohungslandschaft

Was Sie nicht sehen, können Sie auch nicht kontrollieren! Durch die Implementierung von DMARC erhalten Sie einen sofortigen Überblick über Bedrohungen, die sich gegen Ihr Unternehmen richten. Sie erhalten Informationen zu Domain-Phishing- und -Spoofing-Angriffen, die Ihre Kunden und den Ruf Ihrer Marke gefährden. Dank der regelmäßigen Berichte zu den Quellen und Mengen der nicht authentifizierten E-Mails, die Ihre Domain missbrauchen, können Sie Risiken durch potenzielle Schwachstellen und kriminelle Akteure identifizieren und beheben.

Geringere Kosten für den Kundendienst

Durch die Blockierung betrügerischer E-Mails, die Ihre Domain nachahmen, reduziert DMARC die Anzahl der Kundenbeschwerden und Anfragen, mit denen Sie sich befassen müssen. Dadurch sparen Sie Zeit und Geld aufseiten des Kundendienstes und verbessern gleichzeitig die Kundenzufriedenheit und -bindung.

Geringere Kosten für die Reaktion auf Phishing

Laut dem vom FBI geführten Internet Crime Complaint Center (IC3) betrugen die Phishing-Kosten für Marken im Jahr 2021 etwa 6,9 Milliarden US-Dollar.[3] DMARC verringert die Kosten, die durch Betrug, Rückerstattungen und die Reaktion auf Phishing-Angriffe entstehen. Mit DMARC verhindern Sie BEC-Angriffe, die gefälschte E-Mail-Adressen nutzen, um Ihre Mitarbeiter und Partner zum Überweisen von Geldern oder Weitergeben sensibler Informationen zu verleiten. Dadurch verhindern Sie Finanz- und Rufschäden, die durch diese Betrugstaktiken verursacht werden.

3. FBI: „Internet Crime Report 2021“ (Bericht zu Internetkriminalität 2021), April 2022.

ABSCHNITT 4

Zuverlässige Zustellung Ihrer E-Mails in den Posteingang der Kunden gewährleisten

Viele Faktoren entscheiden darüber, ob Ihre E-Mails in den Posteingang oder den Junk-Ordner zugestellt werden. Nachfolgend nennen wir einige Mindestanforderungen, mit denen Sie gewährleisten können, dass Ihre geschäftskritischen E-Mails nicht im Junk-Ordner landen.

Eingerichtete DMARC-Richtlinie

Eine eingerichtete DMARC-Richtlinie bedeutet immer auch, dass SPF- oder DKIM-Authentifizierungsmethoden implementiert sein müssen. Damit Ihre E-Mails die DMARC-Prüfung bestehen, muss der „From“-Header mit der SPF-Domain oder der DKIM-Domain übereinstimmen. (Mit anderen Worten: Ihr Header muss mit der Domain Ihres Unternehmens übereinstimmen bzw. dieselbe Domain verwenden.) Außerdem dürfen Sie Gmail nicht im „From“-Header nachahmen, d. h. alle E-Mails, die vorgeben, von Gmail zu stammen, werden automatisch als Spam eingestuft oder abgelehnt.

Gültige Forward/Reverse-DNS-Datensätze

Domain-Namen werden basierend auf DNS-Datensätzen ihren IP-Adressen zugeordnet – und umgekehrt. Dabei lösen Forward-DNS-Datensätze (z. B. A- oder CNAME-Datensätze) Domain-Namen zu IP-Adressen auf, während Reverse-DNS-Datensätze (z. B. PTR-Datensätze) IP-Adressen zu Domain-Namen auflösen. Wenn Sie über gültige Forward- und Reverse-DNS-Datensätze verfügen, können E-Mail-Anbieter einfacher die Identität und Reputation Ihres E-Mail-Servers verifizieren und Spoofing- sowie Phishing-Angriffe verhindern.

Rate gemeldeter Spam-Nachrichten unter 0,3 %

Mit den Gmail Postmaster Tools können Sie die Leistung und Zustellbarkeit Ihrer E-Mails bei Gmail überwachen und analysieren. Eine der von diesem Service unterstützten Kennzahlen ist die Spam-Rate, d. h. der Anteil der E-Mails, die von Anwendern als Spam gekennzeichnet wurden. Eine hohe Spam-Rate schadet nicht nur der Reputation Ihrer E-Mails, sondern führt auch dazu, dass Ihre E-Mails von Gmail herausgefiltert werden. Eine Meldungsrate von 0,3 % gilt bei Gmail als Schwellenwert, um E-Mails generell als „Spam“ einzustufen.

Nachrichtenformat entsprechend RFC 5322

RFC 5322 ist ein Dokument, in dem das Standardformat und die Syntax für E-Mail-Nachrichten beschrieben werden. Es geht detailliert auf die Regeln und Konventionen bezüglich Struktur und Inhalt von E-Mail-Headern und -Textteilen ein, einschließlich Datum, Betreff, Absender, Empfänger und Nachrichten-ID.

Durch die Einhaltung des Standards RFC 5322 gewährleisten Sie, dass Ihre E-Mail mit den E-Mail-Protokollen konform ist und von E-Mail-Anbietern sowie -Clients richtig verarbeitet und angezeigt werden kann.

Abmelde-Option mit einem Klick

Um für E-Mail-Marketing relevante Gesetze wie den CAN-SPAM Act oder die DSGVO einzuhalten, müssen Sie Ihren Abonnenten eine einfache und unkomplizierte Möglichkeit anbieten, sich aus der E-Mail-Liste auszutragen (Opt-out).

Dies wird üblicherweise mit einem Abmelde-Link (oder einer entsprechenden Schaltfläche) im Fußteil der E-Mail umgesetzt. Auf diese Weise können sich Abonnenten aus Ihrer E-Mail-Liste austragen, ohne ihre E-Mail-Adresse eingeben oder sich bei Ihrer Website anmelden zu müssen. Mit dieser Option berücksichtigen Sie die Präferenzen und Privatsphäre Ihrer Abonnenten und reduzieren die Wahrscheinlichkeit, dass Ihre E-Mails als Spam eingestuft oder als schädlich gemeldet werden.

ABSCHNITT 5

Was passiert bei Nichteinhaltung?

E-Mail-Authentifizierung betrifft nicht nur Ihre Sicherheit, sondern auch das Geschäftsergebnis Ihres Unternehmens und die Zufriedenheit Ihrer Kunden. Wenn Sie die von Google und Yahoo festgelegten E-Mail-Authentifizierungsanforderungen nicht einhalten, werden Ihre E-Mails möglicherweise blockiert oder direkt in den Junk-Ordner zugestellt – was schwerwiegende Auswirkungen auf Ihr Unternehmen haben kann.

Nachfolgend erläutern wir einige der potenziellen geschäftlichen Folgen.

Geringere Effektivität Ihrer Marketing-Aktivitäten

Wenn Ihre E-Mail-Kampagnen nicht authentifiziert werden, könnten sie von Google und Yahoo Mail herausgefiltert werden, sodass Ihre Zielgruppe Ihre Angebote, Neuigkeiten oder Ihren Content gar nicht erst zu sehen bekommt. Das Ergebnis: geringere Öffnungsraten, Klickraten, Konversionen und Umsätze durch E-Mail-Marketing.

Unterbrechung von Geschäftsabläufen und Geschäftseinbußen

Wenn Ihre Kunden wichtige Nachrichten von Ihnen nicht erhalten, können sie mit Ihnen nicht ins Geschäft kommen. Sie können sich möglicherweise nicht anmelden, keine Kennwörter zurücksetzen, Bestellungen nicht bestätigen, keine Bestätigungen erhalten und nicht auf den Support zugreifen. Dies kann zu irritierten, verärgerten und unzufriedenen Kunden und dazu führen, dass sie auf Ihren Service verzichten oder zu einem Mitbewerber wechseln.

Geringere Kundenzufriedenheit und geringeres Ansehen Ihrer Marke

Als minimaler digitaler Kundendienst werden heute Follow-up-E-Mails, Bestellbestätigungen, Lieferbenachrichtigungen und ähnliche Nachrichten erwartet.

Wenn Ihre E-Mail-Nachrichten nicht authentifiziert werden, könnten sie von Ihren Kunden übersehen oder ignoriert werden. Dadurch wird Ihre Marke als unprofessionell, unzuverlässig und nicht vertrauenswürdig wahrgenommen, was Ihrer Markenreputation schadet und die Abwanderung von Kunden erhöht.

So kann Proofpoint helfen

Wenn Sie die neuen E-Mail-Authentifizierungsanforderungen einhalten, können Sie Ihre Digital-Marketing-Maßnahmen stärken, die Zufriedenheit Ihrer Kunden gewährleisten und Ihre Marke schützen. Mit diesen Möglichkeiten kann Proofpoint Sie dabei unterstützen, DMARC zu implementieren und sicherzustellen, dass Ihre geschäftskritischen E-Mails die Kunden und Interessenten erreichen.

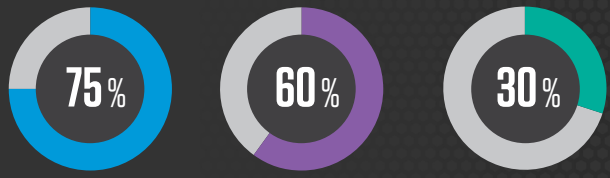
- Mit **Proofpoint Email Fraud Defense (EFD)** erhalten Sie Unterstützung von erfahrenen Beratern, die Sie auf jedem Schritt Ihrer DMARC-Implementierung begleiten, damit Sie die Zustellbarkeit und Sicherheit Ihrer E-Mails optimieren können.
- **Services für gehostetes SPF, gehostetes DKIM und gehostetes DMARC** können die Konfiguration sowie Wartung vereinfachen und gewährleisten, dass Ihre E-Mail-Nachrichten alle Authentifizierungsprüfungen bestehen. Mit diesen Services können Sie auch die bestehende Limitierung auf 10 SPF-DNS-Lookups oder die erforderliche Schlüsselrotation bei DKIM umgehen.
- Mit **Proofpoint Secure Email Relay** können Sie gewährleisten, dass Transaktions-E-Mails (die von Anwendungen oder externen Partnern in Ihrem Namen versendet werden) per DKIM signiert werden, sodass der DMARC-Abgleich beschleunigt wird. Durch diesen Service erhalten Sie zudem detaillierte Transparenz und Kontrolle über den Datenverkehr bei Transaktions-E-Mails. Damit haben Sie die Möglichkeit, eventuelle Probleme, die die Zustellbarkeit oder Leistung Ihrer E-Mails beeinträchtigen können, schnell zu identifizieren und zu beheben.

Gründe für Proofpoint

Wir analysieren täglich mehr als:

2,6 Mrd. E-MAILS	**49 Mrd.** URLs	**1,9 Mrd.** ANHÄNGE
1,7 Mrd. MOBILGERÄTE-NACHRICHTEN	**430 Mio.** WEB-DOMAINS	**143.000** SOCIAL-MEDIA-KONTEN

Auf unsere Lösungen vertrauen mehr als:



DER FORTUNE 100 | DER FORTUNE 1000 | DER FORTUNE GLOBAL 2000

8.000 GROSSUNTERNEHMEN

200.000 KLEINE UNTERNEHMEN

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0501-015-04-01 11/23