mailgun by sinch

LEITFADEN

Der Mailgun-Leitfaden zum Thema Sicherheit und Compliance

Schutz in einer gefährlichen digitalen Welt

Inhaltsverzeichnis

Inhaltsverzeichnis

EINFÜHRUNG

Bittere Wahrheiten zum Thema E-Mail

Es ist Zeit für einen Realitätscheck. So sehr wir das Format E-Mail auch lieben, es stellt ein großes Sicherheitsrisiko für Ihr Unternehmen dar. Wenn Sie diesen Leitfaden lesen, arbeiten Sie wahrscheinlich mit daran, diejenigen zu schützen, die durch eine Sicherheitsverletzung oder die Nichteinhaltung von Datenschutzbestimmungen geschädigt werden könnten.

Machen Sie sich keine Illusionen. Es ist nicht einfach, Betrüger daran zu hindern, E-Mails für ihre Zwecke zu missbrauchen, und Best Practices für Datenschutz und Sicherheit zu befolgen. Das Team von Mailgun by Sinch weiß das genauso wie jeder andere in der Branche.

Jedoch **glauben wir daran, dass Ihre E-Mail-Strategie schützenswert ist**, und wir sind der Meinung, dass Aufklärung helfen kann, eine sicherere digitale Landschaft zu gestalten. In diesem umfassenden Leitfaden erhalten Sie wertvolle Einblicke und Ratschläge von Experten, wie Sie diesen Schutz gewährleisten können.

Schauen wir uns aber zunächst die Fakten an. **Hier sind fünf bittere Wahrheiten über E-Mail:**

1. E-Mail ist die größte Gefahrenquelle

E-Mail ist ein beliebtes Tool von Cyberkriminellen, und der Posteingang ist einer ihrer Lieblingsorte, an denen sie anzufinden sind.

Egal, ob es sich um klassischen Spam, einen Phishing-Angriff oder den Versuch handelt, Ransomware und Malware zu verbreiten: Der Posteingang bietet Betrügern die Gelegenheit, ihre unschönen Taten zu begehen, und zwar zu einem sehr günstigen Preis.

Im Jahr 2022 meldete die Hotelkette Marriot ihre dritte bedeutende Sicherheitsverletzung innerhalb von vier Jahren. Diesmal handelte es sich um einen Social-Engineering-Angriff, durch den ein Betrüger Zugriff auf den Computer eines Mitarbeiters erhielt. Marriot hat in diesem Jahr mehr als 16 Millionen US-Dollar ausgegeben, um sich von einer anderen Sicherheitsverletzung im Jahr 2018 zu erholen.

Betrüger finden sogar Wege, die Multifaktor-Authentifizierung (MFA) mithilfe von Phishing-Tools und -Techniken wie Adversary-in-the-Middle (AiTM) zu umgehen. Laut Microsoft nimmt eine neue Betrugsmasche Tausende von Unternehmen ins Visier.

E-Mail ist ein Weg, auf dem Betrüger in Unternehmen eindringen können. Das Format bietet ihnen die Möglichkeit, eine große Anzahl potenzieller Opfer zu erreichen, oder ganz gezielt eingesetzt zu werden, etwa beim Spear-Phishing. Da nahezu jeder Mensch eine E-Mail-Adresse hat, brauchen Betrüger keine hohe Erfolgsrate. Es reicht manchmal eine betrogene Person, um ein ganzes Unternehmen aus dem Gleichgewicht zu bringen.

Und dennoch können wir das Format E-Mail nicht aufgeben, weil wir es brauchen.

2. E-Mail ist gekommen, um zu bleiben

Trotz des ständigen technologischen Wandels im digitalen Zeitalter ist die E-Mail nach wie vor eine der besten Möglichkeiten, mit Kunden und Kollegen zu kommunizieren, eine Zielgruppe zu erreichen und Geschäfte zu tätigen. Von Transaktions-E-Mails, die wichtige Informationen enthalten, bis hin zu Marketing-E-Mails, die das Wachstum eines Unternehmens vorantreiben: Es wäre eine große Herausforderung, ohne unsere Posteingänge auszukommen.

Jedes Mal, wenn jemand ein neues Mobilgerät einrichtet oder ein Online-Konto eröffnet, benötigt diese Person eine E-Mail-Adresse. Sie ist ein wichtiger Bestandteil der personenbezogenen Daten, die wir alle verwenden, um auf Anwendungen und digitale Dienste zugreifen zu können. Deshalb ist Identitätsdiebstahl für Betrüger ein Leichtes, wenn sie Zugang zu einem E-Mail-Konto erhalten.

Schätzungen zufolge werden täglich mehr als 333 Milliarden E-Mails weltweit versendet und empfangen. **Bis zum Jahr 2025 wird diese Zahl voraussichtlich auf 376 Milliarden ansteigen**. Viele dieser E-Mails stammen natürlich von Spammern und Betrügern.

3. Datenschutzgesetze und -beschränkungen werden verschärft

In dem Bestreben, den Posteingang und das Internet insgesamt sicherer zu machen, erlassen Regierungen Gesetze und Tech-Konzerne führen neue Funktionen ein, um die Nutzer ihrer E-Mail-Dienste zu schützen.

So hat Apple beispielsweise 2021 die E-Mail-Welt mit der Einführung der E-Mail-Datenschutzfunktion aufgerüttelt. Google hat bereits 2017 aufgehört, die E-Mails von Gmail-Nutzern für gezielte Werbezwecke zu lesen. Und die E-Mail-Experten von Mailgun sagen, dass die KI-gestützten Spamfilter von Gmail die besten der Branche sind.

Verbraucherschutzgesetze wie die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union und der California Consumer Privacy Act (CCPA) in den Vereinigten Staaten sollen die Menschen ermächtigen und den Missbrauch sensibler Daten verhindern.

Das Problem ist, dass die meisten legitimen Absender bereits alle Regeln und Best Practices befolgen. **Es sind die Betrüger, die sich nicht daran halten**. Die Bezeichnung „Gesetzlose" kommt schließlich nicht von ungefähr.

4. Cyberkriminalität entwickelt sich ständig weiter

Was auch immer E-Mail-Anbieter und ESPs tun, um zu verhindern, dass bösartige E-Mails in den Posteingang gelangen, Betrüger scheinen immer einen Weg zu finden. Ihre Taktiken werden immer komplizierter und ihre Strategien immer raffinierter.

Nick Schafer leitet bei Mailgun die Abteilung Zustellbarkeit und Einhaltung. Nick und sein Team arbeiten daran, Betrüger von unserer Plattform fernzuhalten. Dazu gehören unter anderem die Überwachung verdächtiger Aktivitäten und die ständige Beobachtung von E-Mail-Sicherheitstrends. Er beschreibt diese Arbeit als einen nie enden wollenden Kampf:

„Es ist nicht schön, aber die Wahrheit ist, dass man sie nicht aufhalten kann, man kann sie jedoch besiegen. Sobald wir einen Weg gefunden haben, eine Betrugsmasche zu stoppen, kommen sie schon mit einer neuen Taktik um die Ecke. Das bedeutet aber nicht, dass man es nicht versuchen sollte. Wenn das Beste, was wir tun können, ist, ihr Agieren zu drosseln, dann machen wir das."

Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

5. Versender müssen immer einen Schritt voraus sein

All dies bedeutet, dass die Versender mit Blick auf E-Mail-Sicherheit und Datenschutz wachsam sein müssen. Ihr Unternehmen muss alles in seiner Macht Stehende tun, um Probleme zu vermeiden. Gleichzeitig muss es darauf vorbereitet sein, die Situation zu entschärfen, falls es doch einmal zu einem Vorfall kommt.

Um Betrügern immer einen Schritt voraus zu sein, die E-Mails nutzen wollen, um Ihre Abonnenten zu betrügen oder Personen in Ihrem Unternehmen zu täuschen, sind mehrere wichtige Faktoren erforderlich:

- Eine geschulte Belegschaft, die sich der Risiken bewusst ist
- Zuverlässige E-Mail-Authentifizierungsprotokolle
- Ein Verständnis von datenschutzrechtlichen Bestimmungen und deren Zusammenhang mit E-Mails
- Partner, die Ihr Team dabei unterstützen, E-Mails zu schützen

Wir werden uns in diesem Leitfaden auf diese Bereiche konzentrieren. Und Sie werden auch von Mailgun-Experten lesen, die eng mit den Benutzern zusammenarbeiten, um unsere Plattform und die E-Mail-Strategien unserer Kunden zu schützen.

Warum das Format E-Mail schützenswert ist

Auch wenn Spammer und Betrüger unermüdlich sind, ist die Konzentration auf E-Mail-Sicherheit und Datenschutz definitiv ein lohnendes Unterfangen.

Wen und was Sie schützen, wenn Sie der Sicherheit und der Einhaltung von Vorschriften Priorität einräumen:

1. Das Unternehmen

Laut einer globalen Studie von IBM betrugen die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2021 über 4 Millionen US-Dollar. **Der durchschnittliche finanzielle Schaden eines Phishing-Angriffs lag bei 4,65 Millionen US-Dollar**. Business Email Compromises (BEC), also die Kompromittierung von Geschäfts-E-Mails, die eine Form des Spear-Phishings darstellen, waren mit knapp 5 Millionen US-Dollar pro Verletzung am teuersten.

Dieselbe IBM-Studie ergab, dass Unternehmen üblicherweise mehr als 280 Tage brauchen, um diese Art von Angriffen zu stoppen und zu beheben. Dazu zählen auch die Zeit und die Ressourcen, die IT- und Cybersicherheitsteams benötigen, um Sicherheitslücken zu erkennen und zu schließen.

2. Markenreputation

Sicherheitsverletzungen und Betrug im Zusammenhang mit Ihrem Unternehmen führen zu schlechter Presse und schädigen die Markenreputation, was einen Vertrauensverlust zur Folge hat. Die IBM-Studie ergab, dass **entgangene Geschäfte 38 % der Gesamtkosten bzw. fast 1,6 Millionen US-Dollar pro Verletzung ausmachten**.

Die Auswirkungen auf die Markenreputation können natürlich über das hinausgehen, was an finanziellen Kosten gemessen wird. Unternehmen, die von Spoofing im Posteingang betroffen sind, stellen möglicherweise fest, dass Kontakte ihre E-Mails seltener öffnen und sich weniger mit ihnen beschäftigen, weil sie nicht sicher sind, ob die Nachrichten sicher sind.

3. Absender-Reputation

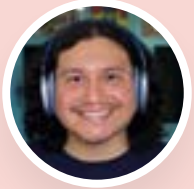
Neben der Markenreputation verfügen E-Mail-Anbieter wie Gmail, Apple Mail und Yahoo Mail über Möglichkeiten, die Reputation eines E-Mail-Absenders zu messen und zu bewerten. Wenn die DNS-Einträge für die E-Mail-Authentifizierung nicht richtig konfiguriert sind, ist es für E-Mail-Anbieter schwieriger, die Legitimität Ihrer E-Mails zu erkennen.

Das könnte bedeuten, dass die E-Mails, die Sie versenden, mit größerer Wahrscheinlichkeit blockiert oder als Spam eingestuft werden. Fehlende oder fehlerhafte Authentifizierungsprotokolle können sich also negativ auf die Absender-Reputation und die Zustellbarkeit von E-Mails auswirken.

4. Benutzer und Kunden

Die vielleicht wichtigste Überlegung ist, wie E-Mail-Sicherheit und Authentifizierung zum Schutz Ihrer Kunden und/oder der Benutzer Ihrer Anwendungen beitragen. Die Privatsphäre, Identitäten und Finanzen derjenigen, die Sie als Unternehmen bedienen, sind gefährdet, wenn Sie der Sicherheit und der Einhaltung von Vorschriften keine Priorität einräumen.

Jonathan Torres leitet Teams von Technical Account Managern (TAMs) für Mailgun und andere Sinch-Produkte. Er erinnert uns daran, dass das E-Mail-Format Teil eines vernetzten digitalen Ökosystems ist.



„Compliance, Sicherheit und Zustellbarkeit von E-Mails sind nicht nur ein Problem für den Absender. Wenn Sie lediglich darüber nachdenken, wie sich diese Dinge auf Sie auswirken, ist das eine zu enge Sichtweise. E-Mail-Anbieter, Abonnenten, Kunden, Mitarbeiter und Unternehmen; diese Probleme berühren alle Bereiche, und alle sind am Ende davon betroffen.“

Jonathan Torres, TAM-Teammanager, Mailgun

TEIL 1

E-Mail-Betrug: Damals und heute

Um zu verstehen, warum E-Mail die größte Gefahrenquelle im Bereich der Cybersicherheit ist, und um den Ernst der Lage zu begreifen, ist es hilfreich, sich anzusehen, woher wir kommen und wie wir hierher gekommen sind.

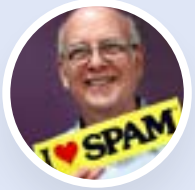
Lassen Sie uns zunächst eine Zeitreise machen an den Punkt, als E-Mails noch in den Kinderschuhen steckten. Und dann schauen wir uns einige gängige Strategien an, die Betrüger in modernen Angriffen auf E-Mails anwenden.

Die Anfänge des Formats E-Mail

Anfangs war das E-Mail-Format vor allem eine Form der Kommunikation zwischen Abteilungen. Der Programmierer Ray Tomlinson stellte 1971 im Computer-Netzwerk ARPANET eine vermutlich frühe Version des E-Mail-Formats vor. Einige Jahre später entwickelte ein junger Mann namens Shiva Ayyadurai ein Softwareprogramm, das er „EMAIL" nannte, und das an einer medizinischen Fakultät in New Jersey Briefkästen und Papiernotizen ersetzen sollte.

Schon bald wurden E-Mails für die Kommunikation zwischen verschiedenen Unternehmen verwendet, was zu dem führte, was viele als die erste E-Mail-Spam-Nachricht bezeichnen. Der Marketer Gary Thuerk schickte 1978 unaufgefordert eine Nachricht an Hunderte von ARPANET-Mitarbeitern, in der ein neues Computermodell von Digital Equipment Corporation (DEC) beworben wurde. Thuerk behauptet, die Nachricht habe DEC 13 Millionen US-Dollar eingebracht.

E-Mail stellte sich also als ein idealer Kanal heraus, um Menschen davon zu überzeugen, Geld auszugeben. Als das Wall Street Journal im Jahr 2008 das 30-jährige Jubiläum von Spam feierte, erklärte Thuerk jedoch, warum er sich nicht für das Monster verantwortlich fühlte, zu dem E-Mail-Spam geworden war.



„Wenn die Fluggesellschaft Ihr Gepäck verliert, machen Sie dann die Wright Brothers dafür verantwortlich?"

Gary Thuerk, „Vater des Spam"

Als immer mehr Verbraucher PCs kauften und schließlich online gingen, sahen Betrüger die Gelegenheit, den Posteingang noch gewinnbringender für sich zu nutzen. Und es erwies sich als einfach.

Als das Format E-Mail noch neu und aufregend war, öffneten, lasen und beantworteten die Menschen so ziemlich alles, was in ihrem Posteingang landete. Der durchschnittliche Internetnutzer war außerdem auch ziemlich leichtgläubig. Einige der Tricks, auf die Leute damals hereinfielen, sind zu Witzen geworden, weil sie so lächerlich sind.

Der sogenannte „Nigerianischer Prinz" E-Mail-Betrug, eine Form des Vorschussbetruges, ist ein perfektes Beispiel für E-Mail-Betrug. Es gab viele ähnliche Betrugsmaschen, bei denen den Empfängern vorgetäuscht wurde, sie hätten im Lotto gewonnen oder eine unerwartete Erbschaft von einem verschollenen Verwandten erhalten. Es ist überraschend, dass viele dieser altmodischen Taktiken auch heute noch verwendet werden.

In den 1990er Jahren war E-Mail ein bisschen wie der Wilde Westen, mit gesetzlosen Spammern, die ihr Unwesen trieben. Aber ein neuer Sheriff kam in die Stadt – oder, genauer gesagt, in den Posteingang.

Hartes Durchgreifen gegen Spam

Machen wir nun einen Sprung in die frühen 2000er Jahre. Es war eine Zeit, in der das Modem, Stone-Washed-Jeans und Compact Discs aus den 1990er Jahren auf dem Rückzug waren. Es war auch eine Zeit, in der E-Mail-Spam sprunghaft anstieg und der US-amerikanische Gesetzgeber 2003 den CAN-SPAM Act verabschiedete.

Etwa zur gleichen Zeit nahm Kate Nowrouzi eine Stelle bei America Online (AOL) an. Heute ist Kate VP für den Bereich Zustellbarkeit und Produktentwicklung bei Mailgun. Damals gehörte sie zum Anti-Spam-Team von AOL.

Im Jahr 2003 war AOL neben Hotmail und Yahoo Mail noch einer der größten E-Mail-Anbieter der Welt. Zu Spitzenzeiten hatte AOL mehr als 35 Millionen Benutzer. Die meisten Menschen nutzten es für ihre E-Mails und Internet-Verbindungen. Und auch im Kampf gegen Spam spielte AOL ganz vorne mit.

Kate und das Anti-Spam-Team von AOL erkannten, wie schwierig es war, festzustellen, ob es sich bei einer Nachricht um Spam oder um eine legitime E-Mail handelte, die ein Abonnent erhalten wollte. Die Art des Inhalts oder der Branche war nicht das beste Signal. Auch Unternehmen mit nicht jugendfreien Inhalten oder die Viagra verkaufen, haben valide Gründe, E-Mails an ihre Abonnenten zu versenden.

„Wir hatten Algorithmen in die Filter integriert, um Spam-Muster zu erkennen, und wir haben eingehenden Datenverkehr, der verdächtig war, manuell analysiert. Aber die Definition von Spam kann von Person zu Person sehr unterschiedlich sein. Deshalb haben wir beschlossen, die AOL-Mitglieder zu ermächtigen. Sie sollten selbst entscheiden, ob sie diese oder jene E-Mail erhalten wollten oder nicht."

Kate Nowrouzi, VP Zustellbarkeit und Produktentwicklung, Mailgun

Dies führte zur ersten **Spam-Meldefunktion** und machte AOL zum ersten E-Mail-Anbieter, der eine **Feedback-Schleife** mit seinen Benutzern hatte. Als Nächstes begann das Anti-Spam-Team mit der Entwicklung von Regeln, um zu bewerten, wie viele Spam-Beschwerden (basierend auf einem Prozentsatz des Volumens) ein Absender erhalten konnte, bevor AOL seine E-Mails blockierte. Dies führte schließlich zu der als **Beschwerderate** bezeichneten E-Mail-Kennzahl, die von E-Mail-Anbietern herangezogen wird, um die Absender-Reputation zu beurteilen.

Während all dies dazu beitrug, Spam zu *kontrollieren,* hat es ihn nicht gestoppt. Betrüger mussten einfach nur neue Taktiken entwickeln.

Zunehmende Komplexität

Kate weist darauf hin, dass nicht jeder E-Mail-Spam gleich ist. Es gibt die traditionellen Spammer, die einfach keine Erlaubnis haben, Ihnen E-Mails zu schicken, und die sich schnell verdientes Kleingeld erhoffen. Die größte Bedrohung stellen jedoch Absender dar, die potenziell schädigende Ziele verfolgen. Und diese Betrüger werden immer gewiefter.

„Es hat sich einiges geändert. Spam entwickelt sich weiter. Es ist ein Spiel ohne Ende. Während Mailgun seine Plattform als E-Mail-Service-Provider weiterentwickelt und ISPs auf der anderen Seite dasselbe tun, arbeiten wir alle hart daran, unsere Nutzer vor bösartigen Aktivitäten zu schützen. Aber manchmal gehen die Spammer ziemlich überzeugend vor, vor allem mit Social Engineering.“

Kate Nowrouzi, VP Zustellbarkeit und Produktentwicklung, Mailgun

Angreifer können Social-Engineering-Angriffe über den Posteingang durchführen, weil im Internet so viele Informationen über Personen und Unternehmen verfügbar sind. Sie können viel in Erfahrung bringen, indem sie einfach die öffentliche Präsenz des Angriffsziels in den sozialen Medien durchforsten.

Betrügerische E-Mails kommen heutzutage nicht mehr von dem falschen Prinzen aus Nigeria, **sondern geben vor, von Ihrer Bank, Ihrem besten Freund oder Ihrem Chef zu stammen**.

Vor nicht allzu langer Zeit nahm Kate an einer öffentlichen Spendenaktion auf Facebook teil. Dann erhielt sie, wie *sie dachte*, eine E-Mail vom Initiator dieser Spendenaktion, einem bekannten Gründer im Silicon Valley. In der E-Mail wurde ihr für ihre Spende gedankt und um weitere Unterstützung in Form von Amazon-Geschenkkarten gebeten.

Zunächst übersah Kate eines der verräterischen Zeichen – einen Unterstrich in der E-Mail-Adresse zwischen dem Vor- und Nachnamen des Absenders, der sich geringfügig von der echten E-Mail-Adresse unterschied. Doch in der Folgekommunikation bemerkte Kate offensichtlichere Anzeichen wie schlechtes Englisch und eine ungewöhnliche Verwendung von Emojis, die für die Person, für die sich die Betrüger ausgaben, untypisch wirkten.

Ich arbeite seit 20 Jahren in dieser Branche und bin auf diesen Trick hereingefallen. Ich kann mir nicht vorstellen, warum jemand wie meine Mutter nicht darauf hereinfallen würde.

Kate Nowrouzi, VP Zustellbarkeit und Produktentwicklung, Mailgun

Die Gedankenwelt des modernen Betrügers

Es gibt viele verschiedene Arten von E-Mail-Betrug und diverse Möglichkeiten, ihn durchzuführen. Eine der häufigsten Angriffsmethoden der letzten Jahre ist das „**Brand Spoofing**“, eine Form von Phishing, bei der Betrüger sich in E-Mails und auf Webseiten als Ihr Unternehmen ausgeben, um Menschen dazu zu verleiten, ihnen Zugangsdaten zu Konten oder andere sensible Informationen zu geben. Die E-Mail-Authentifizierung mit DMARC ist der beste Schutz davor.

Wenn jedoch ein Betrüger einfache E-Mail-Übertragungsprotokolle oder API-Schlüssel in die Hände bekommt, kann er buchstäblich im Namen Ihres Unternehmens versenden und damit möglicherweise großen Schaden anrichten.

Jonathan Torres hat sich in die Lage eines Betrügers versetzt und den grundlegenden Ablauf erklärt. Auf diese oder eine ähnliche Weise läuft es häufig ab, in nur fünf einfachen Schritten.

Wie E-Mail-Brand-Spoofing funktioniert

Schritt 1

Finden Sie ein Unternehmen mit hohem Wiedererkennungswert, das anfällig für Spoofing ist.

Unternehmen aus den Bereichen Finanzen, Online-Handel und Technologie gehören zu den Unternehmen, die am ehesten gefälscht werden.

Schritt 2

Suchen Sie nach ungeschützten API-Schlüsseln oder knacken Sie Passwörter von einfachen E-Mail-Übertragungsprotokollen.

Auf diese Weise können sich Betrüger als das Unternehmen selbst ausgeben und E-Mail-Anbieter sowie Abonnenten täuschen.

Schritt 3

Fälschen Sie eine Landingpage oder Login-Seite.

Mit ein paar einfachen Tools und dem richtigen Logo ist es ein Kinderspiel, das Aussehen der Unternehmens-Webseite zu imitieren.

Schritt 4

Verfassen Sie eine überzeugende Fake-E-Mail.

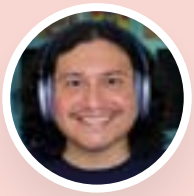
Betrüger erzeugen oft ein Gefühl von Dringlichkeit, um ihre Opfer zu schnellem, unbedachtem Handeln zu bringen.

Schritt 5

Erfassen Sie Zugangsdaten von Opfern.

Die E-Mail verweist auf die gefälschte Landing Page. Dort versuchen die E-Mail-Empfänger, sich anzumelden, geben aber in Wirklichkeit sensible Informationen preis.

Wie Sie sehen, muss man kein Super-Hacker sein, um mit Brand-Spoofing davonzukommen. Jeder, der Zugang zu Tools wie Photoshop, einen kostenlosen Webseiten-Baukasten und eine Liste mit zusammengeklaubten E-Mails hat, kann es versuchen. Ein Unternehmen mit Wiedererkennungswert zu imitieren, ist ein Kinderspiel.



„Wenn es Ihnen gelingt, eine E-Mail zu versenden, die so aussieht, als käme sie von einem bekannten Unternehmen, können Sie die Leute auf gefälschte Landingpages schicken. Und wenn ein Betrüger Zugang zu Ihren tatsächlichen E-Mails hat, lassen sie sich leicht nachahmen.“

Jonathan Torres, TAM-Teammanager, Mailgun

Was können Technikteams also tun, um Brand-Spoofing zu verhindern? **Der beste Schutz gegen Spoofing ist die Implementierung von E-Mail-Authentifizierungsprotokollen**, auf die wir in Teil 5 näher eingehen werden. Aber wenn Sie vor E-Mail-Anbietern und E-Mail-Empfängern nicht als Spammer dastehen wollen, müssen Sie einige wichtige Regeln und Vorschriften beachten.

TEIL 2

Compliance und Regelwerke

Bevor wir uns damit befassen, wie Betrüger davon abgehalten werden können, E-Mails für böswillige Zwecke zu nutzen, sollten wir sicherstellen, dass Sie als seriöser und vertrauenswürdiger Absender alle Rechtsvorschriften befolgen.

Zunächst eine kurze Auffrischung, wer mit E-Mail und Datenschutz zu tun hat:

1. Betroffene Personen:

Dies bezieht sich auf den Verbraucher bzw. den Empfänger von E-Mail-Kommunikation. Betroffene Personen sind diejenigen, deren personenbezogene Daten von anderen erfasst, gespeichert und verwendet werden. Datenschutzbestimmungen sollen ihre Rechte schützen.

2. Datenverantwortliche:

Datenverantwortliche sind diejenigen, die personenbezogene Daten der betroffenen Personen erfassen, speichern und weitergeben. Sie sind dafür verantwortlich, diese personenbezogenen Daten zu schützen, egal wo sie hinfließen oder wer darauf zugreift.

3. Auftragsdatenverarbeiter:

Diese Stellen verarbeiten personenbezogene Daten im Auftrag der Datenverantwortlichen. Es handelt sich dabei üblicherweise um externe Lösungsanbieter, die Zugang zu personenbezogenen Daten benötigen, um einen Dienst bereitzustellen. Zwischen Auftragsdatenverarbeitern und Datenverantwortlichen sollte ein Vertrag geschlossen werden, in dem Dinge wie die Datennutzung, die sichere Speicherung und der Umgang mit personenbezogenen Daten nach Beendigung der Geschäftsbeziehung geregelt werden.

Als Versender von E-Mails fällt Ihr Unternehmen höchstwahrscheinlich in die Kategorie „Datenverantwortlicher“, während Mailgun ein „Auftragsdatenverarbeiter“ wäre. Die Datenschutzbeauftragte von Mailgun, Darine Fayed, sagt, dass auch wenn unser Unternehmen bei der Einhaltung von Vorschriften weit über das normale Maß hinausgeht, die Last letztendlich bei den Versendern liegt.

„Jeder, der mit personenbezogenen Daten in Berührung kommt, muss sie schützen. Datenverantwortliche müssen jedoch genau festlegen, wie personenbezogene Daten gespeichert, behandelt und an Dritte weitergegeben werden sollen. Dies muss auf eine Weise geschehen, die die Vorschriften strikt befolgt."

Darine Fayed, Leiterin der Rechtsabteilung und Datenschutzbeauftragte, Mailgun

Überblick über wichtige Verbraucherschutzgesetze

Schauen wir uns kurz einige wichtige Normen und Vorschriften zum Verbraucherdatenschutz an und inwiefern sie sich auf das Format E-Mail beziehen.

Da es beim Thema Datenschutz viel zu beachten gibt, behandeln wir hier nur die Grundlagen und verweisen auf weitere Ressourcen, wo Sie weitere Informationen über bestimmte Vorschriften und deren mögliche Auswirkungen auf Sie als Versender erhalten.

DSGVO

Eine der wichtigsten Regelungen. Die 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) der EU hat viel dazu beigetragen, den Datenschutz für Verbraucher in die richtige Bahn zu lenken.

Während einige Marketer große Bedenken hatten, wie sich die DSGVO auf ihre Arbeitsweise auswirken könnte, erwies sie sich als Volltreffer für alle. Viele der DSGVO-Anforderungen galten bereits als Best Practices für E-Mail-Versender, und andere wurden dazu veranlasst, den Datenschutz ernster zu nehmen und zu stärken, um dem Gesetz zu entsprechen.

Einige wichtige DSGVO-Richtlinien für E-Mail-Versender:

- Zustimmung des E-Mail-Empfängers erforderlich
  - Ausdrückliche Zustimmung für Werbebotschaften erforderlich
  - Stillschweigende Zustimmung für die meisten Transaktions-E-Mail
- Die Möglichkeit, E-Mails abzubestellen (Abmeldelink)
- Sichere Speicherung der für die E-Mail-Personalisierung verwendeten Daten
- Die Möglichkeit, sämtliche personenbezogenen Daten zur Verfügung zu stellen oder zu löschen, wenn eine Datenzugriffsanfrage durch die betroffene Person gestellt wird

- Verlinkungen zur Datenschutzerklärung des Unternehmens, wo immer Sie personenbezogene Daten wie E-Mail-Adressen erfassen

Darine betont, dass Datenschutzerklärungen von Unternehmen einfach und verständlich formuliert sein und sich auf ein Minimum an juristischer Fachsprache beschränken sollten.

> *„Jede Datenschutzerklärung muss eindeutig, verständlich und transparent sein. Das bedeutet, Sie müssen Ihren Abonnenten und Kunden mitteilen, welche Daten Sie erfassen, wofür Sie sie nutzen wollen, wie lange diese Daten gespeichert werden und ob sie irgendwohin übertragen werden. Ihre Großmutter sollte in der Lage sein, im Internet einzukaufen und die Datenschutzerklärung zu verstehen."*
>
> Darine Fayed, Leiterin der Rechtsabteilung und Datenschutzbeauftragte, Mailgun

Die DSGVO hat viele Länder dazu veranlasst, ihre eigenen Datenschutzgesetze genauer unter die Lupe zu nehmen. Wenn man sich die folgende Liste anschaut, hat man das Gefühl, in einer Buchstabensuppe zu schwimmen.

- Brasilien hat den Gesetzesentwurf über den Personendatenschutz vorgelegt (Personal Data Protection Bill, PDPB)
- China hat das Gesetz zum Schutz personenbezogener Daten (Personal Information Protection Law, PIPL)
- Japan nutzt sein Gesetz zum Schutz persönlicher Daten (Personal Information Privacy Act, PIPA)
- Australien hat sein Datenschutzgesetz angepasst, um digitalen Belangen Rechnung zu tragen
- Großbritannien hat nach dem Brexit die UK GDPR erlassen
- Brasilien hat ein allgemeines Gesetz zum Schutz personenbezogener Daten (LGPD)
- Kanada verfügt über ein Gesetz zum Schutz personenbezogener Daten und elektronischer Dokumente (PIPEDA)

Denken Sie stets daran, dass wenn Ihr Unternehmen mit Menschen in einem bestimmten Land Geschäfte macht, Sie sich an die Datenschutzgesetze dieses Landes halten müssen. Wenn Sie die DSGVO-Richtlinien bereits befolgen, sind Sie in den meisten Bereichen auf der sicheren Seite.

California Consumer Privacy Act

In den USA ist die umfassendste Datenschutzverordnung der California Consumer Privacy Act (CCPA), der kurz nach der DSGVO in Kraft getreten ist. Es gibt viele Ähnlichkeiten zwischen den beiden Verordnungen, und der CCPA spiegelt gängige Best Practices für Versender von E-Mails wider.

Obwohl der CCPA nur für Einwohner des Bundesstaates Kalifornien gilt, haben viele US-amerikanische und internationale Unternehmen Kontakte, die in diese Kategorie fallen. Mit anderen Worten: Sie müssen CCPA-konform handeln.

Auch wenn es in anderen Bundesstaaten eigene Datenschutzgesetze gibt und andere Gesetzesvorschläge das Gesetzgebungsverfahren durchlaufen, könnte laut Darine Fayed in den kommenden Jahren ein US-Bundesgesetz auf den Weg gebracht werden.

Payment Card Industry Data Security Standard (PCI DSS)

Der Payment Card Industry Data Security Standard (PCI DSS) dient dem Schutz der Daten von Kreditkarteninhabern. Es handelt sich hierbei um einen globalen Standard, der für alle Unternehmen gilt, die Online-Zahlungen akzeptieren.

Die Einhaltung des PCI-Sicherheitsstandards umfasst Bestimmungen zum Schutz von Daten wie Kreditkartennummern, die über offene Netzwerke, einschließlich E-Mail, übertragen werden. Karteninhaberdaten per E-Mail zu versenden ist in der Regel keine gute Idee. Wenn Sie aus irgendeinem Grund Karteninhaberdaten per E-Mail übermitteln müssen, haben Sie sicherzustellen, dass sie ohne Unterbrechung verschlüsselt sind.

Das ist natürlich schwierig. Vor allem dann, wenn diese Nummern im Posteingang oder im Gesendet-Ordner landen, wo ein Hacker sie finden könnte. Aus diesem Grund besagt die PCI DSS-Bestimmung 4.2, dass Kreditkartendaten nicht über Endbenutzer-Messaging-Technologien wie E-Mail erfasst, übertragen oder gespeichert werden dürfen.

Die meisten Unternehmen nutzen für die Kreditkartenabwicklung Drittanbieter, die sich um die Einhaltung der PCI-Vorschriften kümmern. Mailgun verwendet zum Beispiel den Bezahldienst Stripe. Aber auch wenn Sie mit einem Drittanbieter zusammenarbeiten, müssen Sie PCI-konform sein, wenn Sie Daten von Karteninhabern auf eigenen Servern oder Systemen speichern.

Health Insurance Portability and Accountability Act

Der Health Insurance Portability and Accountability Act (HIPAA) ist ein US-amerikanisches Gesetz, das hauptsächlich für Unternehmen im Gesundheitssektor gilt. Es enthält Bestimmungen darüber, wie eine unzulässige Weitergabe von persönlichen Gesundheitsdaten (geschützte Gesundheitsdaten) des Patienten zu verhindern ist.

Die wichtigste HIPAA-Vorschrift für Versender von E-Mails ist, dass jede E-Mail, die geschützte Gesundheitsdaten enthält, **während der Übertragung verschlüsselt sein muss**. Darüber hinaus sollten Unternehmen aus dem Gesundheitswesen die Zustimmung der Patienten einholen, ihnen E-Mails zu senden, in einer Datenschutzerklärung erläutern, wie geschützte Gesundheitsdaten verwendet werden, und eine Möglichkeit haben, E-Mail-Kommunikation, die diese Daten enthält, sicher zu speichern.

Lesen Sie ausführlichere Hinweise von Mailgun zum Thema E-Mails und HIPAA-Compliance.

Die Software und die Dienste, die Sie zum Versenden und Empfangen von E-Mails verwenden, sind weitere wichtige Faktoren. Um herauszufinden, wie ein E-Mail-Service-Provider (ESP) den Datenschutz im Gesundheitswesen handhabt, fragen Sie nach dem HIPAA Business Associate Agreement (BAA), also der Vereinbarung für Geschäftspartner. Diese Vereinbarung legt die Verpflichtungen des Versenders und des Datenauftragsverarbeiters hinsichtlich der HIPAA-Compliance fest.

Lesen Sie sich das HIPAA BAA von Mailgun durch.

In diesem Rechtsdokument erläutern wir, wie wir die Aufteilung von Rechten und Pflichten beim Schutz persönlicher Gesundheitsdaten handhaben.

Warum E-Mail-Konformität wichtig ist

Dass die Nichteinhaltung von Vorschriften zu hohen Geldstrafen führen kann, sollte nicht die einzige Motivation für die Einhaltung von Datenschutzbestimmungen sein, findet Darine Fayed.

> *„Respektieren Sie den Datenschutz nicht, weil Sie Angst vor DSGVO-Bußgeldern haben oder weil eine Datenschutzbehörde bei Ihnen anklopft. Das ist nicht der Grund, warum Sie sich um Datenschutz kümmern sollten. Es ist eine Geschäftsentscheidung. Wenn Sie die Menschen und ihre Privatsphäre respektieren, werden sie wiederkommen. Sie sind sich der Datenschutzrisiken und ihrer Rechte viel stärker bewusst. Sie wollen Unternehmen vertrauen, aber sie erwarten von Unternehmen eben auch, dass sie ihre personenbezogenen Daten mit Sorgfalt behandeln.“*
>
> Darine Fayed, Leiterin der Rechtsabteilung und Datenschutzbeauftragte, Mailgun

Laut der Consumer Privacy Survey von Cisco geben **89 % der Befragten an, dass ihnen Datenschutz wichtig ist und sie sich mehr Kontrolle wünschen**. Allerdings hat weniger als ein Drittel der Befragten ihre Datenschutzbedenken umgesetzt. Die meisten Menschen erwarten, dass die Technologien, die sie verwenden, ihnen den nötigen Schutz bieten. Die vorherrschenden Datenschutzvorschriften einzuhalten hilft Ihnen, diesen Erwartungen gerecht zu werden.

TEIL 3

Die E-Mail-Bedrohungslage

Um Ihr Team zu unterstützen, die sich ständig ändernden E-Mail-Sicherheitsbedrohungen zu verstehen, mit denen Ihr Unternehmen konfrontiert ist, möchten wir einige wichtige Erkenntnisse aus den jüngsten Untersuchungen von führenden Unternehmen im Bereich der Cybersicherheit mit Ihnen teilen.

Auch wenn diese Statistiken von Jahr zu Jahr und sogar von Quartal zu Quartal schwanken, vermitteln sie doch ein Bild von den Herausforderungen, denen sich Technikteams stellen müssen, um E-Mails und alles, was mit diesem Kanal in Zusammenhang steht, zu schützen.

Phishing: Das größte Problem der Cybersicherheit

Laut Deloitte und vielen anderen Quellen beginnen **91 % der Cyberangriffe mit einer Phishing-E-Mail**. Der Posteingang ist der Ausgangspunkt des Angriffs, und von dort aus können die Betrüger Zugangsdaten stehlen, Malware wie Emotet Trojan verbreiten oder die digitalen Dateien und Daten eines Unternehmens gegen Lösegeld einfrieren.

Einem Bericht von Cisco aus dem Jahr 2021 zufolge, waren **50 % der befragten Unternehmen im Vorjahr von Ransomware betroffen**. Diese können extrem kostspielige Sicherheitsverletzungen sein. Untersuchungen von Palo Alto Networks ergaben, **dass die durchschnittliche Ransomware-Zahlung im Jahr 2022 bei fast 1 Millionen US-Dollar lag**, was einem Anstieg von 71 % gegenüber dem Vorjahr entspricht.

Warum E-Mail eine ernste Bedrohung ist

91 %
Angriffe, die mit E-Mail-Phishing beginnen

50 %
Unternehmen, die mit Ransomware-Aktivität konfrontiert sind

96 %
Unternehmen, die von E-Mail-Phishing betroffen sind

Der Bericht State of Email Security 2022 von Mimecast zeigt, dass drei von vier befragten Unternehmen einen Anstieg der E-Mail-basierten Bedrohungen verzeichneten, während **96 % angaben, Angriffsziel von E-Mail-Phishing zu sein**.

Nick Schafer von Mailgun bestätigt, dass Ransomware Betrügern einen großen Zahltag bescheren kann. Er sagt aber auch, dass die schiere Anzahl der E-Mail-Phishing-Angriffe dies zu einer obersten Sicherheitspriorität jedes Unternehmens machen sollte.

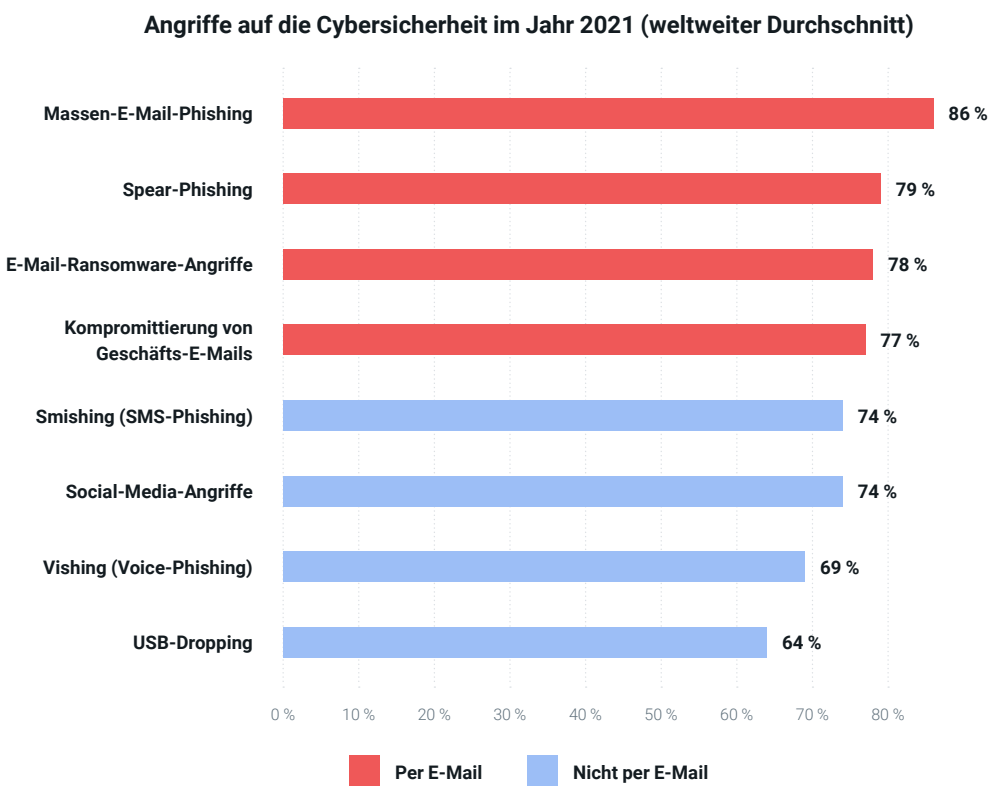
„Aus meiner Sicht ist Phishing das Hauptproblem. Ich bin mir sicher, dass Betrüger wie alle anderen auch über den Return on Investment nachdenken, und einen hohen ROI bekommen sie durch Ransomware-Angriffe. Wie können sehen, dass die Anzahl der Phishing-Angriffe immer mehr zunimmt. Und die Betrüger sind gut in dem, was sie tun."

Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

Vergleich von E-Mail-Bedrohungen mit anderen Kanälen

Der Proofpoint-Bericht State of the Phish aus dem Jahr 2022 untersuchte, wie E-Mail-Phishing und andere Formen von Phishing Unternehmen auf der ganzen Welt beeinträchtigen. Befragt wurden Hunderte von IT-Fachleuten und Tausende von Mitarbeitern in den USA, in Australien, Frankreich, Deutschland, Japan, Spanien und Großbritannien.

Während Unternehmen aus diesen Ländern alle Arten von Bedrohungen auf verschiedenen Kanälen erlebten, **belegten E-Mail-basierte Angriffe die ersten vier Plätze**. Insgesamt gaben 86 % der Unternehmen in der Proofpoint-Umfrage an, dass sie mindestens einen Massen-E-Mail-Phishing-Angriff im Jahr 2021 verzeichnet haben, womit dies die häufigste Angriffsart war.



Von allen verschiedenen Arten von Phishing-Versuchen **gaben 83 % der weltweiten Befragten an, dass mindestens ein Angriff im Jahr 2021 erfolgreich war**.

Die Auswirkungen von Phishing

Wir haben bereits aufgezeigt, dass die potenziellen finanziellen Schäden einer Sicherheitsverletzung sehr hoch sein können, aber die Unsummen an Geld, die nach einem Cyberangriff ausgegeben werden, sind nicht die einzige Art und Weise, wie sich diese Vorfälle auf Unternehmen jeder Größenordnung auswirken.

In der Umfrage von Proofpoint wurden IT-Experten aus aller Welt nach den größten Auswirkungen erfolgreicher Phishing-Angriffe auf ihr Unternehmen befragt. Am häufigsten wurden der Verlust von Kundendaten (54 %), kompromittierte Zugangsdaten (48 %) und Infizierung mit Ransomware (46 %) genannt.

Die stärksten Auswirkungen erfolgreicher Phishing-Angriffe

54 %
Verletzung von Kunden-/ Auftraggeberdaten

48 %
Kompromittierung von Zugangsdaten/ Konten

46 %
Infizierung mit Ransomware

Nicht weit hinter der Infizierung mit Ransomware gaben laut Proofpoint **44 % der Befragten den „Verlust von Daten und geistigem Eigentum" als weitere negative Auswirkung eines erfolgreichen Phishing-Angriffs an**. All diese Faktoren können dauerhafte Auswirkungen auf ein Unternehmen haben, das Vertrauen untergraben, die Kosten explodieren lassen und sogar Geschäftsgeheimnisse enthüllen, die Unternehmen einen Wettbewerbsvorteil verschaffen.

Priorisierung von Sicherheitsprojekten

Worauf sollten sich also Technikteams konzentrieren, wenn es darum geht, Sicherheitsverletzungen zu vereiteln? Angesichts der zitierten Statistiken sollte es nicht überraschen, dass der Schutz von **E-Mails bei vielen Unternehmen ein vorrangiges Sicherheitsanliegen ist**.

GreatHorn hat Hunderte von IT- und Cybersicherheitsexperten befragt, um herauszufinden, was ihnen die größten Sorgen bereitet. Die drei wichtigsten Projektarten, die von den Befragten im Jahr 2021 genannt wurden, waren E-Mail-Sicherheit (48 %), Sicherheit rund um die Fern- und Telearbeit (41 %) sowie Cloud-Sicherheitslagen-Management bzw. CPSM (40 %).

Die wichtigsten Sicherheitsprojekte im Jahr 2021

48 %
E-Mail-Sicherheit

41 %
Sicherheit von Telearbeit

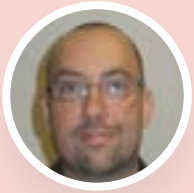
40 %
Cloud-Sicherheitslagen-Management (CPSM)

Ein spezifischeres IT-Projekt, das mit all diesen Sicherheitsanliegen zusammenhängt, ist der Wechsel von einer lokalen E-Mail-Lösung hin zu einem Cloud-eigenen Ansatz. GreatHorn fand heraus, dass zwar lediglich 24 % der Umfrageteilnehmer immer noch eine lokale Lösung nutzen, **aber 77 % dieser Unternehmen planen, zu Anbietern mit Cloud-eigener E-Mail-Infrastruktur zu wechseln**. Dies ermöglicht es Versendern, Anbieter zu finden, die erweiterte Sicherheitsmaßnahmen bieten, einschließlich Partnerschaften mit zuverlässigen öffentlichen Cloud-Computing-Diensten wie Amazon Web Services (AWS), Google Cloud Platform (GCP) und Microsoft Azure.

Die Cybersicherheit im Bereich E-Mail bzw. auch in jedem anderen Bereich zu verbessern, erfordert natürlich Zeit, Ressourcen und Budget. Ein zu geringes Budget für Cybersicherheit kann jedoch dazu führen, dass Technikteams die Hände gebunden sind.

Der Mimecast-Bericht „State of Email Security" aus dem Jahr 2022 ergab, dass **95 % der Unternehmen mit einem defizitären Budget für Cybersicherheit der Meinung sind, dass dies die Widerstandsfähigkeit beeinträchtigt und zu einem Mangel an Bereitschaft geführt hat**. Dem Bericht zufolge sind Maßnahmen wie Schulungen zum Sicherheitsbewusstsein und neue Technologien zwei Bereiche, in denen es an Mitteln mangelt.

Dan Ross leitet das Team Governance, Risk, and Compliance (GRC) bei Mailgun von Sinch. Er sagt, die Selbstverpflichtung unseres Unternehmens, in starke Sicherheit zu investieren, ist ein klarer Pluspunkt für sein Team, unsere Kunden und alle unsere Mitarbeiter.



„Die Führungsetage hat uns dankenswerterweise das Budget zur Verfügung gestellt, das benötigt wird, um unser Unternehmen und die Daten unserer Kunden mit der besten Technologie der Branche zu schützen. Ich denke, was Mailgun als führendes Unternehmen im Sicherheitsbereich auszeichnet, sind die Art und Weise, wie wir auf bekannte Bedrohungen reagieren und die Tools, mit denen wir sicherstellen, dass Betrüger von unserem Netzwerk ferngehalten werden. Und auch intern haben wir Maßnahmen ergriffen, um die Mitarbeiter im Wesentlichen vor sich selbst zu schützen."

Dan Ross, Leitender Manager GRC, Mailgun

TEIL 4

An vorderster Front der E-Mail-Sicherheit

Es gibt verschiedene Stellen, an denen die E-Mail-Sicherheit gefährdet sein könnte:

1. Am Speicherort von E-Mail-Daten und Kontaktinformationen
2. Auf gemeinsam genutzten E-Mail-Versandplattformen
3. Während der Übermittlung von Nachrichten, oder während sie vom ESP an die Empfänger versendet werden
4. Wenn eine E-Mail zur Authentifizierung und Filterung im Posteingang eingeht
5. Nachdem eine Nachricht eingegangen ist und im Posteingang des Empfängers liegt

Bestimmte Beteiligte tragen dabei besondere Verantwortung für die Sicherheit und den Schutz der Privatsphäre auf dem Weg dorthin. Lassen Sie uns jeden der oben genannten Bereiche genauer anschauen und mehr darüber erfahren, was nötig ist, um in allen Bereichen eine zuverlässige E-Mail-Sicherheit zu erreichen.

E-Mail-Sicherheit und Datenspeicherung

Unabhängig davon, ob E-Mail-Daten lokal oder in der Cloud gespeichert werden, sollten sie im Ruhezustand durch Verschlüsselung geschützt werden. **Mailgun verwendet zum Beispiel für sämtliche Kundendaten im Ruhezustand eine AES-256-Verschlüsselung**. Das bedeutet, dass ein 256-Bit-Schlüssel erforderlich ist, um Nachrichtenblöcke zu ver- und entschlüsseln.

AES ist eine weltweit eingesetzte Open-Source-Methode. Sie gilt als wirksames Verfahren, um Brute-Force-Angriffe zu verhindern, und wird von Regierungsbehörden wie der US-amerikanischen Nationalen Sicherheitsbehörde NSA zur Datenverschlüsselung eingesetzt. Führende öffentliche Cloud-Anbieter wie GCP, AWS und Azure verwenden ebenfalls die AES-256-Verschlüsselung.

Die meisten Versender mit hohem E-Mail-Aufkommen setzen bereits auf Cloud-basierte Lösungen. Wenn Sie sich für Partner entscheiden, die E-Mail-Adressen oder andere sensible Daten in Ihrem Namen speichern, gibt es weitere Sicherheitsmaßnahmen, die zum Schutz dieser Informationen in den Datenzentren beitragen. Dazu gehören etwa Maßnahmen wie die Zugangskontrolle zu Datenzentren mit 24-Stunden-Überwachung und biometrischen Kontrollsystemen.

Datenverarbeitung bei Mailgun.

Lesen Sie unsere Vereinbarung über die Datenverarbeitung (AV-Vertrag). Informieren Sie sich über die rechtlichen Details und erfahren Sie, wie wir die Datenverarbeitung und die Einhaltung von Vorschriften für unser Unternehmen und auch im Auftrag unserer Kunden handhaben.

E-Mail-Sicherheit und Absender-Reputation

Wenn Sie einen E-Mail-Service-Provider wie Mailgun nutzen, haben Sie oft die Möglichkeit, Abonnements zu wählen, die entweder dedizierte Adressen oder shared IP(-Adressen) für den E-Mail-Versand verwenden.

Wenn Ihr E-Mail-Aufkommen nicht besonders hoch ist, ist eine shared IP(-Adresse) in der Regel ausreichend. Doch was passiert, wenn Sie E-Mails von derselben IP wie ein Betrüger versenden? **Das könnte dazu führen, dass Ihre Absender-Reputation darunter leidet**.

E-Mail-Anbieter verwenden verschiedene Faktoren, um die Absender-Reputation zu bewerten. Zwei der wichtigsten sind die IP und die Domain-Reputation.

Es scheint, dass E-Mail-Anbieter wie Gmail der Domain-Reputation mittlerweile eine größere Bedeutung beimessen. Dies liegt daran, dass sie stärker auf bestimmte Absender ausgerichtet ist. Viele Domains können von einer einzigen IP-Adresse aus versenden. Die Domain-Reputation ist daher enger mit einem bestimmten Unternehmen oder einer bestimmten Marke verbunden. Die IP-Reputation spielt jedoch immer noch eine wichtige Rolle, insbesondere beim E-Mail-Client Outlook. Mit anderen Worten: **Die IP-Reputation kann einen sehr großen Einfluss auf B2B-E-Mails haben**.

Unter anderem aus diesem Grund arbeitet Mailgun hart daran, Betrüger daran zu hindern, unsere Plattform zum E-Mail-Versand über shared IP-Adressen zu nutzen. Nick Schafer und das Team für Zustellbarkeit und Einhaltung überprüfen und durchleuchten neue Benutzer, bevor sie die Plattform nutzen dürfen.

„Wenn betrügerische Absender auf eine unserer shared IPs gelangen, werden die E-Mail-Anbieter darauf aufmerksam. Die Absender-Reputation anderer Kunden mit derselben IP könnte Schaden nehmen, da der E-Mail-Anbieter die shared IP als einen Ort ansieht, an dem zwielichtige Aktivitäten stattfinden. Deshalb ist es uns ein Anliegen, sowohl Betrüger zu stoppen als auch dafür zu sorgen, dass unsere Kunden sich richtig verhalten. Auf diese Weise schützen wir die Reputation von Mailgun als Absender, was für Benutzer mit shared IP-Adressen sehr wichtig ist.“

Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

Mailgun-Kunden sind außerdem verpflichtet, sich an unsere Nutzungsrichtlinie (AUP) zu halten. Auf diese Weise schützen wir auch die Absender-Reputation aller Benutzer. **Unsere Nutzungsrichtlinie beinhaltet (unter anderem) folgende Bedingungen**:

- Maximale Bounce-Rate 5 %
- Maximale Abmelderate 1,4 %
- Maximale Spam-Beschwerderate 0,8 %
- Keine gekauften, gemieteten oder illegal gesammelten Kontaktlisten
- Es ist die ausdrückliche Empfängerzustimmung für Nachrichten einzuholen, die keine Transaktions-E-Mail sind
- Jede E-Mail muss einen Abmelde-Link beinhalten
- Die Speicherung, Übermittlung oder Veröffentlichung von verbotenen Inhalten (Kleinkredite, illegale Glücksspiele, verleumderisches Material, gewaltverherrlichende Inhalte usw.) ist untersagt
- Die exzessive Nutzung von gemeinsam genutzten Plattform-Ressourcen ist zu vermeiden

Die Nutzungsrichtlinie stellt sicher, dass wir alle zusammenarbeiten, um als Versender Best Practices in einer gemeinsamen digitalen Umgebung einzuhalten. Sie dient nicht dazu, jemanden zu verschrecken oder zu bedrohen. Die Nutzungsrichtlinie ist vielmehr ein Verhaltenskodex.

„Dies sind die Richtlinien, die wir bei den Mailgun-Kunden überwachen. Aber wenn jemand einen dieser Schwellenwerte überschreitet, schließen wir ihn nicht unbedingt von der Plattform aus. Wir wissen, dass manchmal Dinge passieren können. Deshalb raten wir in so einem Fall zunächst, sich um die Sache zu kümmern."

Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

Verschlüsselung: E-Mail-Sicherheit während der Übertragung

SMTP ist ein einfaches E-Mail-Übertragungsprotokoll und der Standard für die E-Mail-Übertragung. SMTP-Server verarbeiten E-Mails, indem sie Nachrichten von einem Server zum anderen versenden, empfangen und weiterleiten. Aber SMTP hat ein ziemlich großes Problem: Es ist nicht sicher.

SMTP in seiner Grundform unterstützt keine Verschlüsselungs- oder Authentifizierungsalgorithmen. Dies ist ein weiterer Grund, warum Spammer und Betrüger das E-Mail-Format nutzen und warum eigenständige E-Mail-Authentifizierungsprotokolle wie SPF und DKIM entwickelt wurden.

Spammer und Phisher haben häufig SMTP-Server ausgenutzt, die mit offenen Relays konfiguriert sind. Aber auch passwortgeschützte SMTP-Server können gehackt werden, wodurch die in den E-Mails enthaltenen Daten offengelegt werden. Betrüger können SMTP nutzen, um Viren und Malware zu verbreiten und DoS-Angriffe durchzuführen. Es ist sogar möglich, eine Nachricht zu verändern, während die E-Mail auf dem Weg zu einem Empfänger ist. Das heißt, Daten müssen auch während der E-Mail-Übertragung geschützt werden.

Versender und ESPs fügen deshalb Verschlüsselungsprotokolle wie Transport Layer Security (TLS) und Secure Sockets Layer (SSL) zu SMTP hinzu. Mailgun hat die Unterstützung von SSL bereits 2014 aufgrund der Sicherheitslücke POODLE eingestellt, die Man-in-the-Middle-Angriffe (MTM) zuließ.

TLS verwendet eine asymmetrische Verschlüsselung, um zwischen Client und Server eine sichere Sitzung aufzubauen. Dann wird eine symmetrische Verschlüsselung verwendet, um Daten innerhalb der gesicherten Sitzung auszutauschen. Der Vorgang, bei dem die Kommunikation zwischen einem Client und einem Server hergestellt und definiert wird, wird als TLS-Handshake bezeichnet.

Mailgun verwendet jetzt für E-Mails standardmäßig die sogenannte **opportunistische TLS-Verschlüsselung** (TLS-Version 1.2), die bei Bedarf versucht, ein Upgrade auf TLS durchzuführen, aber zum Klartext-Protokoll SMTP wechselt, wenn TLS nicht unterstützt wird. Auf diese Weise wird die Zustellbarkeit sichergestellt.

Sie können zur opportunistischen TLS-Verschlüsselung auch Kennzeichnungen (Flags) hinzufügen, um die Verbindungseinstellungen für die E-Mail-Zustellung anzupassen. Diese sind `TLS erforderlich` und `Validierung überspringen`.

- `TLS erforderlich:`
  - Bei TRUE stellt der empfangende Server eine Nachricht nur dann zu, wenn der Server TLS unterstützt.

  - Bei FALSE versuchen wir, ein Upgrade durchzuführen, liefern aber ein einfaches E-Mail-Übertragungsprotokoll in Klartext, wenn das Upgrade nicht erfolgreich ist.
- `Validierung überspringen`
  - Bei TRUE versuchen wir beim Aufbau einer TLS-Verbindung nicht, das Zertifikat und den Hostnamen zu validieren.
  - Bei FALSE versuchen wir, das Zertifikat zu validieren. Ist keine Validierung möglich, wird keine TLS-Verbindung hergestellt.

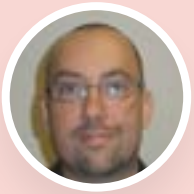
Erfahren Sie mehr über TLS und E-Mail.

Wir informieren Sie über die Verschlüsselung der E-Mail-Kommunikation und wie die TLS-Verbindungskontrolle bei Mailgun funktioniert.

Mailgun empfiehlt häufig die Verwendung unserer E-Mail-API anstelle eines einfachen E-Mail-Übertragungsprotokolls (SMTP). Die API ist bis zu dreimal schneller, einfach zu bedienen und ideal für den Versand eines großen E-Mail-Aufkommens. Mailgun bietet außerdem die Möglichkeit, für die Verwaltung mehrerer Absender unterschiedliche Domain-Schlüssel für den Versand zu verwenden. Hacker können jedoch möglicherweise sowohl auf die Zugangsdaten einfacher E-Mail-Übertragungsprotokolle als auch auf API-Schlüssel zugreifen.

Deshalb ist es so wichtig, API-Schlüssel regelmäßig zu ändern und Ihre SMTP-Passwörter zu schützen. Jonathan Torres von Mailgun betont, dass die unbeabsichtigte Preisgabe von API-Schlüsseln und SMTP-Zugangsdaten zu den häufigsten Arten gehört, wie die E-Mail-Sicherheit beeinträchtigt wird.

Dan Ross weist darauf hin, dass E-Mail-Daten auch dann geschützt werden müssen, wenn Kontaktlisten zwischen Plattformen übertragen werden. Denn dies ist eine weitere Situation, in der sensible Daten während der Übermittlung einem Risiko ausgesetzt sind.



„Es ist wichtig, dass Sie verstehen, wie die E-Mail-Adressen und Kontakte in die Tools gelangen, die Sie für den Versand Ihrer Nachrichten verwenden. Mailgun verfügt über eine sichere API, die uns in der Branche auszeichnet. Unsere Kunden nutzen diese API, um E-Mails und E-Mail-Adressen in einer unglaublichen Geschwindigkeit hochzuladen. Wenn Sie eine sichere Schnittstelle haben, verringert sich das Risiko, dass die Daten während der Übertragung abgefangen werden."

Dan Ross, Leitender Manager GRC, Mailgun

E-Mail-Sicherheit und Authentifizierung

Wenn Betrüger versuchen, sich mithilfe von Phishing-E-Mails als Ihr Unternehmen auszugeben, gibt es einige äußerst effektive Methoden, um zu verhindern, dass solche E-Mails im Posteingang landen. **E-Mail-Authentifizierungsprotokolle helfen E-Mail-Anbietern dabei, zu bestimmen, ob E-Mails gefälscht sein könnten,** bevor die Nachrichten an die Empfänger zugestellt werden.

E-Mail-Authentifizierungsprotokolle wurden Anfang der 2000er Jahre entwickelt, um die Sicherheit von SMTP zu erhöhen und einen Anstieg von E-Mail-Spam zu verhindern. SPF und DKIM waren die ersten weit verbreiteten Methoden. Kurz darauf wurde DMARC eingeführt, eine Richtlinie zur Bestätigung und Erweiterung von SPF und DKIM. Im nächsten Abschnitt werden wir diese Protokolle ausführlich behandeln.

Bei Mailgun verpflichten wir die Benutzer dazu, sowohl SPF- als auch DKIM-Einträge auf ihren DNS-Servern (Domain Name System) einzurichten. Wenn Sie das noch nicht getan haben oder Unterstützung dabei brauchen, können wir Ihnen helfen. Wir empfehlen außerdem dringend die Durchsetzung einer DMARC-Richtlinie und können unsere Kunden bei Bedarf an vertrauenswürdige Service-Provider verweisen. **Das Einrichten von DNS-Einträgen zur Authentifizierung verbessert darüber hinaus auch die Absender-Reputation und die E-Mail-Zustellbarkeit.**

„E-Mail-Anbieter brauchen Möglichkeiten, um die wahre Identität des Absenders erkennen zu können. Ohne E-Mail-Authentifizierung ist nur schwer feststellbar, woher der E-Mail-Verkehr wirklich stammt. Die Authentifizierung ermöglicht dem Absender zu sagen: Diese Nachricht ist von uns, es ist unser E-Mail-Verkehr, und wir dürfen das tun."

Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

E-Mail-Sicherheit und Bewusstsein

Bei der E-Mail-Sicherheit kann die Unwissenheit der Empfänger *definitiv Schaden anrichten*. Aber eine gut geschulte Belegschaft und versierte Abonnenten werden Spammer und Betrüger viel eher erkennen, bevor es zu einem großen Fehler kommt.

Dan Ross von Mailgun sagt, dass ein **Mitarbeiterprogramm zur Schulung des Bewusstseins für die E-Mail-Sicherheit unerlässlich ist**. Man darf nicht vergessen, wie häufig Spear-Phishing und die Kompromittierung geschäftlicher E-Mails geworden sind. Diese Angriffe zielen auf Mitarbeiter in Ihrem Unternehmen ab. Im Idealfall sollten Schulungen und Tests jährlich und bei jeder Neueinstellung stattfinden.

Sie können die Schulung auch auf die Probe stellen, indem Sie im Laufe des Jahres Ihre eigenen „Phishing"-E-Mails an Ihre Mitarbeiter versenden (gewissermaßen gefälschte Fake-E-Mails). Auf diese Weise können Sie einschätzen, wie aufmerksam Ihre Mitarbeiter sind, und haben die Gelegenheit, alle daran zu erinnern, worauf sie bei einem Phishing-Versuch achten müssen.

„Bei Mailgun verschicken wir solche gefälschten Phishing-E-Mails, und wenn ein Mitarbeiter darauf klickt, führen wir ein Gespräch, um dem Kollegen zu erklären, warum er vorsichtiger sein muss. Wir tracken diese Metriken und tun, was wir können, um unsere Mitarbeiter für Phishing zu sensibilisieren."

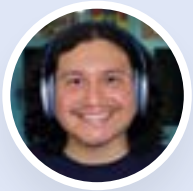
Dan Ross, Leitender Manager GRC, Mailgun

Um es poetisch auszudrücken: Ihre E-Mail-Sicherheit ist nur so stark wie Ihre größte Schwachstelle. Und in fast jedem Unternehmen ist die Schwachstelle ein Mensch, nicht die Technologie.

Laut dem Bericht „State of Email Security" von Mimecast aus dem Jahr 2022 ist die Wahrscheinlichkeit, dass **Mitarbeiter, die eine Schulung zum Thema Cyberbewusstsein durchlaufen haben, bösartige Links erkennen und sie nicht anklicken, fünfmal höher**. Obwohl fast alle befragten Unternehmen eine Art von Training bzw. Schulung haben, bieten nur 34 % diese regelmäßig an. Und dies trotz der Tatsache, dass vier von zehn Befragten die Naivität der Mitarbeiter im Jahr 2022 als große Herausforderung für die E-Mail-Sicherheit bezeichneten.

Auch das Bewusstsein von Kunden und Abonnenten ist wichtig. Wenn Ihr Unternehmen für Phishing-Angriffe und Spoofing anfällig ist, oder wenn Sie von betrügerischen E-Mails erfahren, die sich als E-Mails Ihres Unternehmens ausgeben, sollten Sie proaktiv auf die Situation reagieren. Warten Sie nicht, bis noch größerer Schaden eintritt. Warnen Sie Ihre Kunden und Abonnenten vor diesen Betrugsmaschen. Machen Sie deutlich, welche Arten von Informationen Sie per E-Mail abfragen und welche nicht.

Leider kommen die meisten Unternehmen erst auf die Idee, ihre Kunden über die Risiken von Brand-Spoofing aufzuklären, nachdem eine negative Berichterstattung der Medien veröffentlicht wurde. Jonathan Torres hebt aber hervor, dass ein Spoofing-Vorfall für Unternehmen auch eine Gelegenheit darstellt, transparent zu sein und ein gewisses Vertrauen in Ihr Unternehmen wiederherzustellen.



„Das Letzte, was Sie wollen, ist, dass Ihr Unternehmen in einer E-Mail genannt wird, die seriös aussieht, aber den Empfänger in eine schlechte Lage bringt. Ich glaube, das erkennen Absender oft erst dann, wenn es schon zu spät ist. Und dann müssen Sie schnell handeln. Wenn Sie also Opfer von Spoofing geworden sind, seien Sie transparent. Gute Kommunikation ist alles. Erzählen Sie, was passiert ist, und welche Maßnahmen Sie treffen werden, um eine Wirkung zu entfalten, damit so etwas nicht noch einmal passieren kann."

Jonathan Torres, TAM-Teammanager, Mailgun

Wie genau können Sie also „die Wirkung entfalten", von der Jonathan spricht? Wenn Ihre Zugangsdaten versehentlich durchsickern, und jemand Spam von Ihrem Konto aus versendet, wird Mailgun das wahrscheinlich vor Ihnen erfahren und dem Spuk ein Ende setzen. Mailgun hilft Versendern auch dabei, den Zugriff auf API-Schlüssel und SMTP-Zugangsdaten einzuschränken, indem es Ihnen die Option gibt, Benutzerrollen innerhalb der Plattform zuzuweisen.

Unabhängig davon, welche Plattform Sie für den E-Mail-Versand verwenden, empfehlen wir dringend, API-Schlüssel und SMTP-Passwörter sofort zurückzusetzen und zu überprüfen, ob Ihre Absenderdomain aufgrund des Lecks auf eine Blockliste gesetzt wurde. Das Einrichten einer Zwei-Faktor-Authentifizierung (2FA) wird ebenfalls dazu beitragen, dass dieses Problem nicht mehr auftritt.

Können Versender noch mehr tun, um sich vor Brand-Spoofing zu schützen? Aber ja doch. **Es dreht sich alles um die E-Mail-Authentifizierung**, und mit diesem wichtigen Thema werden wir uns als Nächstes beschäftigen.

TEIL 5

Authentifizierung: Die letzte Verteidigungslinie

Die Stunde der Wahrheit bei der E-Mail-Übertragung schlägt, wenn ein E-Mail-Anbieter wie Gmail oder Outlook entscheiden muss, wie eine Nachricht gefiltert werden soll. Ist der Absender dieser E-Mail wirklich derjenige, für den er sich ausgibt? Handelt es sich um Spam? Ist der Absender gefährlich? Sollten wir diese Nachricht blockieren, sie als Junk einstufen oder in den Posteingang durchlassen?

Wie Kate Nowrouzi bereits erwähnt hat, gibt es auf diese Fragen nicht immer einfache Antworten, auch nicht, wenn man ein Anti-Spam-Experte ist. Deshalb hat die E-Mail-Branche **E-Mail-Authentifizierungsprotokolle** und andere technische Spezifikationen entwickelt, die im Wesentlichen die Identifizierung eines Absenders abfragen, bevor er in den Posteingang gelassen wird.

Protokolle und Spezifikationen haben jeweils einen eigenen DNS-TXT-Eintrag, der auf Domainnamen-Servern hinzugefügt und korrekt formatiert werden muss. Schauen wir uns vier wichtige Bereich der E-Mail-Authentifizierung an und klären wir die Frage, wie diese Bereiche helfen, wie sie funktionieren und wie sie untereinander zusammenarbeiten.

1. SPF-Authentifizierung

SPF-Authentifizierung (SPF) ist ein Protokoll, das die IP-Adressen von Mailservern und Domainnamen auflistet, die berechtigt sind, in Ihrem E-Mails zu versenden. Der SPF-Eintrag funktioniert wie ein Türsteher in einem Nachtclub. Wenn Sie nicht auf der Liste stehen, kommen Sie nicht rein.

Wenn Sie beispielsweise Transaktions-E-Mails über Mailgun versenden, einen anderen ESP für Marketing-E-Mails nutzen und Google Workspace für interne E-Mails verwenden, müssen alle drei in Ihrem SPF-Eintrag angegeben werden. Auf diese Weise können E-Mail-Anbieter, die E-Mails von nicht autorisierten Absendern bemerken, diese Nachrichten entweder blockieren oder als Spam filtern.

Die technischen Details

Hier ist ein Beispiel für einen SPF-DNS-Eintrag:

```
v=spf1
ip4:61.949.100.188 ip6:98.422.200.766 a:smtp.example.com -all
```

Schlüsseln wir den obigen DNS-TXT-Eintrag für SPF einmal auf:

Die verwendete SPF-Version:

Diese sollte immer „`v=spf1`“ (die erste Version) sein, da alle anderen Versionen eingestellt wurden.

Die Liste der autorisierten Absender:

Jede Domain, die in Ihrem Namen E-Mails versendet, sollte mithilfe von Mechanismen wie IP-Adressen, Hostnamen oder „`a“ -Einträgen aufgeführt`werden. Sie können alle Mechanismen desselben Typs verwenden oder sie untereinander kombinieren.

Es stehen mehrere Mechanismen zur Auswahl:

1. Der `ip4`- oder `ip6`-Mechanismus listet die tatsächlichen IP-Adressen auf, die autorisiert sind, in Ihrem Namen zu versenden.
2. Der „`a`“ **-Mechanismus** ermöglicht es dem Posteingangsserver, auf die „`a`“ -Einträge einer Domain statt auf eine bestimmte IP zu verweisen. Wenn die IP, von der die E-Mail stammt, in dem „`a`“-Eintrag gefunden wird, hält die E-Mail der SPF-Authentifizierung stand.
3. Der `MX` -Mechanismus zeigt die IP-Adressen an, die Ihre Domain zum Empfangen von E-Mails verwendet. Wenn eine E-Mail von einer dieser IPs versendet wird, sollte der Posteingangsserver sie akzeptieren.
4. Der „`include“`-Mechanismus wird auch verwendet, um den SPF-Eintrag der entsprechenden Domain mit einzubeziehen. Mailgun verwendet diesen Mechanismus, damit Kunden alle Mailgun-IPs zu ihrem SPF hinzufügen können.

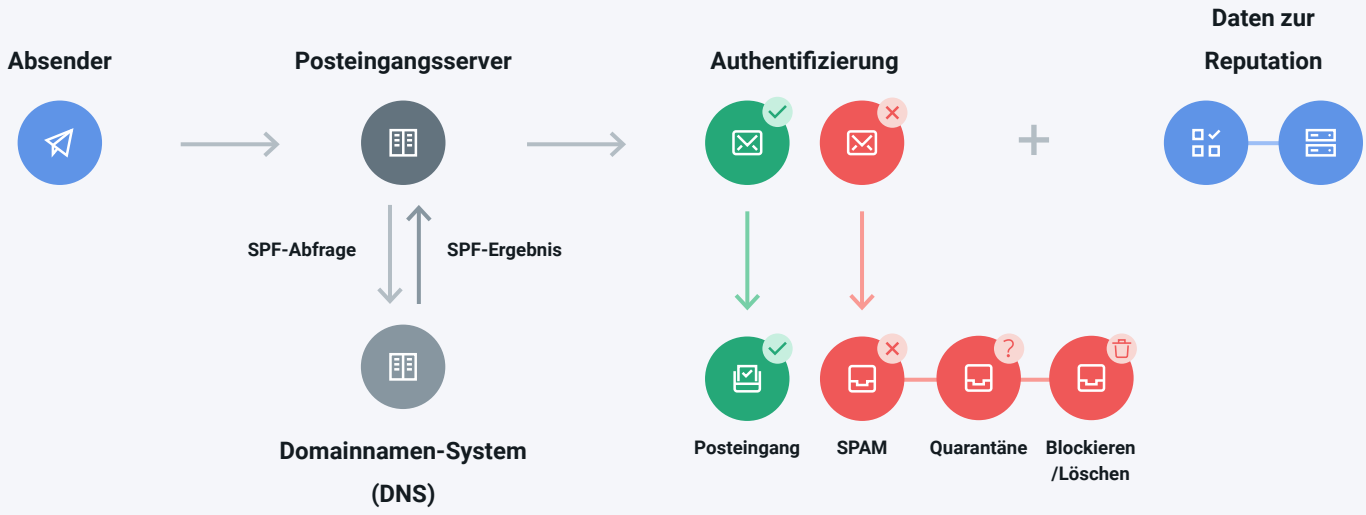
Der „all”-Mechanismus oder Fail Qualifier:

Am Ende jedes SPF-Eintrags ist ein „all”-Mechanismus enthalten. Er informiert die Posteingangsserver darüber, was zu tun ist, falls eine Nachricht nicht authentifiziert werden kann.

- `-all`: Wenn keine exakte Übereinstimmung gefunden wird, ist die E-Mail fehlgeschlagen. Die Nachricht wird blockiert und gelangt nicht in den Posteingang. Dies ist die beste Möglichkeit, SPF zu verwenden, um Spoofing zu verhindern.
- `~all`: Wenn keine exakte Übereinstimmung gefunden wird, ist die E-Mail fehlgeschlagen, wird aber dennoch zugestellt. Sie wird als verdächtig markiert und landet wahrscheinlich im Spam-Ordner.
- `+all`: Damit kann jeder Server von Ihrer Domain aus versenden. Dieser Mechanismus sollte nur selten verwendet werden, da alles der SPF-Authentifizierung standhält. Anders formuliert: Jeder kann sich für Sie als Absender ausgeben.
- `?all`: Dies ist eine neutrale Einstellung. Die Nachrichten bestehen oder scheitern nicht an der SPF-Authentifizierung, wenn die IP nicht gelistet ist. Die Entscheidung wird dem E-Mail-Anbieter überlassen.

> ***Eine Domain kann immer nur einen SPF-Eintrag haben:*** *Mehrere SPF-Einträge in einer Domain führen dazu, dass die Authentifizierung der Nachrichten fehlschlägt. Obwohl Internet-Service-Provider nicht immer Maßnahmen bei SPF-Fehlern ergreifen, ist dies ein wichtiger Teil des DMARC-Abgleichs, auf den wir später eingehen werden.*

Wie SPF-Authentifizierung funktioniert



Wenn E-Mail-Anbieter die SPF-Authentifizierung verwenden, prüft der Posteingangsserver den Return-Path im E-Mail-Header. Dann wird überprüft, ob die E-Mail von einer der im DNS-TXT-Eintrag aufgeführten IP-Adressen stammt.

Wenn der Posteingangsserver den Absender validiert, wird die E-Mail an den Posteingang zugestellt. Wird der Absender nicht gefunden, wird die E-Mail blockiert oder als Spam eingestuft, je nachdem, wie der Fail Qualifier (`all`-Mechanismus) definiert ist.

SPF hat einige Nachteile. Zum einen funktioniert es nicht, wenn eine E-Mail weitergeleitet wird, denn dann wird von einer IP versendet, die nicht im Datensatz aufgeführt ist. **SPF ist außerdem auf 10 Mechanismen (oder zulässige IPs) beschränkt**, was für große Unternehmen und Versender mit einem hohen E-Mail-Aufkommen und vielen Parteien, die im Namen der Hauptdomain versenden, gegebenenfalls nicht ausreicht.

2. DKIM

DKIM ist ein Authentifizierungsprotokoll, das zwei Methoden miteinander kombiniert, um E-Mail-Fälschung zu verhindern: „DomainKeys“ von Yahoo und „Identified Internet Mail“ von Cisco.

Wie bei SPF beinhaltet die DKIM-Authentifizierung einen DNS-TXT-Eintrag, auf den Posteingangsserver verweisen, wenn sie die Authentizität eines Absenders überprüfen. Die DKIM-Authentifizierung ist jedoch etwas fortschrittlicher. Mithilfe von DKIM lässt sich auch feststellen, ob eine Nachricht während der Übertragung verändert wurde. Heutzutage überprüfen alle großen E-Mail-Anbieter E-Mails auf DKIM.

DKIM verwendet chiffrierte Schlüssel, die auch als digitale Signaturen bezeichnet werden. Der geheime Schlüssel wird in den Header einer E-Mail eingefügt, um die Nachricht einer bestimmten Domain zuzuordnen und den Absender zu validieren. Der chiffrierte DKIM-Schlüssel wird mit einem öffentlichen Schlüssel gekoppelt, der im DNS-TXT-Eintrag zu finden ist.

Die technischen Details

Hier ist ein Beispiel für einen DKIM-DNS-Eintrag:

```
dk1024-2012._domainkey.example.com TXT "v=DKIM1; t=y; k=rsa;
p=MIGfMA0GCSqGSiuTHjQWercnvEr54A2CA;"
```

Schlüsseln wir den DNS-TXT-Eintrag für eine DKIM-Signatur auf:

- `v=` Die verwendete Protokollversion
- `t=` Dieses optionale Tag zeigt an, dass die Absenderdomain DKIM testet
- `k=` Die Art des Schlüssels, üblicherweise rsa
- `p=` Der öffentliche Schlüssel, der mit der verschlüsselten DKIM-Signatur gekoppelt ist
- Der öffentliche Schlüssel ist das einzige erforderliche Tag im DNS-Eintrag (`p=`). Der DKIM-Eintrag enthält auch die Absenderdomain und den sogenannten Selektor, mit dessen Namen bzw. Nummer der Absender den Posteingangsservern mitteilt, wo der öffentliche Schlüssel zu finden ist. **Der DKIM-Signatur-Header** wird den E-Mail-Nachrichten hinzugefügt und enthält die Authentifizierungsdaten, die Posteingangsserver benötigen, um die Echtheit einer Nachricht zu validieren.

Hier ist ein Beispiel eines DKIM-Headers:

```
DKIM-Signatur v=1; a=rsa-sha256; q=dns;
d=example.com;
s= dk1024-2012; t=1117574938; x=1118006938;
h=Content-Typ: Mime-Version: Betreff: Von: An: Absender; Datum:
List-
Abmelden
bh=PV3AoaeTApQYJwe3qgbuUFFTVhjwhv1q2gGNBL+KHU=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4lszZVoG00lszZVoG4ZHRNiYzR
```

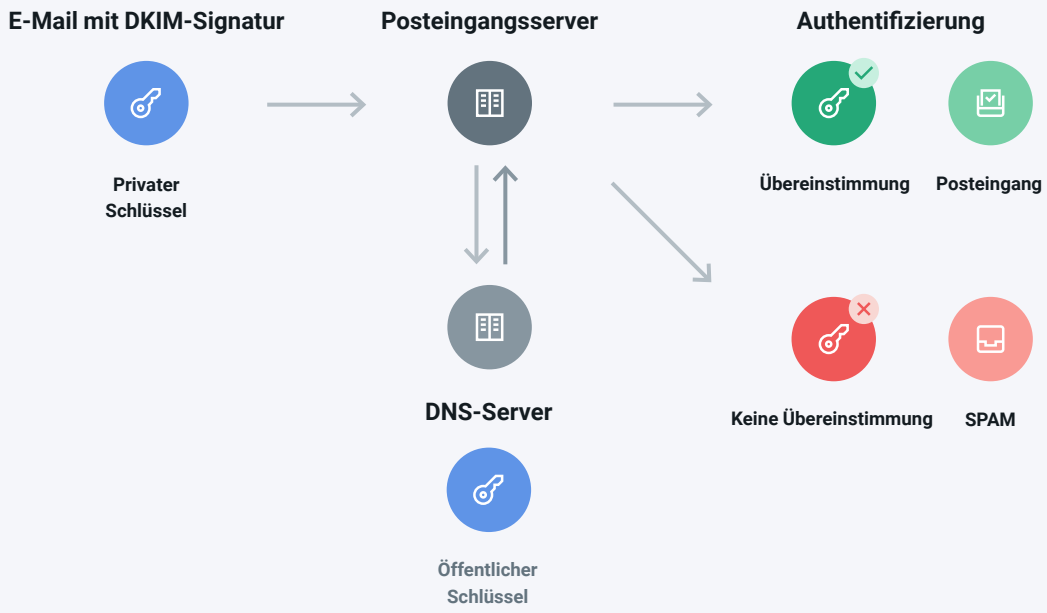
Hier ist eine Aufschlüsselung der Tags, die in den DKIM-Header-Informationen enthalten sind:

- `v=` Die verwendete DKIM-Version
- `a=` Der Signaturalgorithmus
- `q=` Das Standard-Abfrageverfahren
- `d=` Die mit einem Selektor-Eintrag verknüpfte signierende Domain, um einen öffentlichen Schlüssel zu finden

- `s=` Der Selektor, der zum Auffinden des öffentlichen Schlüssels verwendet wird und mehrere Schlüssel in einer Domain zulässt
- `t=` Der Signaturzeitstempel
- `x=` Die Ablaufzeit
- `h=` Die Liste der Header, die im Signieralgorithmus verwendet werden
- `bh=` Der Body-Hash nach dem vorschriftsgemäßen Informbringen durch Base64, wodurch Binärcode in Text umgewandelt wird
- `b=` Die eigentliche DKIM-Signatur von Headern und Body, die mit Base64 codiert ist

Einige DKIM-Tags, die zu den Header-Informationen hinzugefügt werden können, sind optional. Andere sind erforderlich: `v`, `a`, `d`, `s`, `h`, `bh` und `b`. Wieder andere, wie `t` und `x`, sind optional, werden jedoch empfohlen.

Wie DKIM-Authentifizierung funktioniert



Anhand einer DKIM-Signatur können E-Mail-Anbieter und Mail Transfer Agents (MTAs) erkennen, wo der öffentliche Schlüssel abgerufen werden kann. Wenn der öffentliche Schlüssel mit der verschlüsselten Signatur übereinstimmt, ist es wahrscheinlicher, dass die E-Mail-Anbieter die Zustellung an den Posteingang erlauben. Ohne Übereinstimmung oder gar ohne DKIM-Signatur wird die E-Mail mit größerer Wahrscheinlichkeit abgelehnt oder als Spam eingestuft.

DKIM selbst filtert keine E-Mails. Es hilft jedoch den empfangenden Mailservern zu entscheiden, wie eingehende Nachrichten am besten gefiltert werden sollen. Eine erfolgreiche DKIM-Validierung bedeutet für eine Nachricht oft eine geringere Spambewertung.

3. DMARC

Streng genommen handelt es sich beim Domain Message Authentication Reporting (DMARC) nicht um ein Authentifizierungsprotokoll. Es ist vielmehr eine technische Spezifikation, die eine Richtlinie für die E-Mail-Authentifizierung definiert. DMARC hilft Absendern und E-Mail-Anbietern dabei, SPF und DKIM optimal einzusetzen, und gibt Ihnen gleichzeitig Aufschluss darüber, wer versucht, unter Ihrer Domain zu versenden.

Der Hauptzweck einer DMARC-Richtlinie besteht darin, SPF- und DKIM-Abgleiche zu überprüfen. Sie gilt außerdem als effektivste Methode, um zu verhindern, dass sich Betrüger per E-Mail als Ihr Unternehmen ausgeben. Wenn DMARC implementiert ist, überprüfen die E-Mail-Anbieter sowohl SPF als auch DKIM und verweisen dann auf die vom Absender im DMARC-DNS-Eintrag definierte Richtlinie.

Es gibt folgende DMARC-Richtlinienoptionen:

- **Ablehnen:** Nachrichten, die DMARC nicht standhalten, werden nicht zugestellt (`p=reject`).
- **Quarantäne:** Nachrichten, die DMARC nicht standhalten, landen im Spam-Ordner (`p=quarantine`).
- **Keine:** Lässt Nachrichten unabhängig vom Ergebnis durch. Diese Option wird nur für Berichte oder während der Einrichtung und Testung von DMARC verwendet. (`p=none`).

Die technischen Details

```
1  v=DMARC1; p=quarantine; sp=none; rua=mailto:dmarc-reports@example.com; pct=100; aspf=s; adkim=s
```

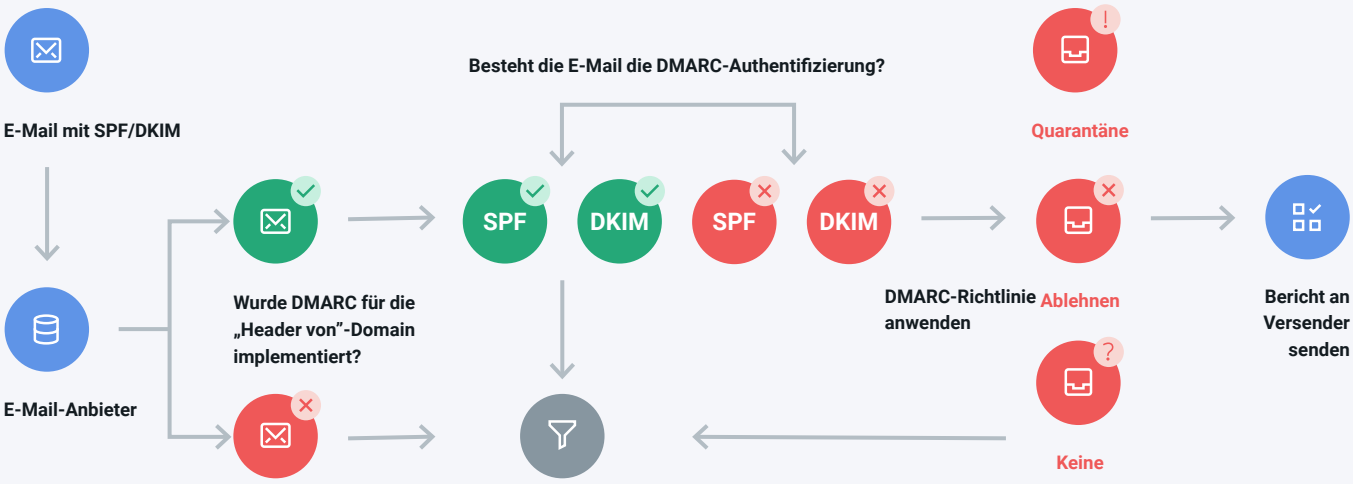
DMARC-Einträge können einfacher oder auch komplexer sein, je nachdem, wie viele Tags ein Absender verwenden möchte. Hier ist eine vollständige Liste der möglichen DMARC-Tags mit Erläuterungen:

- `v=` Die verwendete DMARC-Version.
- `p=` Die DMARC-Durchsetzungsrichtlinie: Keine, Quarantäne oder Ablehnen.
- `rua=` Eine Liste der E-Mail-Adressen, an die DMARC-Berichtszusammenfassungen versendet werden.
- `pct=` Der Prozentsatz der Nachrichten, die unter die Durchsetzungsrichtlinie fallen. Standardmäßig ist pct=100.
- `aspf=` Definiert den Abgleichmodus für SPF, der bei Pass/Fail-Szenarien streng oder locker sein kann.
- `adkim=` Definiert den Abgleichmodus für DKIM, der bei Pass/Fail-Szenarien streng oder locker sein kann.
- `sp=` Stellt verschiedene Durchsetzungsrichtlinien für Subdomains dar.
- `ruf=` Listet E-Mail-Adressen für den Versand von DMARC-Fehler-/forensischen Berichten auf, die detaillierter sind als Berichtszusammenfassungen.
- `fo=` Gibt die Optionen für die Erstellung eines DMARC-Fehler-/forensischen Berichts an.
- `rf=` Gibt das forensische Berichtsformat für nachrichtenspezifische Fehlerberichte an.

- `ri=` Legt das Intervall für den Versand von DMARC-Berichten fest. Das Intervall wird in Sekunden angegeben, beträgt in der Regel aber 24 Stunden oder mehr.

In unserem DNS-TXT-Beispieleintrag hat der Absender eine DMARC-Richtlinie, die auf Quarantäne gesetzt ist, ohne dass es eine Unterscheidung für Subdomains gibt. Es gibt eine E-Mail-Adresse, an die Berichtszusammenfassungen geschickt werden sollen. 100 % der Nachrichten unterliegen der DMARC-Richtlinie, und sowohl der SPF- als auch der DKIM-Abgleichsmodus sind auf „streng" eingestellt. Wenn „streng" festgelegt ist und entweder SPF oder DKIM der Authentifizierung nicht standhalten, schlägt die gesamte DMARC-Prüfung fehl.

Wie eine DMARC-Richtlinie funktioniert



Wenn ein Versender DMARC implementiert hat, prüft der E-Mail-Anbieter, ob er SPF und DKIM standhält. Dann setzt es die im DNS-Eintrag angegebene Richtlinie durch und filtert die E-Mail entsprechend. Zuletzt erhält der Versender einen Bericht mit Informationen über den E-Mail-Verkehr, der im Namen der Domain versendet wurde, und wie damit umgegangen wurde.

DMARC-Berichte

DMARC-Berichte liefern aussagekräftige Erkenntnisse darüber, wie sich Nachrichten durch das E-Mail-Ökosystem bewegen, und wie oft Betrüger versuchen, E-Mails zu fälschen und sich als Ihr Unternehmen auszugeben. Vielleicht haben Sie schon bemerkt, dass es zwei Arten von DMARC-Berichten gibt: zusammengefasste und forensische Berichte.

Zusammengefasste DMARC-Berichte werden täglich versendet, sofern nicht anders angegeben. Sie umfassen:

- Alle Domains, die E-Mails mit Ihrer Domain im Feld „Von" versenden
- Die Versand-IP-Adresse für jede Domain im Bericht
- Ergebnisse der SPF- und DKIM-Authentifizierung

- E-Mails, die unter Quarantäne gestellt wurden (wenn Ihre Richtlinie `p=quarantine ist`)
- E-Mails, die blockiert wurden (wenn Ihre Richtlinie `p=reject ist`)
- Informationen über den gesamten täglichen E-Mail-Traffic

> ***Hinweis:*** *Sie sollten in Erwägung ziehen, eine dedizierte E-Mail-Adresse für den Empfang Ihrer DMARC-Berichte einzurichten. Ganz einfach aus dem Grund, weil tägliche E-Mails von jedem Internet-Service-Provider versendet werden, der Nachrichten mit Ihrer Domain im Feld „Von" erhält. Bei manchen Versender dürften das ziemlich viele E-Mails sein.*

Forensische DMARC-Berichte werden immer dann versendet, wenn eine E-Mail der DMARC-Authentifizierung nicht standhält, weil SPF und/oder DKIM nicht übereinstimmen. Diese Berichte werden auch als **Fehlerberichte** bezeichnet und sind sehr hilfreich, wenn Sie Spoofing-Vorfälle untersuchen wollen und zusätzliche Details über bestimmte Nachrichten benötigen. Forensische DMARC-Berichte enthalten zum Beispiel die Betreffzeile der betroffenen Nachrichten, die Felder `An:` und `Von:` sowie Informationen über Anhänge und URLs in diesen E-Mails.

Wenn Ihr Team für die E-Mail-Sicherheit zuständig ist, sind DMARC-Berichte wie regelmäßige Briefings, die Ihnen dabei helfen, Probleme zu erkennen und zu lösen, bevor sie außer Kontrolle geraten.

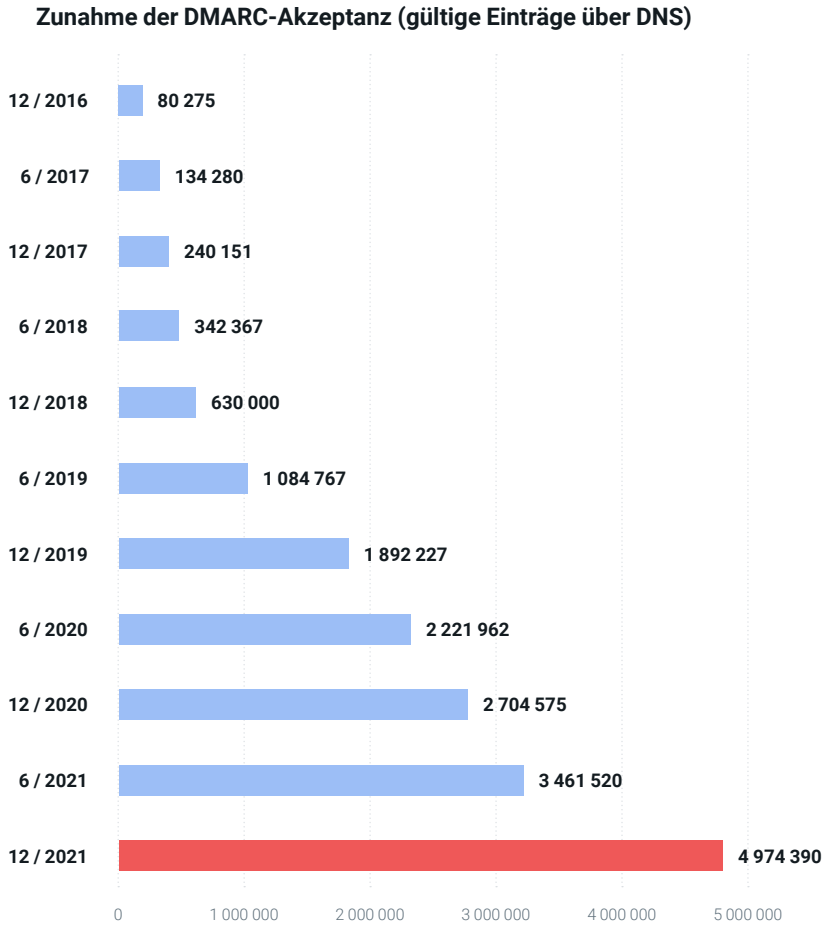
Wenn Ihr Team für die E-Mail-Sicherheit zuständig ist, sind DMARC-Berichte wie regelmäßige Briefings, die Ihnen dabei helfen, Probleme zu erkennen und zu lösen, bevor sie außer Kontrolle geraten.

„Als wir zum ersten Mal DMARC-Richtlinien für Mailgun eingerichtet haben, war es wirklich interessant, diese Berichte zu erhalten und den gesamten Datenverkehr zu sehen. Uns fielen all diese Stellen auf, die mailgun.com als Absenderdomain verwenden. Vieles davon war tatsächlich eigener Traffic, aber wir wussten davon nichts. Unser Marketingteam könnte zum Beispiel einen neuen Dienst ausprobieren, und die Protokolle sind nicht aufeinander abgestimmt. Dank der DMARC-Berichte sehen wir wenigstens, was passiert."

Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

Was ist die beste DMARC-Richtlinie?

Immer mehr Versender wissen DMARC zu schätzen. Jüngste Zahlen von DMARC.org zeigen, dass die Akzeptanz der Spezifikation im Jahr 2021 um 84 % gestiegen ist, zum Jahresenden hin gab es fast 5 Millionen eindeutige Einträge.



Jedoch gibt DMARC.org auch an, dass **annähernd zwei Drittel dieser Einträge (65,6 %) lockere Richtlinien haben, die auf p = none** stehen. Dies könnte daran liegen, dass einige Versender nur ihre DMARC-Berichte sehen wollen und zögern, eine strenge Richtlinie durchzusetzen, die fehlgeschlagene Nachrichten ablehnt oder unter Quarantäne stellt. Die Richtlinie p=none bietet die Vorteile der Berichterstattung, aber sie wird absolut nichts dazu beitragen, Phishing-Angriffe und Brand-Spoofing zu verhindern.

Kate Nowrouzi sagt, dass Mailgun seine Benutzer dazu animiert, strengere DMARC-Richtlinien durchzusetzen. Es ist natürlich völlig in Ordnung, mit einer lockeren Richtlinie zu beginnen, doch sollten Versender irgendwann den nächsten Schritt machen, um die E-Mail-Sicherheit zu erhöhen.

Mit dem `pct=` Tag in Ihrem DMARC-Eintrag können Sie **einen Prozentsatz der Nachrichten angeben, auf die Ihre Richtlinie angewendet werden soll**. Sie können dann die Auswirkungen der Richtlinie `p=quarantine` oder `p=reject` auf die Zustellbarkeit von E-Mails einschätzen, ohne dass DMARC sich auf alle Ihre ausgehenden E-Mails auswirkt. Anschließend können Sie alle Probleme mithilfe der Erkenntnisse, die Sie aus den DMARC-Berichten erlangen, beheben und den Prozentsatz, auf den die Richtlinie angewendet wird, schrittweise erhöhen.

Kate ist der Meinung, das eigentliche Ziel von DMARC bestehe darin, eine Richtlinie einzuführen, die E-Mail-Anbieter dabei unterstützt, legitime Absender zu validieren und Empfänger vor Betrügern zu schützen, die sich als Ihr Unternehmen ausgeben. Zunächst müssen die Versender jedoch ihre Angst vor DMARC überwinden.

„Viele bekannte Traditionsunternehmen halten DMARC immer noch für neu und haben einige Bedenken. Sie befürchten zum Beispiel, dass mit der Richtlinie p=reject ihre E-Mails blockiert werden, weil DMARC nicht richtig eingerichtet ist. Ich beobachte, dass viele Unternehmen damit prahlen, dass sie DMARC implementiert haben. Aber wenn ihre Richtlinie auf p=none gesetzt ist, ist es im Grunde so, als würde man nichts tun.“

Kate Nowrouzi, VP Zustellbarkeit und Produktentwicklung, Mailgun

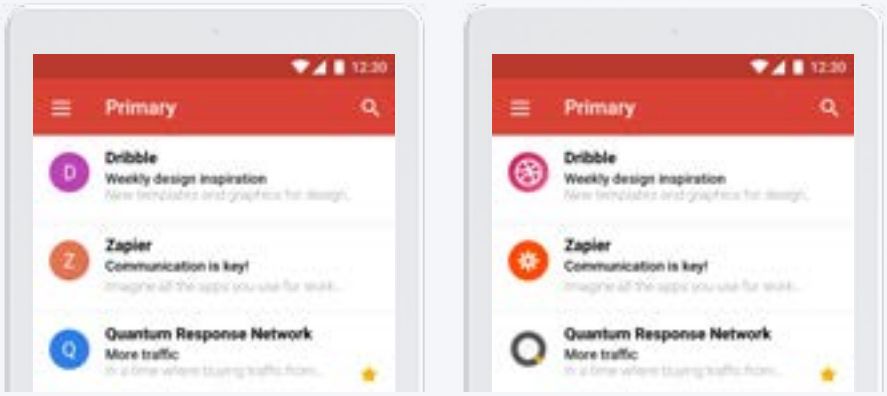
4. BIMI

Ein weiterer Grund, warum einige Versender zögern, eine DMARC-Richtlinie durchzusetzen, ist, dass sie keine großen Vorteile für sich darin sehen. Sie kommen schnell zu dem Schluss, dass es sicher nur den Nachteil gibt, dass legitime E-Mails blockiert oder als Spam eingestuft werden, weil die eigenen E-Mail-Authentifizierungseinträge nicht perfekt konfiguriert sind.

Um eine stärkere Akzeptanz von DMARC-Richtlinien zu fördern, hat die E-Mail-Branche Brand Indicators for Message Identification (BIMI) eingeführt. Das Ergebnis der BIMI-Implementierung ist ein Markenlogo, das im Posteingang und auf Nachrichtenebene erscheint. Um „BIMI-ready" zu sein, müssen Sie jedoch eine DMARC-Richtlinie haben, die auf Ablehnen oder Quarantäne eingestellt ist.

Hier sehen Sie eine Nachbildung der BIMI-Logos:

Vor BIMI **Nach BIMI**



Wenn ein E-Mail-Anbieter eine Nachricht von Ihrem Unternehmen erhält, verwendet er zunächst den DMARC-Eintrag, um nach der SPF- und DKIM-Authentifizierung zu suchen. Wenn die Nachricht dem DMARC standhält, kann der E-Mail-Anbieter nach einem BIMI-DNS-Eintrag suchen, in dem eine SVG-Bilddatei mit dem Unternehmenslogo gespeichert ist.

BIMI-Logos sind etwas, das Marketer und alle anderen, die sich für Branding interessieren, haben wollen. Es sind jedoch die Technikteams, die mit der Aufgabe betraut werden, BIMI-Einträge zu erstellen. Und der erste Schritt besteht darin, sicherzustellen, dass alle sonstigen E-Mail-Authentifizierungsprotokolle korrekt eingerichtet sind, einschließlich einer in Kraft gesetzten DMARC-Richtlinie.

Man könnte BIMI also auch als eine Art Belohnung für Versender betrachten, die sich ernsthaft mit der E-Mail-Authentifizierung beschäftigen. Jonathan Torres von Mailgun sagt, dass die E-Mail-Branche mit BIMI als Anreiz für die DMARC-Implementierung „ins Schwarze getroffen" hat.

Gmail unterstützt den Standard seit 2021, was ihn zu einem viel attraktiveren Anreiz macht. Nun plant Apple, mit den nächsten Versionen seiner Betriebssysteme die BIMI-Unterstützung für den Apple Mail-E-Mail-Client einzuführen (mit Ventura ist voraussichtlich im Oktober 2022 zu rechnen).

Jonathan hält es jedoch auch für möglich, dass E-Mail-Anbieter dazu übergehen könnten, Versender mit DMARC-Authentifizierung zu belohnen und sie zur Voraussetzung für die Platzierung im Posteingang zu machen.

„Irgendwann beschließen E-Mail-Anbieter möglicherweise, Nachrichten von Versendern zu priorisieren, deren DMARC-Richtlinien auf Ablehnen oder Quarantäne eingestellt sind, da sie diese validieren und ihnen vertrauen können. Wir haben noch niemanden gesehen, der diesen Schritt gemacht hat, aber die Grundlage ist vorhanden, um von den Versendern zu verlangen, dass sie die DMARC-Richtlinie auf etwas anderes als p=none setzen. Das könnte die Voraussetzung für die Akzeptanz sein.“

Jonathan Torres, TAM-Teammanager, Mailgun

E-Mail-Authentifizierung und Reputation

Schauen wir den Tatsachen ins Gesicht. Posteingangslogos sind zwar schön, aber sie sind nicht viel mehr als ein Eitelkeitssymbol für CMOs und E-Mail-Marketer. Es gibt wichtigere Gründe, sich auf die E-Mail-Authentifizierung zu konzentrieren: **Absender- und Markenreputation**.

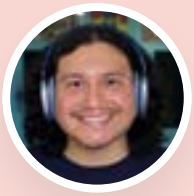
Die Absender-Reputation ist wie eine Art Kreditwürdigkeit für Unternehmen, die E-Mails versenden. Sie ist im Grunde eine Metrik für Ihre Vertrauenswürdigkeit und die Qualität Ihrer E-Mail-Kommunikation.

E-Mail-Anbieter achten darauf. Sie verwenden Spam-Fallen, um Versender zu identifizieren, die sich auf fragwürdige Weise Kontakte verschaffen. Sie wissen, wie oft Abonnenten Ihre Nachrichten öffnen und damit interagieren. Sie wissen, ob Nachrichten ignoriert, gelöscht oder als Spam markiert werden. Deshalb gilt: **Je besser Ihre Absender-Reputation, desto besser die E-Mail-Zustellbarkeit**.

Dies ist auch der Grund, warum die Nutzungsrichtlinie von Mailgun Metriken wie Abmeldungen und Spam-Beschwerden beinhaltet und warum die Plattform Tools und Dienste zur Überwachung der Absender-Reputation einsetzt. Wir wollen vertrauenswürdige Versender auf unserer Plattform und wir möchten unseren Nutzern helfen, ihre Absender-Reputation zu verbessern.

Die Verwendung oder das Fehlen einer E-Mail-Authentifizierung wirkt sich auch auf die Absender-Reputation und die Zustellbarkeit aus. Wenn Sie die E-Mail-Authentifizierung richtig einsetzen, erhöhen Sie die Wahrscheinlichkeit, dass Ihre Nachrichten erfolgreich zugestellt werden. Wenn Sie jedoch die Authentifizierung vernachlässigen, werden Sie von E-Mail-Anbietern weniger wahrscheinlich als vertrauenswürdiger Absender angesehen. Das ist einer der Gründe, warum Mailgun DKIM und SPF voraussetzt. Wir empfehlen unseren Nutzern dringend die DMARC-Implementierung.

Technikteams glauben vielleicht nicht, dass die **Markenreputation** in ihrer Verantwortung liegt. Es kann daher leicht der Eindruck entstehen, dass Brand-Spoofing und Ihre Arbeit nichts miteinander zu tun haben. Wenn Ihre Aufgabe jedoch in irgendeiner Weise mit Cybersicherheit zu tun hat, gehört die Markenreputation zu den wichtigsten Dingen, die Sie schützen. Sie müssen kein Marketer sein, um sich um die Marke des Unternehmens zu kümmern.



„Ich denke, dass der Schutz der Unternehmensmarke eines Versenders ein immer wichtigeres Thema im E-Mail-Bereich wird, da sich die Branche im Wandel befindet. Die Marke ist das A und O des Unternehmens. Wenn die Leute das Vertrauen in Ihr Unternehmen verlieren, weil nicht klar ist, ob E-Mails, die scheinbar von Ihnen stammen, sicher sind, kann dies Ihre Reputation dauerhaft schädigen.“

Jonathan Torres, TAM-Teammanager, Mailgun

TEIL 6

Die Wahl der richtigen Partner

Vertrauen ist natürlich ein entscheidender Faktor, wenn es um Sicherheit geht. Es ist für alle Arten von Beziehungen und Partnerschaften entscheidend. So wie die E-Mail-Anbieter vertrauenswürdige Absender identifizieren können müssen, brauchen auch Sie Methoden, um vertrauenswürdige Anbieter im E-Mail-Bereich zu finden.

Die Mailgun-Experten für E-Mail-Sicherheit und Compliance haben aus ihrer Sicht berichtet, worauf es bei einem SaaS-Partner ankommt, der Best Practices befolgt.

Audits und Zertifizierungen

Eine der naheliegendsten Möglichkeiten, einen potenziellen Partner zu beurteilen, ist die Prüfung der Standards, die er einhält, und der Zertifizierungen, die er erworben hat. Wie es der Zufall so wollte, führte Dan Ross, der leitende Manager der Mailgun-Abteilung Governance, Risiko und Compliance, zu dieser Zeit gerade einige größere Audits durch.

Dan hat Erkenntnisse über diese Audits und Zertifizierungen und weiß, was sie für Sie als E-Mail-Versender bedeuten.

SOC 2 Type I und II Audits

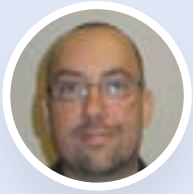
Ein SOC 2-Bericht gibt Ihnen Gewissheit über die Sicherheit, Verfügbarkeit, Datenverarbeitungsintegrität, Vertraulichkeit und Datenschutzkontrollen eines Unternehmens. Er basiert auf der Einhaltung der Trust Services Criteria (TSC) des American Institute of Certified Public Accountants (AICPA).

- **Ein SOC 2 Type I Audit** bewertet die Ausgestaltung von Sicherheitsprozessen und prüft, ob zu einem bestimmten Zeitpunkt Sicherheitskontrollen vorhanden sind.
- **Beim SOC 2 Type II-Audit** wird bewertet, wie gut diese Sicherheitskontrollen funktionieren, während der Betrieb über einen Zeitraum von sechs bis zwölf Monaten beobachtet wird.

Als Prüfer beispielsweise den SOC 2 Type II-Bericht auf Mailgun zusammenstellten, bewerteten sie Dinge wie Mitarbeiterschulungen zum Thema Bewusstsein für Cybersicherheit. Sie wählten 25 Namen aus und überprüften, ob diese Mitarbeiter eine Schulung absolviert und den Test bestanden hatten.

Die Prüfer untersuchten außerdem 25 verschiedene Code-Anpassungen an der Mailgun-Plattform, um festzustellen, ob jede dieser Änderungen den Best Practices entsprach, d. h. ob Mailgun eine Qualitätssicherung (QA) durchführte und ob der neue Code auf Sicherheitslücken überprüft wurde.

Ein weiterer Aspekt von SOC 2 Typ II ist die Möglichkeit, die Prüfung um HIPPA-Kontrollen zu erweitern. Mailgun tut dies. Einen E-Mail-Service-Provider zu finden, der SOC 2 Typ II-Berichte bietet, ist relativ selten. Aber Dan ist der Meinung, dass Sie diesen Bericht wirklich brauchen, wenn Sie Partner finden wollen, die sich an die Datenschutzgesetze halten. Während der Erstellung des Berichts wird sein Team von den Prüfern mit Fragen gelöchert.



„Mit SOC 2 Type II wird tatsächlich geprüft, ob die Sicherheitskontrollen effizient funktionieren. Wenn Mailgun sich einem SOC 2 Typ II-Audit unterzieht, sind das für uns mehrere Wochen lang 12-Stunden-Tage. Das wird ziemlich intensiv.“

Dan Ross, Leitender Manager GRC, Mailgun

ISO 27001 und 27701 Zertifizierungen

Internationale Normen (ISOs) helfen Verbrauchern und B2B-Käufern bei der Beurteilung von Sicherheit, Qualität und in diesem Fall auch bei der Beurteilung von Produktsicherheit und Diensten. ISO 27001 und ISO 27701 sind internationale Normen zur Bewertung von Informationssicherheit und Datenschutzkontrollen.

Wenn ein potenzieller Partner eine **ISO 27001 Zertifizierung hat**, zeigt dies, dass er ein Managementsystem für Informationssicherheit (ISMS) eingerichtet und implementiert hat, es wartet und kontinuierlich verbessert. Im Wesentlichen bescheinigt die Norm, dass ein Partner über die richtigen Prozesse und Richtlinien verfügt und die Informationssicherheit Jahr für Jahr weiterentwickelt. In einer SaaS-Partnerschaft bedeutet dies, dass die Plattform für Kunden und Benutzer immer sicherer wird.

Laut Dan gehören dazu Faktoren wie ein Budget für Sicherheit und ein jährlich wachsendes Team.

Eine **ISO 27701 Zertifizierung** erweitert die Norm ISO 27001, indem sie Bereiche der Datenschutzkontrollen in einem Datenschutz-Informationsmanagementsystem (PIMS) abdeckt. Diese Norm orientiert sich an Datenschutzvorschriften wie der DSGVO und dem CCPA und wurde 2019 eingeführt, um die Einhaltung von Gesetzen eines Unternehmens zu bewerten.

Diese ISO-Zertifizierungen sind zwar keine Garantie dafür, dass ein potenzieller Partner die Vorschriften auch wirklich vollständig einhält, aber sie sind ein starker Indikator, dass das Unternehmen alles in seiner Macht Stehende tut, um Kundendaten zu schützen. Und es ist wichtig, einen Partner für E-Mails zu finden, der datenschutzkonform agiert, denn dies hängt direkt mit der Compliance Ihres eigenen Unternehmens zusammen.

„Es gibt keine spezielle DSGVO-Zertifizierung, weil diese Datenschutzverordnung ein Gesetz ist. Es gibt keine Zertifizierung für etwas, an das man sich halten muss, weil es das Gesetz ist. Aber wir haben Zertifizierungen wie ISO 27701, die wir unseren Kunden vorlegen und mit denen wir nachweisen können, dass wir tatsächlich das tun, was wir behaupten zu tun.“

Dan Ross, Leitender Manager GRC, Mailgun

Sonstige Zertifizierungen und Sicherheitsrichtlinien

Neben den wichtigsten Sicherheitsprüfungen und -normen gibt es noch weitere Fragen, die Sie potenziellen Partnern stellen sollten. Laut Dan geht es hierbei um Fragen wie: Wie wird der Zugriff auf Ihre Daten verwaltet? Wie wird auf Verstöße gegen die Cybersicherheit reagiert? Wie werden Backups gehandhabt, wie wird mit geografischer Redundanz umgegangen, und welche Lösung gibt es für die Notfallwiederherstellung?

Vielleicht haben Sie auch Fragen zur Benutzersicherheit, zum Beispiel zu Single Sign-On (SSO) und Multifaktor-Authentifizierung (MFA). Möglicherweise haben Sie konkrete Bedenken, was die PCI-Zertifizierung betrifft, haben Fragen zur Sicherheit in Büros oder möchten ein Netzwerkdiagramm überprüfen. **Ein zuverlässiger Partner wird alle Ihre Fragen beantworten und Ihnen sämtliche erforderlichen Unterlagen zur Verfügung stellen.**

Erfahren Sie mehr über die Mailgun-Sicherheit.

Mailgun hat ein umfassendes Sicherheitsportal aufgebaut, in dem alle Arten von Dokumentationen zu finden sind, die für Kunden und potenzielle Geschäftspartner interessant sein könnten.

Schutz des Produkts

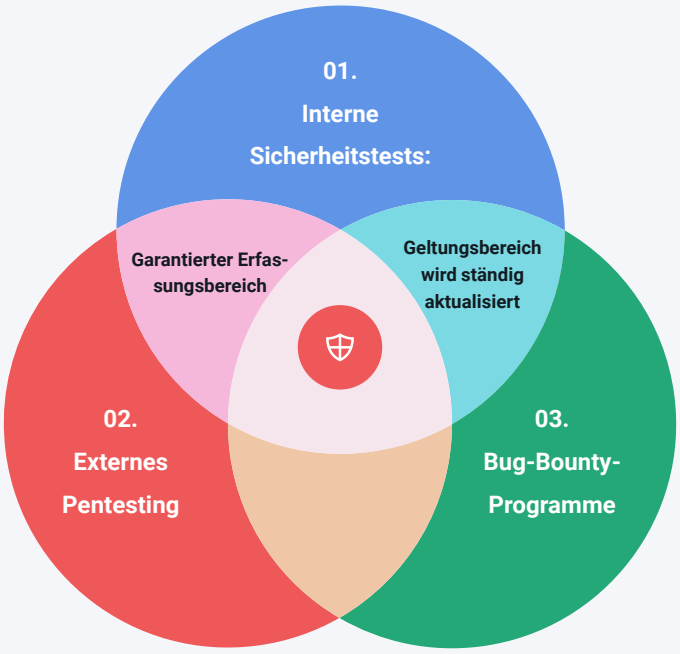
Steve Proud ist leitender Manager der Abteilung Sicherheitstechnik bei Mailgun. Er ist für den Schutz unserer Plattform verantwortlich und dafür sorgt, dass sie für die Versender sicher zu nutzen ist. Er sagt, dass die im vorigen Abschnitt behandelten Kontrollen (ISO 27701 und SOC 2 Typ II) wichtige Faktoren sind, und zwar unabhängig davon, welche Art von Technologiepartner Sie bewerten wollen. Denn Cyberkriminelle sind unerbittlich.

„Hacker greifen ständig Anwendungen an, die mit dem Internet verbunden sind. Unabhängig davon, ob es sich um eine Plattform für den E-Mail-Versand handelt oder um ein soziales Netzwerk, sollten Unternehmen auf Partner mit einer soliden Sicherheitsstrategie setzen, damit die Sicherheit in Bezug auf Mitarbeiter, Prozesse und Technologie geregelt und strukturiert umgesetzt wird."

Steve Proud, Leitender Manager, Sicherheitstechnik, Mailgun

Bevor Sie einen Vertrag mit einem Partner unterzeichnen, der E-Mail-Lösungen anbietet, sollten Sie sich darüber informieren, wie er seine Anwendungen vor Bedrohungen schützt, die die Cybersicherheit betreffen. Das Mailgun-Sicherheitsteam setzt auf eine dreigleisige Strategie, um unsere Plattform zu schützen.

Dreifache Bedrohung der Produktsicherheit



1. **Interne Sicherheitstests:** Verfügt der potenzielle Partner über eigene Sicherheitsexperten, die Produkt-Updates vor der Markteinführung testen?

2. **Externes Pentesting:** Nutzt der potenzielle Partner einen externen Dienst für Cybersicherheitstests, der über die Standardprüfungen und Berichte hinausgeht?
3. **Bug-Bounty-Programme:** Werden Sicherheitsforscher und sogenannte White-Hat-Hacker gebeten, auf der Plattform des potenziellen Partners nach unbekannten Sicherheitslücken zu suchen?

Sie haben in diesem Leitfaden bereits einige der Personen kennengelernt, die an der Produktsicherheit von Mailgun beteiligt sind. Dazu gehört Dan Ross, der sagt, dass die Frage nach dem „Change Management" ein wichtiger Bestandteil der Bewertung eines potenziellen Technologiepartners ist. **Testen die Produkt- und Sicherheitsteams neuen Code auf Sicherheitslücken, bevor ein Update live geht?** Hier bei Mailgun werden sie immer durchgeführt.

Steve Proud sagt, dass in seinem Arbeitsbereich ständige Wachsamkeit erforderlich ist. Ebenso wichtig ist, dass Ihre potenziellen Partner eine Strategie haben, um sicherheitsgefährdende Situationen schnell und effizient zu lösen.

„E-Mail-Versender müssen bei der Bewertung von E-Mail-Marketing- und Zustellbarkeits-Tools sorgfältig abwägen, mit wem sie zusammenarbeiten... Es ist keine Frage, ob Sicherheitslücken und Fehlkonfigurationen entdeckt werden, sondern wann sie entdeckt werden. Und es ist wichtig, dass Ihre Partner eine Methodik haben, die es ermöglicht, schnell zu handeln, um neuen, sicheren Code zu veröffentlichen und so die Auswirkungen der Sicherheitslücke zu verringern.

Steve Proud, Leitender Manager, Sicherheitstechnik, Mailgun

Sicherheit und Automatisierung

Selbst mit dem besten und klügsten Informationssicherheitsteam ist es schwierig, den Überblick über Trends zu behalten und Betrügern immer einen Schritt voraus zu sein. Deshalb wird ein starker Partner auch seine **Sicherheitsmaßnahmen automatisieren, damit er schnell und effektiv auf Bedrohungen reagieren kann**.

Dan Ross erklärt, dass Mailgun zwar über ein talentiertes Team verfügt, wir aber alle nur Menschen sind und deshalb manchmal Dinge übersehen, die Maschinen nicht entgehen. Dan und seine Kollegen haben also daran gearbeitet, „das Denken aus der Sicherheit herauszunehmen". Das mag ein bisschen seltsam klingen, bedeutet aber einfach nur, dass automatisierte Tools vorhanden sind, die das Sicherheitsteam fast unmittelbar auf ein Problem aufmerksam machen.

Bei Mailgun nutzen wir interne Sicherheitstools, die es uns ermöglichen, Bedrohungen im Netzwerk und auf Endpunkten in Echtzeit zu überwachen. Unsere Mitarbeiter untersuchen dann jede Warnung, die eingeht. Wenn zum Beispiel auf dem Computer eines Remote-Mitarbeiters seltsame Aktivitäten festgestellt werden, weiß das Sicherheitsteam Bescheid und kümmert sich darum, bevor der Mitarbeiter überhaupt bemerkt, dass etwas nicht stimmt.

Nick Schafer sagt, dass sich diese Art der Automatisierung auch auf die Vorgänge innerhalb der Mailgun-Anwendung erstreckt. Wir wollen sicherstellen, dass nur sichere und zulässige E-Mails unsere Plattform verlassen.

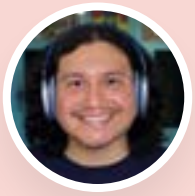
> *„Würden wir uns allein auf manuelles menschliches Handeln verlassen müssen, wären wir zu langsam. Selbst wenn wir denken, dass wir schnell handeln, könnten bereits Tausende von potenziell schädlichen Nachrichten unterwegs sein. Deshalb haben wir alle möglichen Warnungen und Automatisierungen eingerichtet, die uns benachrichtigen und dabei helfen, bösartige Vorgänge zu verhindern."*
>
> Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

Kundenaufklärung

Ein guter Partner im Bereich E-Mail-Sicherheit wird immer sein Wissen und seine Erfahrung mit Ihnen teilen. Wie wir gesehen haben, entwickeln sich die Sicherheitsbedrohungen im Cyberbereich ständig weiter, und das E-Mail-Format steht dabei im Mittelpunkt des Geschehens. Ein Anbieter von E-Mail-Lösungen, der Sie und Ihr Unternehmen auf dem Laufenden hält, ist daher ein sehr wertvoller Partner.

Bei Mailgun wird viel Aufklärungsarbeit geleistet. Auf diese Weise wollen wir sicherzustellen, dass unsere Kunden nicht versehentlich etwas tun, was entgegen der Best Practices ist oder sogar gegen das Gesetz verstößt.

Jonathan Torres erklärt, dass wir dies proaktiv tun, indem wir E-Mail-Sicherheitsprobleme während des Onboardings sowie mit dem Technical Account Manager (TAM) des Kunden kontinuierlich thematisieren.



„Nicht jeder Anbieter bringt die Themen Sicherheit und Compliance zur Sprache. Wir möchten mit unseren Kunden über diese Themen sprechen und sind gerne bereit, sie über Best Practices zu beraten, auch wenn ein Problem nicht direkt mit unserem Produkt zusammenhängt."

Jonathan Torres, TAM-Teammanager, Mailgun

TEIL 7

Wie Mailgun helfen kann

Hoffentlich konnten wir Sie davon überzeugen, dass eine sichere Plattform für den E-Mail-Versand von größter Bedeutung ist. Von Sicherheitsmaßnahmen für Benutzer über das Aufhalten von Betrügern bis hin zur strikten Einhaltung von Compliance-Standards: Mailgun by Sinch kümmert sich täglich darum. Nennen Sie uns ruhig verrückt, aber wir lieben, was wir tun.

„Unser Team ist sehr engagiert und erfahren. Es bereitet uns wirklich Freude, Betrüger von der Mailgun-Plattform fernzuhalten. Es macht Spaß, weil es eine Art Superhelden-Aufgabe ist. Ich erzähle meinen Kindern gerne, dass wir die Guten sind, die die Plattform schützen."

Nick Schafer, Manager Zustellbarkeit & Einhaltung, Mailgun

Sie wissen bereits, dass ein Partner, bei dem E-Mail-Sicherheit und Compliance ganz oben auf der Prioritätenliste stehen, eine wertvolle Ergänzung für jedes Unternehmen ist. Mailgun by Sinch ist bereit, dieser Partner für Sie zu sein.

Hier nochmal eine kurze Übersicht, wie wir mit unseren Benutzern in Hinblick auf E-Mail-Sicherheit und Compliance zusammenarbeiten:

- **Sichere Datenzentren:** Die Cloud-basierten Dienste von Mailgun fußen auf einer branchenführenden GCP-Infrastruktur. Alle Datenzentren sind mit vollkontinuierlicher Überwachung und biometrischen Zugangskontrollsystemen ausgestattet.
- **Redundanz, Datenwiederherstellung und Backups:** Unsere Datenzentren sind mit mindestens N+1-Redundanz für die Strom-, Netzwerk- und Kühlungsinfrastruktur ausgestattet. Innerhalb einer Region erfolgt die Datenverarbeitung in mindestens drei verschiedenen Verfügbarkeitsbereichen. Für alle Primärdatenbanken erfolgen tägliche Kontodatensicherungen mit inkrementeller/punktgenauer verschlüsselter Wiederherstellung.
- **Verschlüsselung:** Mailgun verwendet AES-256-Verschlüsselung um Kundendaten im Ruhezustand zu schützen, und wendet opportunistische TLS-Verschlüsselung an, um von der Plattform versendete Nachrichten während der Übertragung zu schützen.
- **Einhaltung von Vorschriften:** Mailgun erfüllt oder übertrifft die DSGVO- und CCPA-Vorschriften, um die Privatsphäre und Integrität der Kundendaten zu schützen. Rechte und Pflichten für die Einhaltung des HIPAA sind in einem Beiblatt für Geschäftspartner (Engl. Business Associate Addendum) festgelegt. Stripe ist unser PCI-konformer Bezahldienstleister.
- **Berichte und Zertifizierungen:** Wir sind nach ISO 27001 und 27701 zertifiziert. Mailgun verfügt außerdem über SOC 2 Typ I- und SOC 2 Typ II-Berichte, was bedeutet, dass unsere Sicherheitskontrollen sich an Vorschriften wie DSGVO, CCPA und HIPAA orientieren. Darüber hinaus sind alle Anbieter nach SOC Type II und ISO 27001 zertifiziert.
- **Zugriffsrechte und Bewusstsein von Mitarbeitern:** Mailgun beschränkt den Zugriff auf Daten und Systeme auf Grundlage der Arbeitsrollen. Der administrative Zugriff auf Mailgun-Systeme und -Dienste erfolgt nach dem Prinzip der geringsten Privilegien. Alle Mitarbeiter sind verpflichtet, eine jährliche Schulung zum Thema Cyber-Bewusstsein zu absolvieren und werden jährlich individuell bewertet.
- **Anwendungssicherheit:** Für Kunden-Logins sind SAML und 2FA verfügbar. Ein Meldesystem (Engl. Intrusion Detection System, IDS) ist im Einsatz, um unbefugte Zugriffe auf Konten zu erkennen. Änderungen am Produktcode werden auf Sicherheitslücken getestet, und ein externes Bug-Bounty-Programm hilft Mailgun, unbekannte Probleme zu identifizieren.
- **Plattformschutz:** Mailgun hat Tools und automatisierte Systeme und Mitarbeiter, die dafür sorgen, Betrüger von der Plattform fernzuhalten und die unser Netzwerk auf verdächtige Aktivitäten hin überwachen. Eine Nutzungsrichtlinie skizziert die Erwartungen der Benutzer.
- **E-Mail-Authentifizierung:** SPF- und DKIM-Authentifizierung werden für die Nutzung der Mailgun-Plattform vorausgesetzt. Darüber hinaus empfehlen wir dringend eine DMARC-Richtlinie.

Sicherheit, Compliance und E-Mail-Authentifizierung sind komplexe Themen. Aus diesem Grund stellt Mailgun seinen Kunden Technical Account Manager (TAMs) an die Seite, die beim Onboarding und während der gesamten Vertragslaufzeit Hilfe und Unterstützung anbieten. Wir können auch bei Aufgaben wie der Implementierung von DKIM und SPF helfen. Außerdem sind wir gerne bereit, über diese Themen zu sprechen und hilfreiche Ratschläge zu geben.

„Wir haben eine sehr enge Beziehung zu unseren Kunden, dazu gehört auch eine umfassende Kundenaufklärung zu Best Practices für Themen wie E-Mail-Authentifizierung und Compliance. Wir treffen uns jedes Jahr mit unseren Kunden, um diese Themen aufzufrischen und neue Mitarbeiter zu schulen. Wir tun dies alles, weil es uns ein Anliegen ist, dass sie als Versender Erfolg haben und um sicherzustellen, dass sie die Risiken kennen."

Kate Nowrouzi, VP Zustellbarkeit und Produktentwicklung, Mailgun

Sind noch Fragen offen geblieben? Erfahren Sie mehr über Sicherheit und Compliance bei Mailgun by Sinch in unserem speziellen Sicherheitsportal. Kontaktieren Sie uns, wenn Sie weitere Fragen zu Sicherheit, Compliance oder anderen Themen haben. Wir erläutern gerne, wie Mailgun E-Mails schützt.

TEIL 8

Ressourcen

Vertiefen Sie Ihr Wissen über E-Mail-Sicherheit, Compliance und Authentifizierung mit detaillierten Informationen, Mailgun-Blogartikeln, Studien, die in diesem Leitfaden zitiert wurden, und anderen nützlichen Quellen.

Ressourcen auf mailgun.com

- Das Mailgun-Sicherheitsportal: Sehen Sie unsere Richtlinien, Zertifizierungen und Berichte ein oder beantragen Sie Zugriff darauf. Dazu gehören ISO 27001, ISO 27701 und SOC 2 Typ I und II-Berichte.
- DSGVO-Hub: Erfahren Sie, wie Mailgun die Datenschutz-Grundverordnung der Europäischen Union einhält.
- HIPPA Business Associates Addendum (BAA): Informieren Sie sich in unserem Beiblatt für Geschäftspartner über Rechte und Pflichten im Zusammenhang mit dem Schutz privater Gesundheitsdaten.
- Auftragsdatenvereinbarung: Erfahren Sie mehr darüber, wie Mailgun mit Kundendaten umgeht.
- Nutzungsrichtlinie: Lesen Sie, welche Richtlinien es für die Benutzer der Mailgun-Plattform gibt.

Nützliche Inhalte von Mailgun

- Bewährte Verfahren zur E-Mail-Sicherheit: Wie Sie Ihr E-Mail-Programm sicher halten (nur auf Englisch verfügbar)
- Glossar zum Thema E-Mail-Betrug (nur auf Englisch verfügbar)
- Wie schützt Mailgun Ihre E-Mails? (nur auf Englisch verfügbar)
- Schwachstellenmanagement: Bei der Behebung von Sicherheitsbedrohungen arbeiten wir eng mit der Community zusammen (nur auf Englisch verfügbar)
- TLS-Grundlagen: Was ist TLS-Verbindungskontrolle? (nur auf Englisch verfügbar)
- DKIM verstehen: Wie es funktioniert und warum es notwendig ist (nur auf Englisch verfügbar)
- Implementierung von DMARC: Eine Schritt-für-Schritt-Anleitung (nur auf Englisch verfügbar)
- Welchen SMTP-Port sollte ich verwenden? (nur auf Englisch verfügbar)
- Phishing-E-Mails: Wie Sie Phishing erkennen und sich davor schützen können (nur auf Englisch verfügbar)
- Fallstudie: Datenschutz für skalierbare und sichere E-Mails optimieren (nur auf Englisch verfügbar)

Ressourcen zur E-Mail-Authentifizierung

- Open-SPF.org: Erfahren Sie mehr über das SPF-Authentifizierungsprojekt.
- DKIM.org: Erfahren Sie mehr über die DKIM-Authentifizierung.
- DMARC.org: Erfahren Sie mehr über Domain-basierte Nachrichtenauthentifizierung, Konformität und Reporting.
- BIMIGroup.org: Erfahren Sie mehr über BIMI.
- Der Weg zur BIMI-Implementierung: Mehr Infos über die BIMI-Einrichtung von Email on Acid by Sinch.

Externe Quellen in diesem Leitfaden

- IBM: Wie hoch sind die Kosten einer Datenschutzverletzung im Jahr 2021 (nur auf Englisch verfügbar)
- Cisco: 2021 Trends bei Sicherheitsbedrohungen (nur auf Englisch verfügbar)
- Mimecast: Stand der E-Mail-Sicherheit 2022 (nur auf Englisch verfügbar)
- Proofpoint: 2022 Stand des Phish (nur auf Englisch verfügbar)
- GreatHorn: Benchmark-Bericht zur E-Mail-Sicherheit 2021 (nur auf Englisch verfügbar)

Mehr als 100 000 Unternehmen weltweit nutzen Mailgun by Sinch, um über eine erstklassige Infrastruktur ein leistungsstarkes E-Mail-Erlebnis für ihre Kunden zu schaffen. Unternehmen wie Vodafone, Etsy, NHL und McKinsey setzen auf die innovativen Technologien und die zuverlässige Infrastruktur von Mailgun, um jedes Jahr mehrere Milliarden E-Mails zu versenden. Mailgun wurde mit Fokus auf Entwicklerteams als Zielgruppe konzipiert und ermöglicht es Unternehmen mit unterschiedlichem Sendebedarf, E-Mails mühelos zu versenden, zu empfangen und zu verfolgen.

2010 füllte Mailgun eine Marktlücke: Es hatte bis zu diesem Zeitpunkt keinen entwicklerfreundlichen, API-basierten E-Mail-Dienst gegeben. Inzwischen hat sich Mailgun mit **Sinch** zusammengeschlossen, dem Anbieter einer führenden Kommunikationsplattform (CPaaS), und wurde so zur entwicklerzentrierten E-Mail-Lösung für Sinch-Kunden auf der ganzen Welt. Mailgun ist DSGVO-konform und nach HIPAA sowie SOC I und II zertifiziert und bietet somit höchste Datenschutzstandards.

Weitere Informationen erhalten Sie unter **mailgun.com/de**.