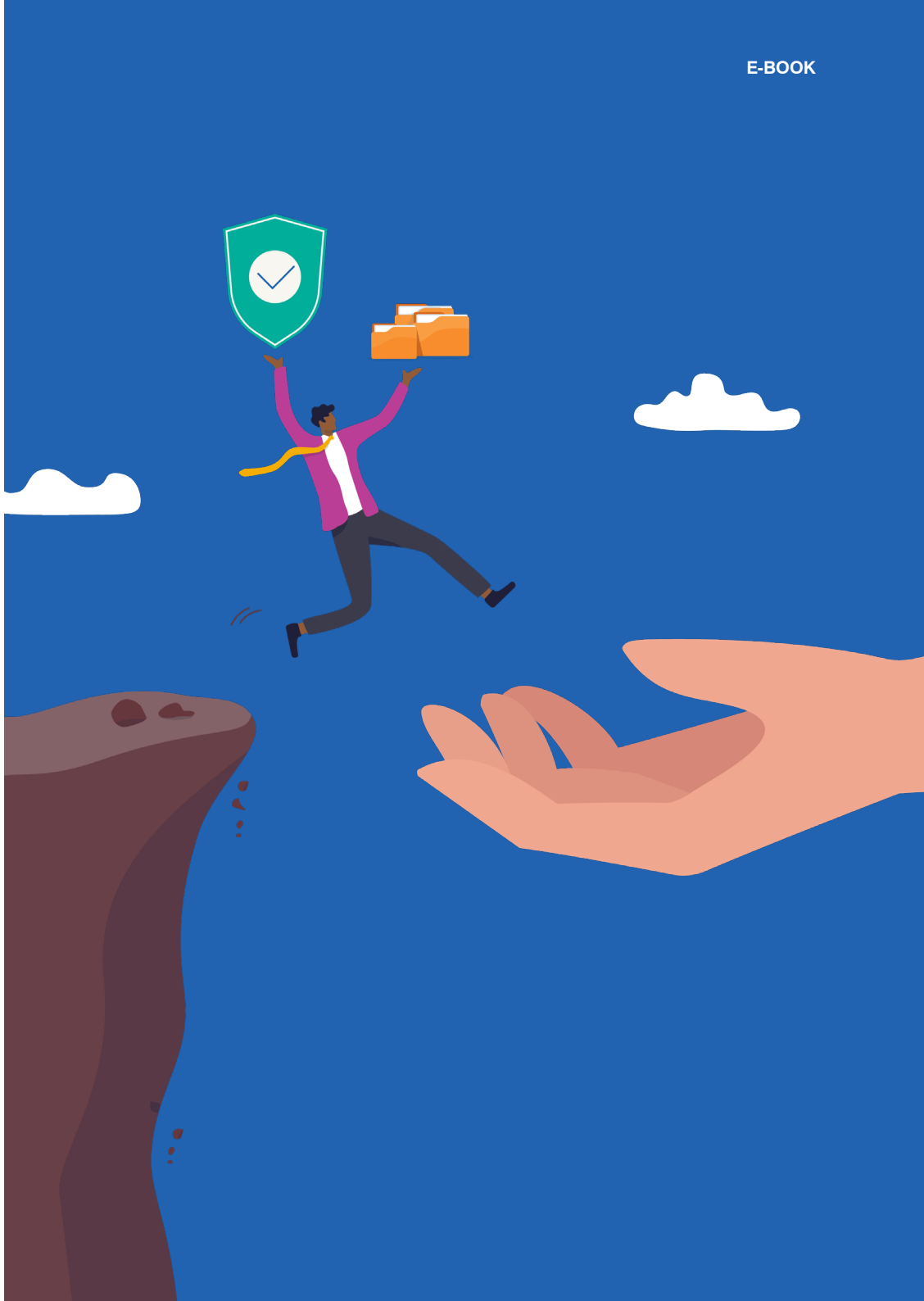
E-BOOK

Erste Schritte mit DMARC

Wie Sie mit E-Mail-Authentifizierung Ihre E-Mail-Domain absichern, Business Email Compromise (BEC) verhindern und Ihre Marke schützen können



proofpoint.

Einführung

E-Mails sind gut fürs Geschäft: Sie sind preisgünstig, skalierbar und – noch viel wichtiger – hervorragend geeignet, um Leads zu generieren und den Umsatz zu fördern. Leider sind E-Mails wegen ihrer großen Vorteile – Benutzerfreundlichkeit, Komfort und Transparenz – jedoch auch der bevorzugte Angriffsvektor von Cyberkriminellen.

E-Mail-Betrug verursacht bei Unternehmen auf der ganzen Welt Kosten in Milliardenhöhe und kann die Markenreputation sowie das Vertrauen der Kunden innerhalb von Minuten zerstören. Das wohl größte Gefahrenpotenzial birgt äußerst gezielter BEC-Betrug (Business Email Compromise, auch als Chefmasche bezeichnet). Laut FBI beläuft sich der hierdurch seit 2016 entstandene finanzielle Schaden bei Unternehmen auf der ganzen Welt auf 43 Milliarden US-Dollar.[1]

1 FBI: „Business Email Compromise: The 43 $ Billion Scam“ (Business Email Compromise: Der 43-Milliarden-Dollar-Betrug), Mai 2022.

43 Mrd. $

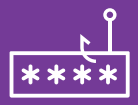
Weltweite Kosten durch BEC für Unternehmen seit 2016
(Quelle: FBI)

180.000 $

Kosten bei einem durchschnittlichen BEC-Angriff pro Zwischenfall, weltweit
(Quelle: FBI)

12 %

Zunahme bei Unternehmen (im Jahresvergleich), die im Jahr 2021 Phishing-Angriffe gemeldet haben
(Quelle: Proofpoint)



86 %

Anteil der Unternehmen, die 2021 Ziel eines Phishing-Angriffs waren
(Quelle: Proofpoint)

Der im Februar 2012 von einer Gruppe führender E-Mail-Anbieter vorgestellte DMARC-Standard ist im Kampf gegen Phishing und Spoofing bis heute eines der schlagkräftigsten und proaktivsten Instrumente.

Er hat die Bedrohungslage durch E-Mail-Betrug grundlegend verändert und seit langem bestehende Phishing-Strategien ausgehebelt, sodass Cyberkriminelle ihre bevorzugten Ziele aufgeben mussten. DMARC hat das Potenzial, eine ganze Betrugsform zunichtezumachen.

In diesem Leitfaden erfahren Sie, was der DMARC-Standard ist, wie er funktioniert, welche wesentlichen Vorteile er bietet und warum er ein zentraler Bestandteil der Verteidigungsstrategie Ihrer Marke gegen BEC-Angriffe und Impostor-Bedrohungen sein sollte.

ABSCHNITT 1

Was ist DMARC?

Das offene E-Mail-Authentifizierungsprotokoll DMARC, das im Jahr 2012 von einem Industriekonsortium vorgestellt wurde, ermöglicht Domain-basierten Schutz des E-Mail-Kanals.

Das DMARC-Protokoll baut auf den bestehenden Standards SPF (Sender Policy Framework) und DKIM (DomainKeys Identified Mail) auf und 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.

DMARC

Domain-based

Message

Authentication

Reporting and...

Conformance

Offener E-Mail-Authentifizierungsstandard

Eingeführt im Jahr 2012

Etabliert von über 20 Unternehmen

Mit DMARC können E-Mail-Absender:

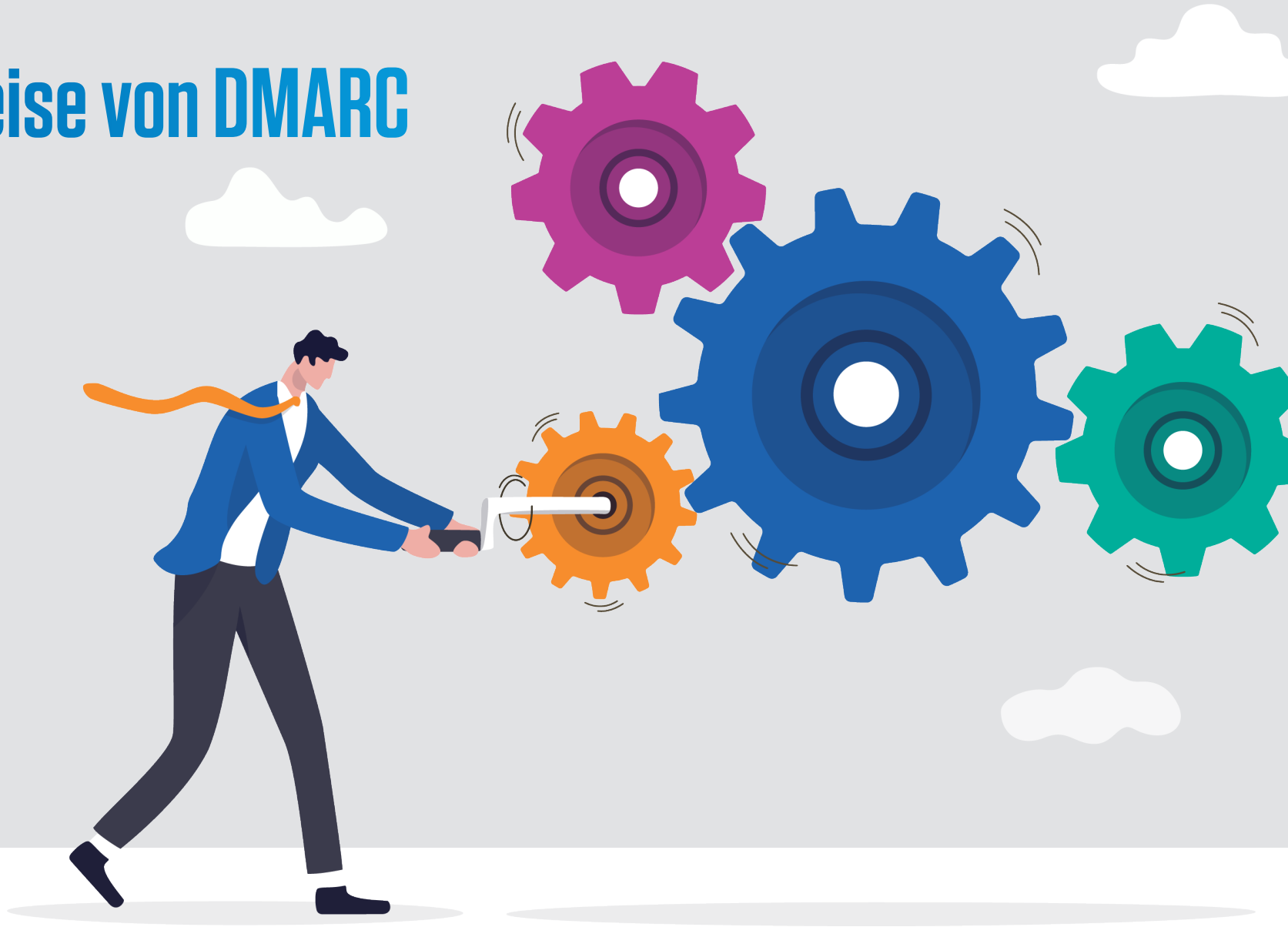
Kontrolle wiedererlangen, da legitime E-Mails für ihre Versand-Domains authentifiziert werden.

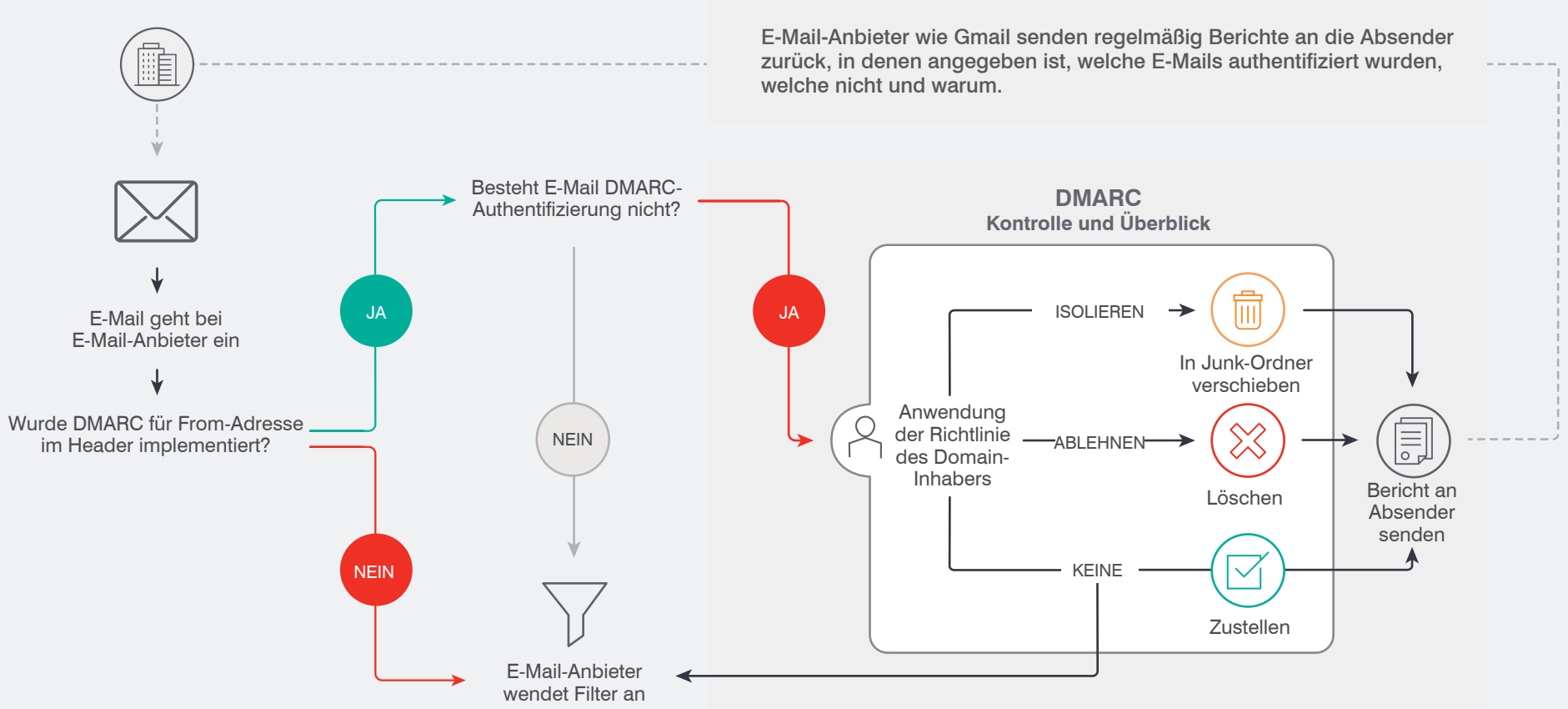
E-Mail-Anbieter festlegen (über eine explizite Richtlinieneinstellung), wie mit Nachrichten umzugehen ist, deren Authentifizierung fehlschlägt. Diese Nachrichten können entweder in einen Junk-Ordner verschoben oder gleich abgelehnt werden, wodurch die Kunden weniger anfällig für Angriffe sind.

Einblicke erhalten in die E-Mail-Bedrohungslandschaft. Auf diese Weise können Sie gegen Ihre Kunden gerichtete Bedrohungen leichter erkennen und Ihre Marke besser gegen Phishing und Spoofing schützen.

ABSCHNITT 2

Funktionsweise von DMARC





DMARC-Richtlinieneinstellungen

Keine: Das gesamte E-Mail-Authentifizierungssystem wird überwacht, um legitimen Datenverkehr zu identifizieren.

Isolieren: Nachrichten, deren DMARC-Authentifizierung fehlschlägt, werden in den Spam-Ordner verschoben.

Ablehnen: Nachrichten, deren DMARC-Authentifizierung fehlschlägt, werden gar nicht zugestellt.

ABSCHNITT 3

Warum DMARC?

DMARC unterstützt Absender wie folgt:

Sie erhalten einen Überblick darüber, wer Nachrichten in Ihrem Namen versendet, welche E-Mails authentifiziert werden (und welche nicht) und warum.

Sie können E-Mail-Empfängern mitteilen, wie nicht authentifizierte E-Mails gehandhabt werden sollen.

Phishing-Angriffe, die Ihre eigenen Domains fälschen, werden blockiert, bevor die Nachrichten die Postfächer der Mitarbeiter und Verbraucher erreichen.

DMARC unterstützt Empfänger wie folgt:

Sie können zwischen legitimen und böswilligen Absendern unterscheiden.

Sie stärken Kundentreue und Mitarbeiterschutz.

Sie verbessern und schützen die Reputation des E-Mail-Kanals.

„Kurz gesagt: Der DMARC-Standard funktioniert. Bei einem kombinierten Ansatz zur Bekämpfung von E-Mail-Betrug ist DMARC der Grundpfeiler der technischen Kontrollen ... um wieder für mehr Vertrauen zu sorgen und den E-Mail-Kanal für legitime Marken und Kunden zurückzugewinnen."

Edward Tucker, Head of Cyber Security, HM Revenue & Customs

„Mit strengeren DMARC-Richtlinien sind die Anwender besser geschützt – und den Cyberkriminellen wird ihr Tun erschwert. Noch wichtiger ist jedoch, dass verifizierte Absender eine enorme Innovationen und Verbesserungen für all unsere Postfächer anstoßen werden."

Jeff Bonforte, SVP of Communications Products, Yahoo!

ABSCHNITT 4

Die Vorteile von DMARC

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.
Sofortiger 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.
Bessere Zustellbarkeit und stärkere Nutzung von E-Mails	Etwa 20 % der Phishing-Angriffe beeinträchtigen die Zustellbarkeit und 33 % reduzieren die Nutzung von E-Mails. DMARC verbessert die Zustellbarkeit und führt dazu, dass legitime E-Mail-Programmen intensiver genutzt werden.
Geringere Kosten für den Kundendienst	Da DMARC Phishing-Angriffe blockiert, werden die Kosten für den Kundendienst erheblich gesenkt. Der skandinavische Einzelhändler Blocket verzeichnete nach der Implementierung von DMARC 70 % weniger Kundendienst-Tickets.
Geringere Kosten für die Reaktion auf Phishing	Phishing verursacht jedes Jahr Markenschäden in Höhe von 4,5 Milliarden US-Dollar. DMARC verringert die Kosten, die durch Betrug, Rückerstattungen und die Reaktion auf Phishing-Angriffe entstehen.

ABSCHNITT 5

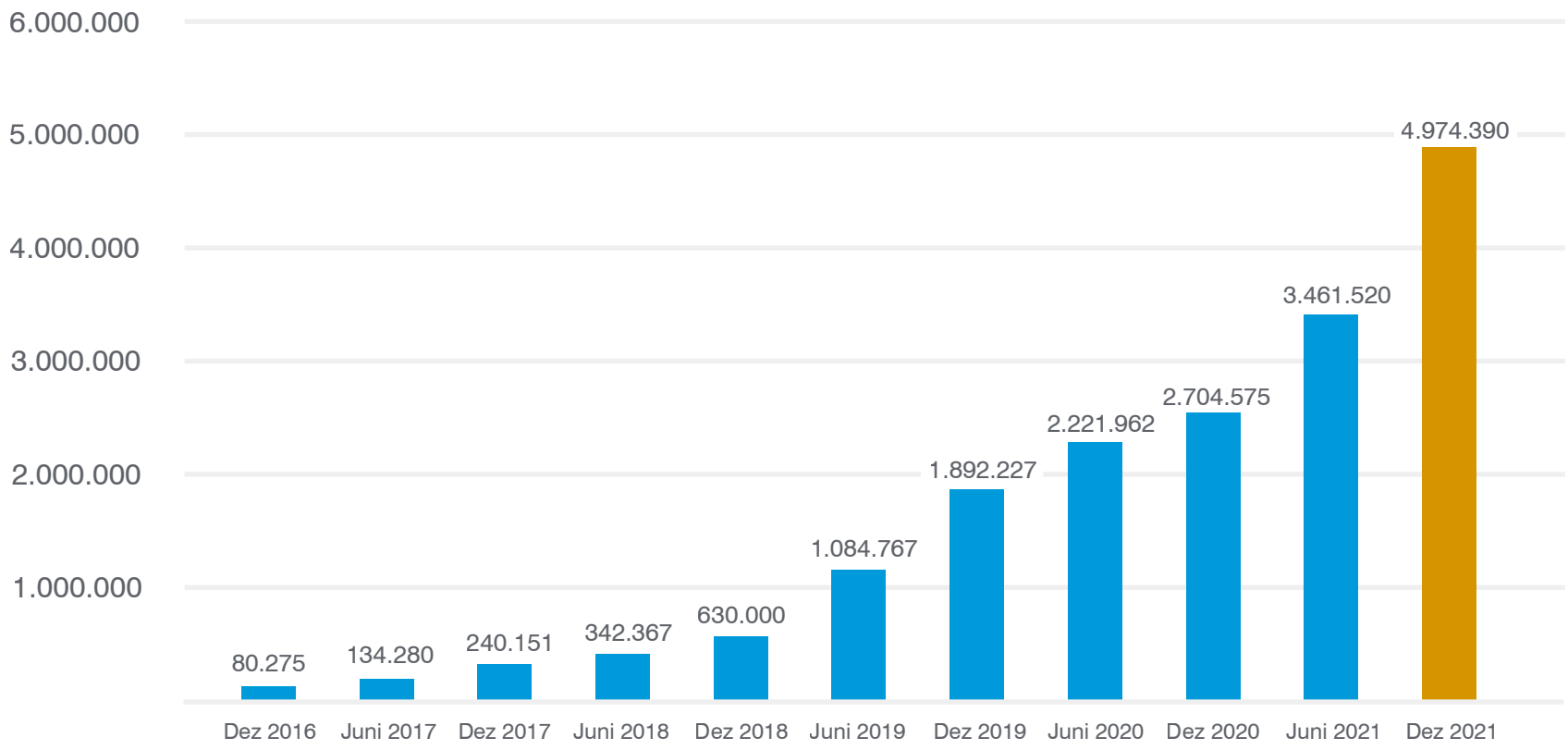
DMARC in Zahlen

5 Millionen
individuelle DMARC-Datensätze sind aktiv. (Stand: Dezember 2021)

65 %
der Global 2000-Unternehmen haben die DMARC-Authentifizierung eingeführt.

26 %
der Global 2000-Unternehmen haben eine DMARC-Richtlinie zur E-Mail-Ablehnung implementiert.

Gültige DMARC-Datensätze, die per DNS bestätigt wurden



Quelle: DMARC.org

ABSCHNITT 6

Auf einen Blick: E-Mail-Authentifizierung

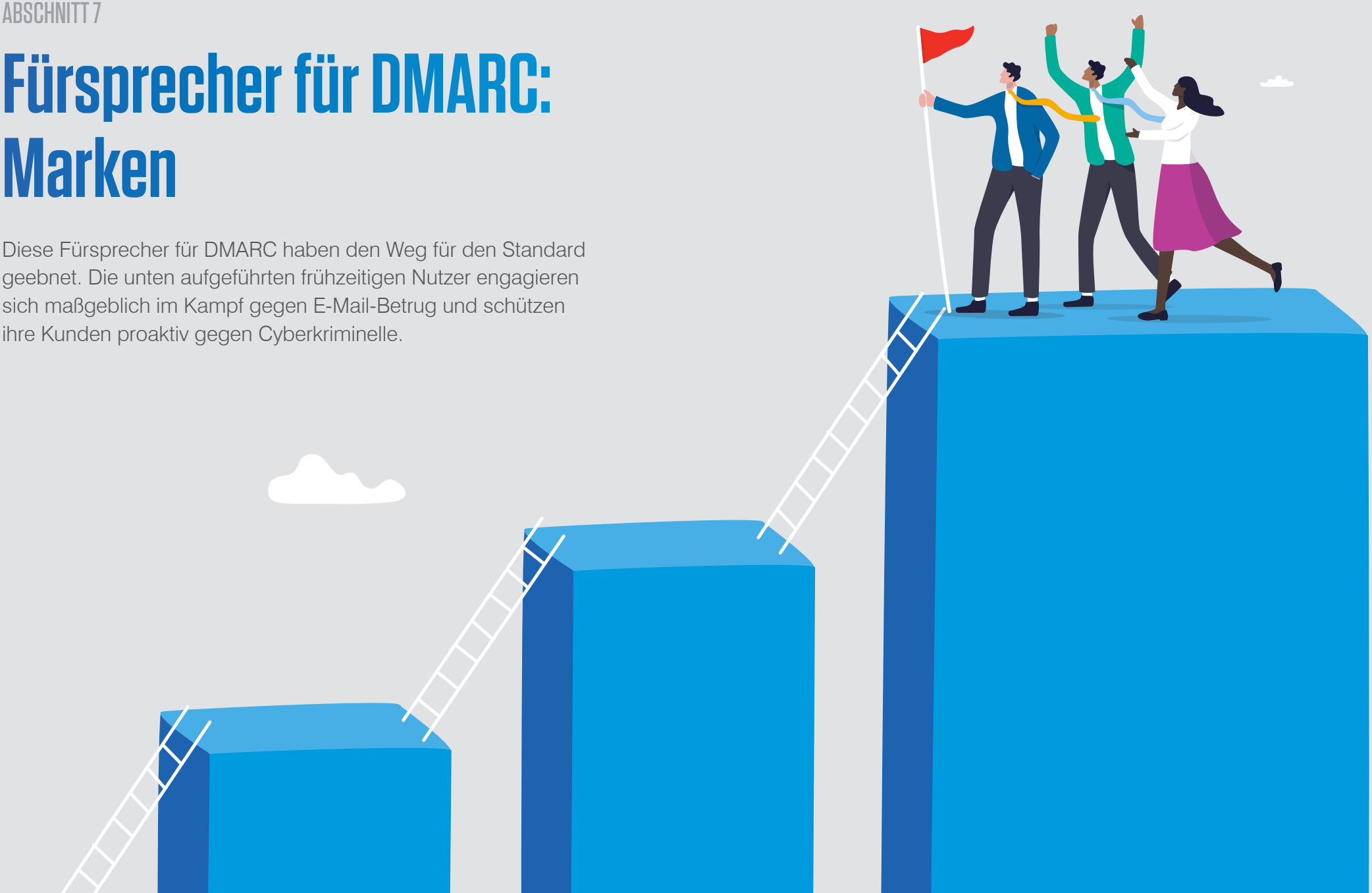
DMARC baut auf zwei weiteren wichtigen E-Mail-Authentifizierungsstandards auf: SPF und DKIM. Zum genauen Verständnis von DMARC müssen Sie auch die Vorteile von SPF und DKIM kennen – und ebenso ihre Schwachpunkte.

	SPF	DKIM	DMARC
	(Sender Policy Framework) **www.open-spf.org**	(DomainKeys Identified Mail) **www.dkim.org**	(Domain-based Message Authentication Reporting & Conformance) **www.dmarc.org**
Vorteile	Mit SPF können Marken festlegen, wer im Namen ihrer Domain eine E-Mail senden kann, und die IP-Adressen autorisierter Absender in einem DNS-Datensatz auflisten. Wenn die IP-Adresse, über die E-Mails im Namen der Marke gesendet werden, in diesem SPF-Datensatz nicht aufgeführt ist, schlägt die SPF-Authentifizierung der Nachricht fehl.	Mit DKIM kann ein Unternehmen die Verantwortung dafür übernehmen, dass eine Nachricht in einer Form übermittelt wird, in der sie vom E-Mail-Anbieter verifiziert werden kann. Die Verifizierung erfolgt mithilfe kryptografischer Authentifizierung innerhalb der digitalen Signatur der E-Mail.	DMARC stellt sicher, dass legitime E-Mails ordnungsgemäß anhand etablierter DKIM- und SPF-Standards authentifiziert werden und dass betrügerische Aktivitäten, die scheinbar von markeneigenen Domains ausgehen, noch vor Erreichen des Kundenpostfachs blockiert werden.
DNS-Beispieldatensatz	v=spf1 ip4:204.200.197.197 -all	v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4zOo3N	v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_agg@auth.yourdomain.com;ruf=mailto:dmarc_afrf@auth.yourdomain.com
Schwächen	• Die Aktualisierung der SPF-Datensätze bei einem Anbieterwechsel der Marke und das Hinzufügen von E-Mails gestalten sich schwierig. • Nur weil die SPF-Authentifizierung einer Nachricht fehlschlägt, bedeutet das nicht, dass die Zustellung in einer Postfach dauerhaft blockiert wird. • Bei der Weiterleitung einer Nachricht wird SPF unterbrochen. • SPF schützt Marken nicht vor Cyberkriminellen, die den Anzeigenamen oder die Absender-Adresse im Header einer Nachricht spoofen.	• Die Implementierung von DKIM ist schwieriger, weshalb es von weniger Absendern genutzt wird. • Aufgrund dieser nur punktuellen Nutzung ist das Fehlen einer DKIM-Signatur nicht unbedingt ein Hinweis auf eine betrügerische E-Mail. • DKIM allein ist keine durchgängig zuverlässige Methode zur Authentifizierung der Identität eines Absenders. • Die DKIM-Domain ist für den nicht-technischen Endnutzer nicht sichtbar. Außerdem kann das Spoofing der sichtbaren Absender-Adresse (aus der From-Zeile im Header) nicht verhindert werden.	• DMARC ist äußerst wichtig, aber keine vollständige Lösung. • DMARC schützt Ihre Marke nur gegen 30 % der E-Mail-Angriffe (direkte Bedrohungen von Domains). • DMARC schützt nicht gegen Marken-Spoofing (einschließlich Display Name-Spoofing und Doppelgänger-Domains).

ABSCHNITT 7

Fürsprecher für DMARC: Marken

Diese Fürsprecher für DMARC haben den Weg für den Standard geebnet. Die unten aufgeführten frühzeitigen Nutzer engagieren sich maßgeblich im Kampf gegen E-Mail-Betrug und schützen ihre Kunden proaktiv gegen Cyberkriminelle.



„In den letzten Jahren haben immer mehr Unternehmen DMARC und die E-Mail-Authentifizierung eingeführt. Außerdem integrieren viele allgemeine Anbieter und Service-Anbieter die erforderliche Unterstützung in ihre Angebote, um die Nutzung zu vereinfachen.“

Steven Jones, DMARC.org

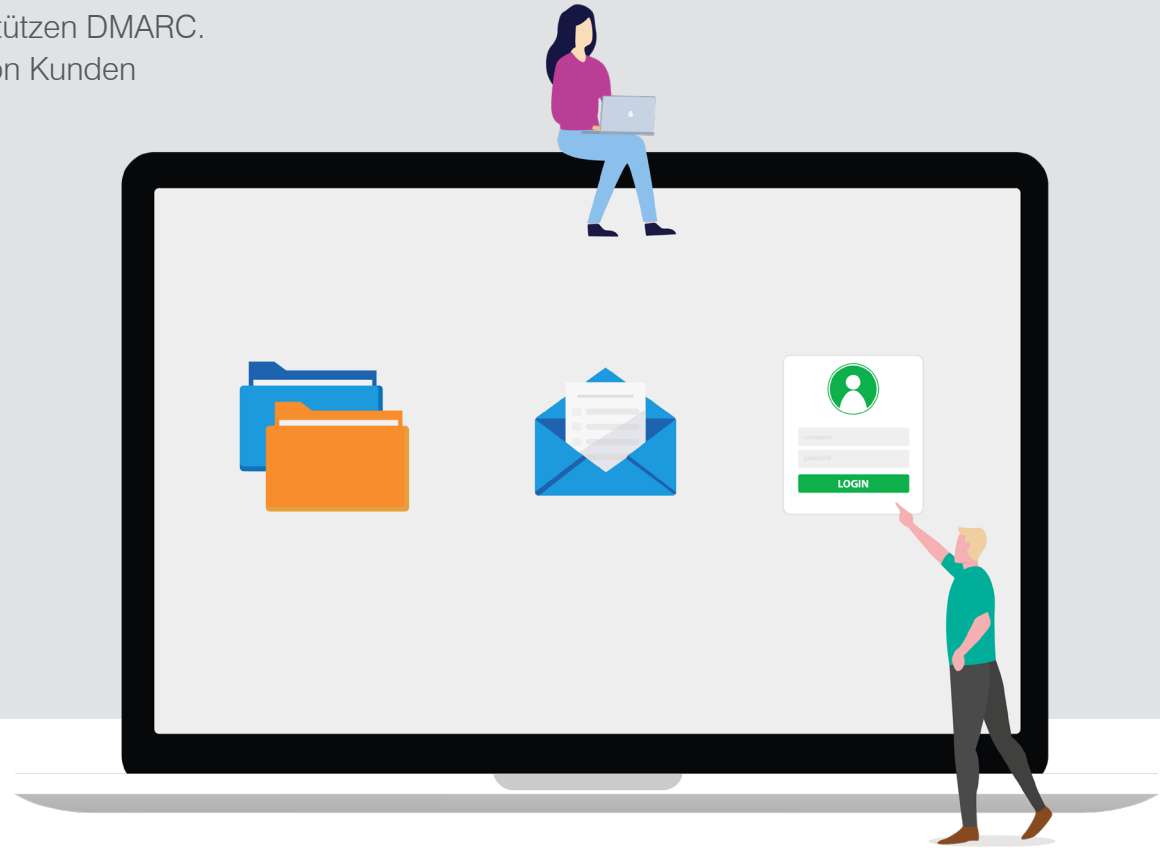
„Nachdem wir eine DMARC-Richtlinie zur E-Mail-Ablehnung implementiert hatten, sank die Anzahl der Phishing-bezogenen Kundendienst-Tickets um über 70 %. Die Kundendienstmitarbeiter konnten sich also auf die Unterstützung von Kunden bei Anfragen konzentrieren, mit denen Umsatz generiert wird.“

Thomas Bäcker,
Head of Customer Security,
Blocket

ABSCHNITT 8

Fürsprecher für DMARC: E-Mail-Anbieter

Einige der weltweit größten E-Mail-Anbieter unterstützen DMARC. Heute sind geschätzt etwa 80 % der Postfächer von Kunden auf der ganzen Welt durch DMARC geschützt.



„Der Trend geht schnell hin zu einer Welt, in der alle E-Mails authentifiziert werden. Durch die Implementierung einer DMARC-Richtlinie wird sichergestellt, dass der Ruf eines Absenders nicht durch die Aktivitäten von Spammern geschädigt wird. Wenn Ihre Domain nicht durch DMARC geschützt wird, steigt die Wahrscheinlichkeit, dass Ihre Nachrichten direkt im Spam-Ordner landen oder sogar blockiert werden.“

John Rae-Grant,
Product Manager, Google

DMARC








„Die Cyberkriminellen, die E-Mail-Spoofing einsetzten, um E-Mails zu fälschen und Phishing-Kampagnen mit vorgeblich aus einem Yahoo! Mail-Konto stammenden E-Mails zu starten, wurden von einem Tag auf den anderen fast vollständig abgewehrt.“

Jeff Bonforte,
SVP of Communications Products, Yahoo!

ABSCHNITT 9

Glossar der DMARC-Tags

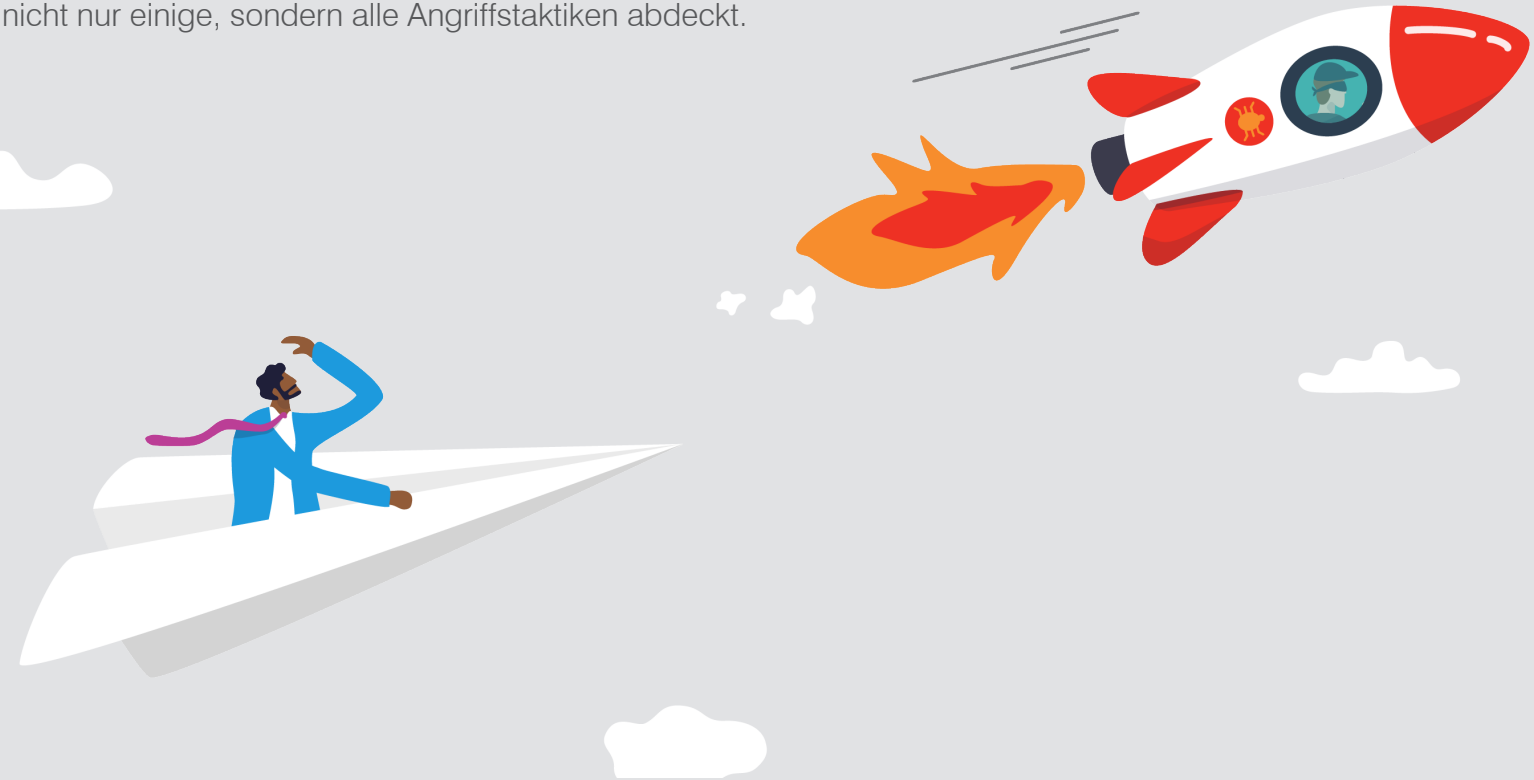
Tag-Name	Zweck	Beispiel
v	Protokollversion	v=DMARC1
p	Richtlinie für Domain	p=quarantine
pct*	Prozentualer Anteil der Nachrichten, die gefiltert werden	pct=20
rua*	Reporting-URI von aggregierten Berichten	rua=mailto:aggrep@example.com
sp*	Richtlinie für Sub-Domains der Domain	sp=reject
aspf*	Abgleichmodus für SPF (strikt (s) oder ungenau (r))	aspf=r
ruf*	Reporting-URI von forensischen Berichten	ruf=mailto:aggrep@example.com
adkim*	Abgleichmodus für DKIM (strikt (s) oder ungenau (r))	adkim=r
ri*	Anzahl der Sekunden, die zwischen dem Versand aggregierter Berichte an Absender vergehen	ri=86400
fo*	Bietet Optionen zur Generierung von Fehlerberichten	"fo=1"

*Optional

ABSCHNITT 9

Die Zeit ist reif: Implementierung von DMARC

BEC-Angriffe sind komplex und facettenreich. Daher ist eine vollständige Lösung erforderlich, die nicht nur einige, sondern alle Angriffstaktiken abdeckt.



Die Implementierung von DMARC ist keine Wunderwaffe gegen BEC und EAC, aber ein guter Anfang. Dieser Standard ist eine entscheidende Komponente bei der Abwehr von Impostor-Bedrohungen und schützt insbesondere vor Angriffen, bei denen vertrauenswürdige E-Mail-Domains gespoofft werden. DMARC ist der effektivste Schutz vor Domains-Spoofing und vor dem Missbrauch Ihrer Domain durch betrügerische E-Mails.

Proofpoint unterstützt einige der weltweit größten Marken bei der erfolgreichen Bereitstellung von DMARC. Jedes Unternehmen ist einzigartig. Dennoch orientieren sich die meisten an diesen Schritten, um DMARC im Laufe der Zeit vollständig bereitzustellen.

Den Anfang macht ein sehr einfacher erster Schritt: Erstellen Sie einen DMARC-Datensatz im DNS und verschaffen Sie sich einen vollständigen Überblick über Ihr gesamtes E-Mail-Ökosystem.

Schritt 1

Wählen Sie eine Domain aus.

(Dies kann Ihre primäre Top-Level Domain oder eine Sub-Domain sein, über die viele E-Mails gesendet werden.)

Schritt 2

Generieren Sie Ihren Datensatz mit unserem **DMARC Creation Wizard.** (Legen Sie die Richtlinie für den E-Mail-Empfänger auf „none“ (keine) fest.)

Schritt 3

Fügen Sie gemeinsam mit Ihrem Server-Administrator Ihren DMARC-Datensatz dem DNS hinzu.

Schritt 4

Sie erhalten DMARC-Berichte über Ihre Domain.

Schritt 5

Kontaktieren Sie unser Team für Betrugsbekämpfung. Wir setzen alles daran, dass Sie schnell wieder die Kontrolle über Ihr E-Mail-System erhalten.

Glückwunsch! Sie haben den ersten Schritt zur Abwehr von E-Mail-Betrug getan.

Weitere Informationen dazu, wie Proofpoint Sie bei der effektiven Abwehr von BEC-Angriffen und beim Schutz Ihr Marke unterstützen kann, finden Sie unter **proofpoint.com/de**.

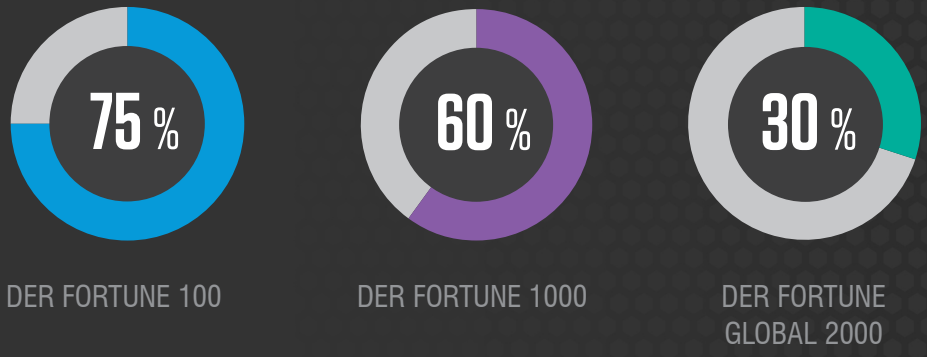
Informationen zu Proofpoint

Proofpoint Nexus Threat Graph verbindet die branchenweit beste Sicherheitsforschung, Technologie und Bedrohungsdaten, um Sie in allen Angriffsphasen zu schützen. Kein anderer Anbieter verfügt über umfangreichere Einblicke in die Mechanismen aktueller Cyberangriffe.

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:



8.000
GROSSUNTERNEHMEN

200.000
KLEINE UNTERNEHMEN

WEITERE INFORMATIONEN

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

proofpoint.

0503-003-04-03 01/23