mailgun by sinch

GUIDE

Le guide de Mailgun sur la sécurité et la conformité des emails

Assurer la protection dans un environnement numérique dangereux

Sommaire

Sommaire

INTRODUCTION

Les quatre vérités sur l'email

Il n'est jamais trop tard pour faire le point sur nos exigences en matière d'emailing. Même si c'est dur à admettre pour nous, l'envoi d'emails constitue un risque majeur pour la sécurité de votre entreprise. Si vous lisez ce guide, vous êtes probablement impliqué dans la protection des personnes qui peuvent être affectées par une violation ou une atteinte à la vie privée.

Mais, soyons réalistes : empêcher les mauvais acteurs d'utiliser l'email à des fins malveillantes et suivre les bonnes pratiques en matière de confidentialité et de sécurité sont des tâches difficiles. L'équipe de Mailgun by Sinch est bien placée pour le savoir, tout comme n'importe qui d'autre entreprise de notre secteur d'activité.

Cependant, **votre programme d'emailing vaut la peine d'être protégé.** Nous pensons qu'éduquer les autres sur les bonnes pratiques favorise un environnement numérique plus sûr. Dans ce guide complet, vous découvrirez des informations stratégiques et des conseils d'experts sur la façon de mettre en place cette protection.

Mais d'abord, **voici cinq vérités incontestables à propos de l'email :**

1. L'email est le plus grand vecteur de risques

L'email est une arme de choix pour les cybercriminels ; la boîte de réception est leur terrain de prédilection.

Qu'il s'agisse d'un spam standard, d'une attaque par hameçonnage ou d'une tentative de lancement d'un rançongiciel ou d'un logiciel malveillant, la boîte de réception offre aux mauvais acteurs l'occasion de commettre leurs mauvaises actions, et ils peuvent le faire pour une bouchée de pain.

En 2022, la chaîne d'hôtellerie Marriott a signalé sa troisième faille de sécurité importante en quatre ans. Cette fois, il s'agissait d'une attaque d'ingénierie sociale qui a permis à un mauvais acteur d'accéder à l'ordinateur d'un employé. Marriott a dépensé plus de 16 millions de dollars cette année pour se remettre d'une autre faille de sécurité survenue en 2018.

Les mauvais acteurs trouvent même des moyens de contourner l'authentification multifacteurs à l'aide d'outils et de techniques de hameçonnage « adversary-in-the-middle » (AiTM). Selon Microsoft, un système récent cible des milliers d'entreprises.

L'email est un canal qui permet aux arnaqueurs d'infiltrer les entreprises. Il peut être utilisé pour atteindre un grand nombre de victimes potentielles ou être très ciblé comme dans le cas du harponnage (de l'anglais « spear phishing »). Comme tout le monde possède une adresse email, les mauvais acteurs n'ont pas besoin d'un taux de réussite élevé. Il suffit de tromper une seule personne pour perturber toute une organisation.

Pourtant, nous ne pouvons pas arrêter d'envoyer des emails.

2. La fin de l'envoi d'emails n'est pas pour demain

Malgré les évolutions technologiques constantes à l'ère numérique, l'email reste l'un des meilleurs moyens de communiquer avec les clients et les collègues, d'atteindre votre audience et de faire des affaires. Qu'il s'agisse d'emails transactionnels contenant des informations importantes ou d'emails marketing qui favorisent la croissance d'une entreprise, il serait difficile de fonctionner sans nos boîtes de réception.

Chaque fois qu'une personne configure un nouvel appareil mobile ou ouvre un compte en ligne, elle a besoin d'une adresse email. Il s'agit d'un élément clé d'informations personnelles identifiables que nous utilisons toutes et tous pour accéder à nos applications et services numériques. C'est pourquoi le vol d'identité est facile lorsqu'un utilisateur accède à un compte de messagerie.

On estime que plus de 333 milliards d'emails sont envoyés et reçus chaque jour dans le monde entier. **D'ici 2025, ce nombre devrait dépasser 376 milliards**. Bien sûr, beaucoup de ces emails proviennent de spammeurs et d'escrocs.

3. Les lois et restrictions relatives à la protection de la vie privée sont de plus en plus strictes

Dans le but de rendre la boîte de réception et Internet plus sûrs, les gouvernements signent des lois, et les grandes entreprises technologiques introduisent de nouvelles fonctionnalités pour protéger les personnes qui utilisent leurs services de messagerie.

Par exemple, Apple a secoué le monde de l'emailing lorsque l'entreprise a introduit la protection de la confidentialité des emails en 2021. En 2017, Google a arrêté de lire les emails des utilisateurs Gmail à des fins de publicité ciblée. Ainsi, les experts en emailing de chez Mailgun affirment que les filtres anti-spam basés sur l'intelligence artificielle de Gmail sont les meilleurs du secteur.

Les lois sur la confidentialité des consommateurs, telles que le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne et la Loi californienne sur la protection de la vie privée des consommateurs (CCPA) aux États-Unis, visent à donner plus de possibilités aux utilisateurs tout en empêchant l'utilisation abusive de données sensibles.

Le problème, c'est que la plupart des expéditeurs légitimes respectent déjà toutes les règles et bonnes pratiques. **On ne peut pas dire la même chose des mauvais acteurs**. Après tout, ils ne sont pas appelés « hors-la-loi » pour rien.

4. La cybercriminalité évolue en permanence

Peu importe les efforts déployés par les services de messagerie et d'emailing pour empêcher les emails malveillants d'atteindre la boîte de réception, les mauvais acteurs semblent toujours trouver un moyen d'y parvenir. Leurs tactiques sont de plus en plus complexes, et leurs stratégies toujours plus élaborées.

Nick Schafer dirige l'équipe chargée de la délivrabilité et de la conformité chez Mailgun. Nick et son équipe font en sorte de garder les mauvais acteurs hors de notre plateforme, ce qui inclut la surveillance des activités suspectes et la mise à jour de la sécurité des emails en fonction des tendances en termes de cybercriminalité. Il le décrit comme une bataille sans fin :

« Je déteste le dire, mais la vérité est que vous ne les arrêterez jamais. Mais vous pouvez les battre. Une fois que nous aurons trouvé un moyen d'arrêter une mauvaise pratique, ils trouveront une nouvelle tactique. Toutefois, cela ne signifie pas que nous devons baisser les bras. Si le mieux que nous puissions faire est de les ralentir, alors c'est ce que nous ferons. »

Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

5. Les expéditeurs doivent garder une longueur d'avance

Cela signifie que les expéditeurs doivent rester vigilants en matière de sécurité des emails et de protection de la vie privée. Votre organisation doit faire le maximum pour prévenir les problèmes tout en étant prête à atténuer la situation si quelque chose tourne mal.

Pour garder une longueur d'avance sur les mauvais acteurs qui veulent utiliser l'email pour tromper vos abonnés ou les personnes de votre organisation, il faut tenir compte de plusieurs facteurs importants :

- Une équipe formée et consciente des risques
- Des protocoles d'authentification de l'email robustes
- La bonne compréhension des réglementations en matière de protection de la vie privée et leur rapport avec l'email
- Des partenaires susceptibles d'aider votre équipe à assurer la sécurité de vos emails

Nous aborderons ces points tout au long de ce guide. Durant votre lecture, vous découvrirez également les opinions des experts de Mailgun, qui travaillent en étroite collaboration avec les utilisateurs, sur la protection de notre plateforme et des programmes d'emailing de nos clients.

Pourquoi protéger vos emails

Même si les spammeurs et les arnaqueurs sont infatigables, se concentrer sur la sécurité des emails et la protection de la vie privée est certainement un effort nécessaire et louable.

Voici qui et ce que vous protégez lorsque vous donnez la priorité à la sécurité et à la conformité :

1. Pour votre entreprise

Selon une étude mondiale réalisée par IBM, le coût moyen d'une fuite de données était supérieur à 4 millions de dollars en 2021, et **l'impact financier moyen d'une attaque par hameçonnage était de 4,65 millions de dollars**. Les attaques BEC (Business Email Compromises), qui constituent une forme de harponnage, étaient les plus coûteuses, à un peu plus de 5 millions de dollars par violation.

La même étude IBM révèle qu'il faut généralement plus de 280 jours aux entreprises pour arrêter et résoudre ce type d'attaques. Cela inclut le temps et les ressources nécessaires aux équipes informatiques et de cybersécurité pour identifier les faiblesses et corriger les vulnérabilités.

2. Pour la réputation de votre marque

Les failles de sécurité et les escroqueries liées à votre organisation ont mauvaise presse et nuisent à la réputation de votre marque, ce qui entraîne une perte de confiance. L'étude d'IBM a révélé que **perte d'activité représentait 38 % des coûts totaux, soit près de 1,6 million de dollars par violation**.

Bien sûr, l'impact sur la réputation de marque peut aller au-delà de ce qui est mesuré en coûts financiers. Les entreprises qui sont la cible d'une usurpation de marque en boîte de réception constatent que les contacts sont moins susceptibles d'ouvrir et de s'engager avec leurs messages, parce que les destinataires craignent pour la sécurité des emails.

3. Pour votre réputation d'expéditeur

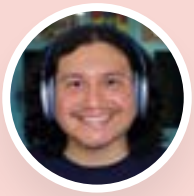
Outre la réputation de marque, les services de messagerie comme Gmail, Apple Mail et Yahoo Mail ont des moyens de mesurer et de noter la réputation d'un expéditeur d'emails. Si vous ne configurez pas correctement les enregistrements DNS pour l'authentification de vos emails, il est plus difficile pour les services de messagerie de s'assurer que vos enoiuvs sont légitimes.

Cela signifie que les emails que vous envoyez sont plus susceptibles d'être bloqués ou d'atterrir dans le dossier du spam. Ainsi, l'absence ou la défaillance des protocoles d'authentification peut avoir un impact négatif sur la réputation d'expéditeur et la délivrabilité des emails.

4. Pour vos utilisateurs et vos clients

Le point le plus important est sans doute la manière dont la sécurité et l'authentification des emails contribuent à protéger vos clients et/ou les utilisateurs de vos services. La vie privée, l'identité et les finances des personnes faisant appel à votre entreprise sont en danger si vous ne donnez pas la priorité à la sécurité et à la conformité.

Jonathan Torres dirige les équipes de chargés de compte pour Mailgun, ainsi que d'autres produits Sinch. Il nous rappelle que l'email fait partie d'un écosystème numérique interconnecté.



« La conformité, la sécurité et la délivrabilité des emails ne sont pas seulement des problèmes pour l'expéditeur. Si vous ne pensez qu'à leur impact pour vous, votre vision est trop étroite. Qu'il s'agisse de services de messagerie, d'abonnés, de clients, d'employés ou de marques, ces questions sont transversales et tout le monde finit par être impliqué. »

Jonathan Torres, Responsable des chargés de compte chez Mailgun

PARTIE 1

Escroqueries par email, hier et aujourd'hui

Pour comprendre pourquoi l'email est le plus grand vecteur de menace de cybersécurité et pour saisir la gravité de la situation, il faut examiner son origine et comment nous en sommes arrivés là.

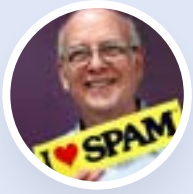
Nous reviendrons d'abord aux origines de l'email. Puis nous examinerons certaines stratégies courantes utilisées par les mauvais acteurs dans les attaques modernes par email.

L'email à ses débuts

Au départ, l'email était surtout une forme de communication interservices dans une entreprise. Ray Tomlinson, programmeur informatique, a introduit ce qu'il pensait être une version préliminaire de l'email à ARPANET en 1971. Plusieurs années plus tard, le jeune Shiva Ayyadurai a créé un logiciel qu'il a appelé « EMAIL » pour remplacer les boîtes de réception physiques et les mémos papier dans une école de médecine du New Jersey.

Bientôt, l'email était utilisé pour communiquer entre différentes organisations, ce qui a conduit à ce que beaucoup considèrent comme le premier spam de l'histoire. Le marketeur Gary Thuerk a envoyé un email non sollicité à des centaines d'employés ARPANET en 1978, promouvant un nouvel ordinateur de Digital Equipment Corporation. Thuerk affirme que le message a rapporté 13 millions de dollars à DEC.

La réalité est donc claire : l'email est un canal idéal pour convaincre les gens de dépenser de leur argent. Cependant, lorsque le Wall Street Journal a célébré les 30 ans du spam en 2008, Thuerk a expliqué pourquoi il ne se sentait pas responsable de l'invention de l'email indésirable tel que nous le connaissons.



« Si une compagnie aérienne perd vos bagages, est-ce que vous le reprochez aux frères Wright ? »

Gary Thuerk, « Père du spam »

À mesure que de plus en plus de consommateurs achetaient des ordinateurs personnels et finissaient par se connecter à l'Internet, les mauvais acteurs ont vu l'occasion d'exploiter encore davantage la boîte de réception à des fins lucratives. Et c'était tellement facile !

Quand l'envoi et la réception d'un email était quelque chose de nouveau et intéressant, les utilisateurs ouvraient, lisaient et répondaient à presque tout. On peut dire que l'internaute moyen était également assez crédule. Certains des pièges auxquels les gens croyaient à l'époque sont devenus des blagues parce qu'ils sont tellement risibles.

La fraude 419 (aussi appelée « scam 419 », ou arnaque nigériane) en est un parfait exemple. De nombreux programmes similaires de fraude par virement indiquent que les destinataires auraient gagné la loterie ou reçu un héritage inattendu d'un parent très lointain. Étonnamment, bon nombre de ces anciennes tactiques restent utilisées même aujourd'hui.

Durant les années 1990, le monde de l'emailing était semblable au Far West, avec des spammeurs courant dans tous les sens et semant le chaos. Mais, un nouveau shérif est arrivé en ville, ou dans la boîte de réception pour être plus précis.

Maîtriser le spam

Maintenant, passons au début des années 2000. À cette époque, nous commençons à dire adieu à l'Internet bas débit via accès téléphonique, aux jeans délavés ainsi qu'aux CDs des années 1990. C'est aussi une époque où le spam monte en flèche et, en réponse, les législateurs américains adoptent la loi CAN-SPAM. Il s'agit d'une loi adoptée en 2003 qui établit les premières normes nationales des États-Unis pour l'envoi d'emails commerciaux.

Cette année-là, Kate Nowrouzi entre en poste chez America Online (AOL). Aujourd'hui, Kate est VP de la délivrabilité et du développement de produit chez Mailgun. À l'époque, elle faisait partie de l'équipe anti-spam d'AOL.

En 2003, AOL était encore l'un des plus grands services de messagerie au monde, à l'instar de Hotmail et Yahoo Mail. À son apogée, AOL comptait plus de 35 millions d'utilisateurs. C'était la messagerie et le fournisseur d'accès principal aux États-Unis. En cela, AOL était également aux premières loges de la lutte contre le spam.

Kate et l'équipe anti-spam d'AOL ont commencé à réaliser à quel point il était difficile de déterminer si un email était du spam ou un email légitime qu'un abonné voulait bien recevoir. Le type de contenu ou le secteur d'activité n'était pas le meilleur indicateur. Même les entreprises qui traitent du contenu pour adultes ou vendent du Viagra ont de vraies raisons d'envoyer des emails aux abonnés.

« Nous avions des algorithmes intégrés dans les filtres pour détecter les modèles de spam, et nous avions l'habitude de faire une analyse manuelle du trafic entrant qui était suspect. Mais la définition du spam peut être très différente d'une personne à l'autre. Nous avons donc décidé de donner un peu de pouvoir aux utilisateurs d'AOL. Ils ont pu décider s'ils voulaient recevoir tel email ou non. »

Kate Nowrouzi, VP de la délivrabilité et du développement de produit chez Mailgun

Cela a abouti à la première fonctionnalité de **signalement de spam**, faisant d'AOL le premier service de messagerie à avoir des **boucles de rétroaction** avec ses utilisateurs. Ensuite, l'équipe anti-spam d'AOL a commencé à développer des règles pour évaluer le nombre de plaintes pour spam (en fonction d'un pourcentage du volume) qu'un expéditeur pouvait recevoir avant qu'AOL ne bloque ses emails. Cela a finalement conduit à la statistique d'emailing connue sous le nom de **taux de plaintes**, qui est un facteur que les services de messagerie utilisent pour juger de la réputation d'expéditeur.

Alors si tout cela a permis de *contrôler* le spam, cela ne l'a évidemment pas arrêté. Les mauvais acteurs n'ont eu qu'à essayer de nouvelles tactiques.

Une menace en évolution constante

Kate souligne que tous les spams ne sont pas égaux. Il existe des spammeurs traditionnels qui n'ont tout simplement pas la permission de vous envoyer un email et qui veulent gagner quelques centimes. Cependant, les cybercriminels aux intentions clairement malfaisantes sont la menace principale. Ces mauvais acteurs s'adaptent sans relâche aux stratégies de protection.

« Beaucoup de choses ont changé. Le spam évolue. C'est une activité sans fin. Comme Mailgun améliore sa plateforme en tant que fournisseur d'emailing et que les fournisseurs d'accès à Internet font de même de leur côté, nous travaillons tous activement pour protéger nos utilisateurs des activités malveillantes. Mais parfois, les spammeurs peuvent être très convaincants, surtout avec l'ingénierie sociale. »

Kate Nowrouzi, VP de la délivrabilité et du développement de produit chez Mailgun

Les pirates peuvent lancer ces attaques d'ingénierie sociale dans la boîte de réception, en raison de la quantité d'informations sur les personnes et les entreprises disponibles en ligne. Ils peuvent apprendre beaucoup en parcourant la présence publique d'une cible sur les réseaux sociaux.

De nos jours, au lieu d'escroqueries par email provenant d'un faux prince nigérian, **les attaques ressembleront davantage à des messages de votre banque, de votre meilleur ami ou de votre patron**.

Il n'y a pas si longtemps, Kate a fait un don à une collecte de fonds publique sur Facebook. Après quoi elle a reçu ce qu'*elle pensait* être un email de l'hôte de cette collecte de fonds, un fondateur bien connu de la Silicon Valley. L'email la remerciait d'avoir fait un don et demandait plus de soutien sous la forme de cartes-cadeaux Amazon.

Au début, Kate a raté l'un des principaux signaux d'alarme - un trait de soulignement dans l'adresse email entre le prénom et le nom de l'expéditeur, légèrement différent de la véritable adresse email. Mais, au fur et à mesure que les communications avec l'escroc se poursuivaient, elle a remarqué des signes plus évidents, tels qu'un mauvais anglais et une utilisation étrange des emojis, qui semblaient inhabituels pour la personne dont les escrocs se faisaient passer.

> *Sachant que je suis dans ce métier depuis 20 ans et que je suis tombée dans ce piège, je ne peux pas imaginer pourquoi quelqu'un comme ma mère ne le ferait pas.*
>
> Kate Nowrouzi, VP de la délivrabilité et du développement de produit chez Mailgun

Qui sont les escrocs modernes ?

Bien qu'il existe de nombreux types d'escroqueries par email et de nombreuses façons de les éliminer, l'une des attaques les plus répandues ces dernières années est une forme d'hameçonnage connue sous le nom d'« **usurpation de marque** ». Les mauvais acteurs trouvent des moyens d'usurper l'identité visuelle des emails et du site web de votre entreprise pour inciter les utilisateurs à leur donner les identifiants de leur compte ou d'autres informations sensibles. L'authentification par email avec DMARC est le meilleur moyen de se protéger contre cela.

Toutefois, si un mauvais acteur parvient à obtenir des informations d'identification SMTP ou des clés API, il peut littéralement envoyer des messages en se faisant passer pour votre marque, ce qui peut causer de sérieux dégâts.

Jonathan Torres s'est mis dans la peau d'un escroc et nous explique le processus de base. Voici comment cela se passe souvent, en seulement cinq étapes simples.

L'usurpation de marque par email

Étape 1

Trouver une marque connue vulnérable à l'usurpation d'identité.

Les entreprises du secteur financier, du e-commerce et de la technologie sont parmi les plus susceptibles d'être usurpées.

Étape 2

Rechercher des clés API non protégées ou déchiffrer les mots de passe SMTP.

Cela permettent aux mauvais acteurs d'envoyer des emails comme la marque elle-même le ferait, trompant les services de messagerie et les abonnés.

Étape 3

Concevoir une fausse page de renvoi ou une fausse page de connexion.

Avec quelques outils de base et le bon logo, il est facile d'imiter l'apparence du site web d'une marque.

Étape 4

Créer un faux email convaincant.

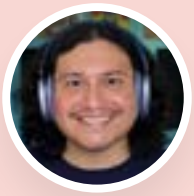
Les arnaqueurs se servent souvent du sentiment d'urgence pour convaincre les victimes d'agir sans réfléchir.

Étape 5

Recueillir les identifiants des victimes.

L'email dirige les destinataires vers la fausse page de renvoi. Là, ils tentent de se connecter, mais saisissent en fait des informations sensibles.

Par conséquent, il ne faut pas nécessairement être un super-hacker pour usurper l'identité d'une marque. Toute personne disposant d'outils tels que Photoshop, d'un service de création de site web gratuit et d'une liste d'emails peut tenter sa chance. Imiter une marque bien connue est un jeu d'enfant.



« Si vous pouvez envoyer un email qui semble provenir d'une entreprise connue, vous pouvez rediriger des personnes vers de fausses pages de renvoi. Lorsqu'un escroc a accès à vos emails, il peut facilement les reproduire. »

Jonathan Torres, Responsable des chargés de compte chez Mailgun

Dans ces conditions, que peuvent faire les équipes techniques pour empêcher l'usurpation de marque ? **La meilleure défense contre l'usurpation est la mise en œuvre de protocoles d'authentification d'email**, dont nous discuterons dans la Partie 5 de ce guide. Mais si vous ne voulez pas avoir l'air d'un spammeur aux yeux des services de messagerie et des destinataires d'emails, vous devrez également connaître certaines règles et réglementations importantes.

PARTIE 2

Conformité et cadre réglementaire

Avant de chercher comment empêcher les mauvais acteurs d'utiliser l'email à des fins malveillantes, vérifions que vous respectez toutes les règles en tant qu'expéditeur légitime et digne de confiance.

Tout d'abord, voici un petit rappel sur les parties concernées par l'email et la confidentialité des données :

1. Personnes concernées :

Il s'agit du consommateur ou du destinataire des communications par email. Les personnes concernées sont les personnes dont les données à caractère personnel sont collectées, stockées et utilisées par d'autres. Les réglementations sur la protection de la vie privée visent à protéger leurs droits.

2. Contrôleurs :

Les contrôleurs de données sont ceux qui collectent, stockent et distribuent les informations personnelles des personnes concernées. Ils doivent protéger ces informations personnelles identifiables, peu importe où elles se trouvent ou qui y a accès.

3. Processeurs :

Ces entités traitent des données à caractère personnel au nom des responsables du traitement des données. Il s'agit généralement de fournisseurs de solutions tiers externes qui ont besoin d'accéder à des informations personnelles identifiables pour fournir un service. Il doit y avoir un contrat entre les sous-traitants et les contrôleurs définissant des éléments tels que l'utilisation des données, le stockage sécurisé et ce que deviennent les données à caractère personnel à la fin de la relation d'affaires.

En tant qu'expéditeur d'emails, votre entreprise tombe très probablement dans la catégorie des « Contrôleurs », tandis que Mailgun serait un « Processeur ». Darine Fayed, responsable de la protection des données personnelles chez Mailgun, affirme que bien que notre entreprise aille au-delà des recommandations légales en matière de conformité réglementaire, en fin de compte, le fardeau incombe aux expéditeurs.

« Quiconque ayant accès à des données à caractère personnel doit les protéger. Mais les responsables du traitement doivent être précis sur la manière dont ces données à caractère personnel doivent être stockées, traitées et transférées à des tiers. Tout cela doit être fait de manière à respecter strictement les lois en vigueur. »

Darine Fayed, responsable juridique et responsable de la protection des données personnelles chez Mailgun

Les principales lois sur la confidentialité des consommateurs

Examinons brièvement les principales lois et réglementations relatives à la protection de la vie privée des consommateurs et leur rapport avec l'email.

Comme il y a beaucoup à décortiquer, nous ne couvrirons que l'essentiel dans ce guide. Néanmoins, nous vous indiquerons d'autres ressources où vous pourrez en savoir davantage sur certains règlements spécifiques et sur la façon dont ils peuvent vous affecter en tant qu'expéditeur.

RGPD

C'est le règlement le plus important que vous devez prendre en compte en tant que expéditeur. Promulgué en 2018, le Règlement Général sur la Protection des Données (RGPD) de l'UE a contribué à faire avancer la protection de la vie privée des consommateurs dans la bonne direction.

Bien que les marketeurs s'inquiétaient initialement beaucoup de la façon dont le RGPD pourrait avoir un impact sur leurs efforts, cela s'est avéré être une bonne chose pour tout le monde. De nombreuses exigences du RGPD étaient déjà considérées comme les bonnes pratiques pour les expéditeurs d'emails, et cela a incité d'autres à renforcer la protection de la vie privée pour se conformer à la loi.

Voici quelques-unes des principales lignes directrices du RGPD pour les expéditeurs d'emails :

- Obtention du consentement avant d'envoyer un email à à un utilisateur
  - Consentement explicite pour les emails commerciaux
  - Consentement implicite pour la plupart des emails transactionnels
- Possibilité de refuser les communications par email (lien de désinscription)
- Stockage sécurisé des données utilisées pour la personnalisation des emails

- Possibilité de fournir ou de supprimer toutes les informations personnelles identifiables liées à une personne si une demande d'accès par la personne concernée est effectuée
- Liens vers la politique de confidentialité de l'entreprise partout où vous collectez des informations personnelles identifiables telles que des adresses email

Darine affirme que les politiques de confidentialité de l'entreprise doivent être rédigées d'une manière simple et ne pas contenir trop de jargon juridique.

> *« Toute politique de confidentialité doit être claire, compréhensible et transparente. Cela signifie que vous devez indiquer à vos abonnés et clients quelles données vous collectez, comment vous prévoyez de les utiliser, combien de temps elles sont stockées et si elles peuvent être transférées n'importe où. En somme, votre grand-mère devrait pouvoir acheter quelque chose en ligne et comprendre la politique de confidentialité accompagnant cet achat. »*

Darine Fayed, responsable juridique et responsable de la protection des données personnelles chez Mailgun

Le RGPD a incité de nombreux autres pays à revoir de plus près leurs lois sur la protection des données personnelles. La liste ci-dessous risque de vous donner l'impression de nager dans une piscine pleine de sigles.

- L'Inde a mis en œuvre le projet de loi sur la protection des données personnelles (PDPB).
- La Chine applique la loi sur la protection des informations personnelles (PIPL).
- Le Japon utilise sa loi sur la protection des données personnelles (PIPA).
- L'Australie a mis à jour sa loi sur la protection de la vie privée pour répondre aux nouvelles préoccupations numériques.
- La Grande-Bretagne a adopté une version britannique du RGPD après le Brexit.
- Le Brésil a une loi générale sur la protection des données à caractère personnel (LGPD).
- Le Canada suit sa Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).

Il est important de garder à l'esprit que si votre organisation fait des affaires avec des personnes d'un pays spécifique, vous devez vous conformer aux lois sur la protection des données personnelles. Heureusement, si vous respectez déjà les lignes directrices du RGPD, vous serez protégé dans la plupart des domaines.

Découvrez l'approche de Mailgun en matière de conformité au RGPD.

Vous trouverez tous les détails importants sur notre approche du RGPD, y compris le stockage, la sécurité, le traitement et la façon dont nous aidons les clients à gérer les droits des personnes concernées.

CCPA

Aux États-Unis, le règlement le plus complet en matière de confidentialité des données est la Loi californienne sur la protection de la vie privée des consommateurs (CCPA), entrée en vigueur peu de temps après le RGPD. Encore une fois, il existe de nombreuses similitudes entre les deux textes, et la CCPA reflète les bonnes pratiques actuelles pour les expéditeurs d'emails.

Même si la CCPA ne couvre que les résidents de l'État de Californie, de nombreuses entreprises américaines et internationales ont des contacts qui entrent dans cette catégorie. Cela signifie qu'elles doivent être conformes à la CCPA.

Alors qu'il existe d'autres États avec leurs propres lois sur la protection des données personnelles et que d'autres propositions sont en cours d'examen avant d'être validées, selon Darine Fayed, une loi fédérale aux États-Unis pourrait voir le jour dans les années à venir.

PCI DSS

La Norme de sécurité de l'industrie des cartes de paiement (PCI DSS) est destinée à protéger les informations des titulaires de carte de paiement. Il s'agit d'une norme mondiale qui s'applique à toute organisation qui accepte les paiements en ligne.

La conformité PCI inclut des exigences pour la protection des données telles que les numéros de carte de crédit lorsqu'elles sont transmises sur des réseaux ouverts, y compris les emails. Dans la plupart des cas, l'envoi et le transfert par email de données sur les titulaires de carte de paiement n'est pas une bonne idée. Si vous devez transmettre par email les données du titulaire de la carte pour une raison quelconque, vous devez vous assurer qu'elles sont cryptées de bout en bout.

Bien sûr, c'est difficile à faire, surtout si les numéros finissent par se trouver dans la boîte de réception ou le dossier « Envoyé » d'un utilisateur, où un pirate pourrait les trouver. La norme PCI DSS 4.0 stipule que les données de carte de paiement ne peuvent pas être capturées, transmises ou stockées via des technologies de messagerie comme l'email.

La plupart des entreprises utilisent un tiers pour le traitement des cartes de paiement ; cette société tiers gère la conformité PCI. Par exemple, Mailgun utilise le processeur de paiement Stripe. Mais même lorsque vous travaillez avec un tiers, si vous avez des données de titulaire de carte stockées sur vos propres serveurs ou systèmes, vous devez être conforme à la norme PCI.

HIPAA

La loi Health Insurance Portability and Accountability Act (HIPAA) est une loi américaine qui s'applique principalement aux sociétés spécialisées dans la santé. Elle inclut des exigences qui définissent comment empêcher la divulgation d'informations personnelles relatives à la santé d'un patient.

La règle HIPAA la plus importante pour les expéditeurs est que tout email contenant des informations médicales protégées **doit être chiffré en transit**. En outre, les entreprises de santé doivent également obtenir le consentement des patients pour leur envoyer des emails, spécifier dans leur politique de confidentialité comment les informations médicales protégées seront utilisés et avoir un moyen de stocker en toute sécurité les communications par email contenant ces informations.

Des conseils plus complets de Mailgun sur l'email et la conformité HIPAA (article en anglais).

Un autre facteur à prendre en compte sont les logiciels et services que vous utilisez pour envoyer et recevoir des emails. Pour savoir comment un service d'emailing répond aux questions de confidentialité pour le secteur de la santé, demandez à consulter l'accord de partenariat HIPAA. Cet accord de partenariat définit les responsabilités de l'expéditeur et du processeur en ce qui concerne la conformité HIPAA.

Consultez l'accord de partenariat HIPAA de Mailgun.

Passez en revue le document juridique qui explique comment nous abordons la division des droits et des responsabilités en matière de protection des informations personnelles relatives à la santé.

L'importance de la conformité des emails

S'il est vrai que le non-respect de ces textes peut entraîner de lourdes amendes, Darine Fayed affirme que cela ne devrait pas être la seule motivation pour respecter les réglementations en matière de protection de la vie privée.

« Ne respectez pas la confidentialité des données parce que vous avez peur des amendes du RGPD ou de toute autorité de protection des données qui pourrait venir vous chercher. Ce n'est pas pour cela que vous devriez vous en soucier. Il s'agit d'une décision commerciale. Si vous traitez les informations personnelles et privées de vos utilisateurs avec respect, ils reviendront sur votre site. Les utilisateurs sont beaucoup très conscients des risques pour leur vie privée ainsi que de leurs droits. Ils veulent faire confiance aux marques, mais ils s'attendent également à ce que les marques traitent leurs données à caractère personnel avec soin. »

Darine Fayed, responsable juridique et responsable de la protection des données personnelles chez Mailgun

Selon l'enquête sur la confidentialité des consommateurs de Cisco, **89 % des personnes affirment qu'elles se soucient de la confidentialité des données et veulent plus de contrôle**. Toutefois, moins d'un tiers d'entre elles ont de fait agi sur leurs propres données personnelles. En fait, la plupart des personnes attendent des technologies qu'elles utilisent qu'elles leur fournissent la protection de la vie privée dont elles ont besoin. Rester conforme vous aide à répondre à ces attentes.

PARTIE 3

Le contexte des menaces par email

Pour aider votre équipe à comprendre les menaces de sécurité des emails en constante évolution auxquelles votre organisation est confrontée, passons en revue quelques conclusions trouvées dans des recherches récentes menées par des leaders dans le domaine de la cybersécurité.

Bien que ces statistiques changent d'une année à l'autre, et même d'un trimestre à l'autre, elles permettent de dresser un tableau des défis que les équipes techniques doivent relever pour protéger l'email et tout ce qui est connecté à ce canal.

Le hameçonnage, le plus grand défi de la cybersécurité

Selon Deloitte et de nombreuses autres sources, **91 % des cyberattaques commencent par un email de hameçonnage**. La boîte de réception sert le point de départ ; à partir de là, les escrocs peuvent voler des identifiants, envoyer des logiciels malveillants tels que Emotet Trojan, ou prendre les fichiers numériques et les données d'une entreprise en otage contre rançon.

Selon un rapport de Cisco réalisé en 2021, **50 % des entreprises interrogées ont subi des activités liées aux rançongiciels l'année précédente**. Ces brèches de sécurité peuvent être extrêmement coûteuses. Une étude réalisée par Palo Alto Networks a révélé **que le paiement moyen des rançongiciels en 2022 approchait le million de dollars**, soit une augmentation de 71 % par rapport à l'année précédente.

Pourquoi l'email est une menace sérieuse

91 %

des attaques commencent par un hameçonnage par email

50 %

des organisations sont confrontées à une activité de rançongiciel

96 %

des organisations sont ciblées par le hameçonnage par email

Le rapport de Mimecast State of Email Security 2022 révèle que trois entreprises sur quatre interrogées ont connu une augmentation des menaces par email, tandis que **96 % déclarent être la cible de hameçonnage par email**.

Nick Schafer, de Mailgun, convient que les rançongiciels peuvent rapporter gros aux mauvais acteurs. Cependant, selon lui, le nombre incalculable d'attaques d'hameçonnage par email devrait en faire une priorité absolue pour chaque organisation.

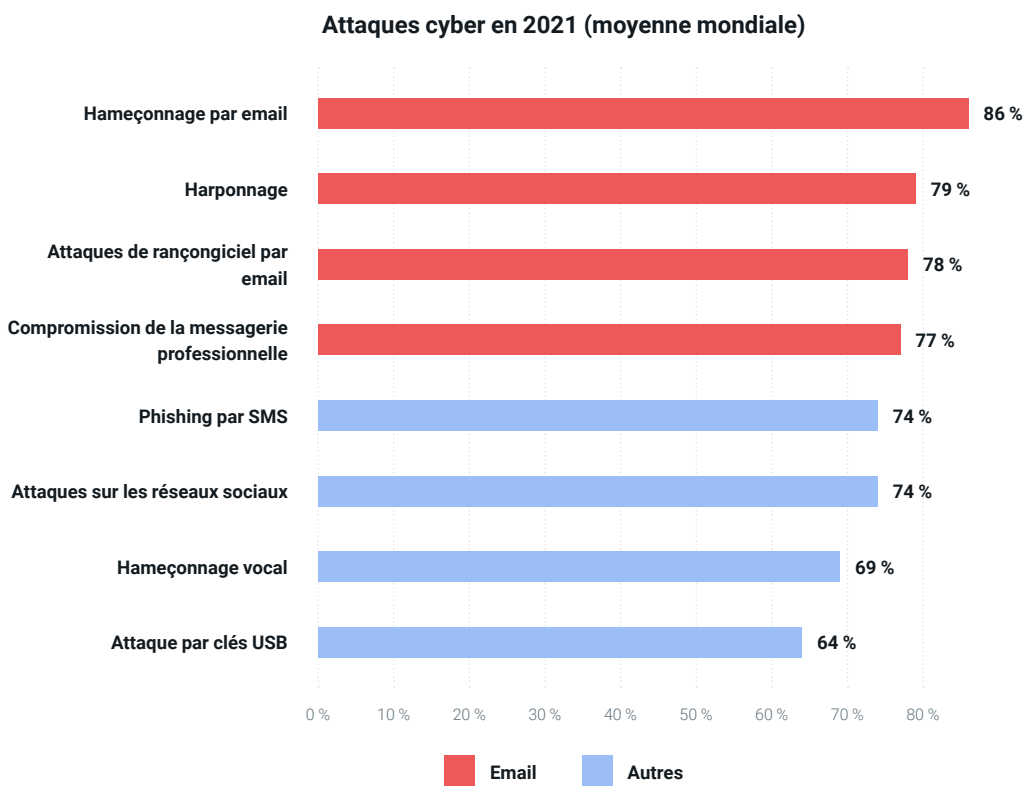
« De mon point de vue, le hameçonnage est le plus grave problème. Je suis convaincu que les escrocs pensent au retour sur investissement comme tout le monde, et qu'ils peuvent l'obtenir grâce aux attaques de rançongiciels. Mais par rapport à ce que nous voyons, la quantité d'attaques de hameçonnage ne fait que s'aggraver. Et les cybercriminels sont doués dans ce qu'ils font »

Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

Les menaces par email comparées à celles sur d'autres canaux

Le rapport 2022 State of the Phish de Proofpoint a examiné l'impact du hameçonnage par email et via d'autres canaux sur les entreprises du monde entier. L'entreprise a interrogé des centaines de professionnels de l'informatique et des milliers d'autres employés aux États-Unis, en Australie, en France, en Allemagne, au Japon, en Espagne et au Royaume-Uni.

Alors que les entreprises de ces pays ont subi toutes sortes de menaces sur différents canaux, **les attaques par email représentaient les quatre principaux points d'attaque**. Un total de 86 % des organisations dans l'enquête de Proofpoint ont signalé au moins une attaque par hameçonnage en masse en 2021, ce qui en fait la plus courante.



Parmi tous les types de tentatives de hameçonnage, **83 % des personnes interrogées dans le monde ont déclaré qu'au moins l'une de ces attaques avait réussi en 2021**.

Les dégâts de l'hameçonnage

Nous avons déjà vu que l'impact monétaire potentiel de l'atténuation d'une brèche de sécurité peut être assez coûteux. Cependant, les millions d'euros dépensés suite à une cyberattaque ne sont pas les seules façons dont ces incidents affectent les entreprises, grandes et petites.

L'enquête de Proofpoint a interrogé les professionnels de l'informatique du monde entier sur l'impact principal des attaques par hameçonnage réussies sur leurs organisations. Les effets les plus cités étaient la fuite des données client (54 %), la compromission d'identifiants (48 %) et les infections par rançongiciel (46 %).

Principaux impacts d'une attaque par hameçonnage réussie

54 %	48 %	46 %
Fuite/perte de données clients	Identifiants/comptes compromis	Infections par rançongiciel

Les infections par rançongiciel ne sont pas loin derrière. Proofpoint a constaté que **44 % des personnes interrogées considèrent la « perte de données et de propriété intellectuelle » comme un autre impact négatif d'une attaque par hameçonnage réussie**. En réalité, tous ces facteurs peuvent avoir un impact durable sur une entreprise, réduisant la confiance, augmentant les coûts et exposant même les secrets commerciaux qui donnent aux entreprises un avantage concurrentiel.

Prioriser la sécurité

Dans ces circonstances, quels sont les points sur lesquels les équipes techniques concentrent leurs efforts lorsqu'il s'agit de déjouer les failles de sécurité ? Compte tenu des statistiques que nous venons d'examiner, il n'est pas étonnant que la protection **des emails soit une préoccupation de premier ordre pour la sécurité dans de nombreuses organisations**.

GreatHorn a interrogé des centaines de professionnels de l'informatique et de la cybersécurité pour savoir ce qui les inquiète le plus. Les trois principaux types de projets cités par les répondants en 2021 étaient la sécurité des emails (48 %), la sécurité autour du travail à distance et du télétravail (41 %), et la gestion de la sécurité dans le cloud (40 %).

Principaux projets de sécurité en 2021

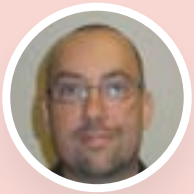
48 %	41 %	40 %
Sécurité des emails	Sécurité du télétravail	Gestion de la sécurité dans le cloud

Un projet informatique plus spécifique lié à tous ces problèmes de sécurité est le passage d'une solution de messagerie sur site à une approche basée dans le cloud. GreatHorn a constaté que si seulement 24 % des répondants à l'enquête utilisent encore une solution sur site, **77 % de ces organisations prévoyaient de passer à des fournisseurs dotés d'une infrastructure de messagerie basée dans le cloud**. Cela permet aux expéditeurs de trouver des fournisseurs disposant de mesures de sécurité plus avancées, notamment des partenariats avec des services de cloud computing public fiables tels qu'Amazon Web Services (AWS), Google Cloud Platform (GCP) et Microsoft Azure.

Certes, renforcer la cybersécurité autour de l'email ou de tout autre domaine nécessitera des investissements en temps, en ressources et en budget. Cependant, l'insuffisance des budgets de cybersécurité peut donner du fil à retordre aux équipes techniques.

Le rapport 2022 State of Email Security de Mimecast a révélé que **95 % des entreprises dont le budget de cybersécurité est insuffisant estiment que cela a nui à la résilience et entraîné un manque de préparation**. Le rapport indique que des efforts tels que la sensibilisation à la sécurité et les formations aux nouvelles technologies sont deux domaines dans lesquels il manque suffisamment de fonds.

Dan Ross dirige l'équipe de gouvernance, risque et conformité chez Mailgun by Sinch. Il explique que l'engagement de notre entreprise à investir dans une sécurité forte est un avantage pour ses équipes, nos clients et tous nos employés.



« Les équipes de direction nous ont donné le budget nécessaire pour protéger notre entreprise et les données de nos clients avec les meilleures technologies du secteur. Je pense que ce qui place Mailgun en tant que leader en matière de sécurité, c'est la façon dont nous réagissons aux menaces connues, et les outils que nous utilisons pour nous assurer que les mauvais acteurs restent hors de notre réseau. Et en interne, nous avons mis en place des dispositifs pour protéger essentiellement les employés d'eux-mêmes. »

Dan Ross, Responsable de la gouvernance, du risque et de la conformité senior chez Mailgun

PARTIE 4

Garantir la sécurité des emails

Il existe plusieurs points où la sécurité de l'email peut être compromise :

1. L'endroit où sont stockées les données de l'email et les informations de contact
2. Les plateformes partagées pour l'envoi d'emails
3. Lors du transit ou de l'envoi des messages d'un service d'emailing vers les destinataires
4. Dans une boîte de réception lorsqu'un email arrive pour être authentifié et filtré
5. Après qu'un email a été reçu et se trouve dans la boîte de réception d'un destinataire

Certaines parties ont des responsabilités spécifiques en matière de sécurité et de confidentialité tout au long du parcours. Penchons-nous sur chacun des points mentionnés ci-dessus et découvrons ce qu'il faut faire pour avoir une sécurité solide dans tous les domaines de votre emailing.

Sécurité des emails et stockage des données

Les données d'emailing, qu'elles soient stockées sur site ou dans le cloud, doivent être protégées par chiffrement lorsqu'elles sont inactives. Par exemple, **Mailgun utilise le chiffrement AES-256 pour toutes les données client**. Cela signifie qu'une clé de 256 bits est nécessaire pour chiffrer et déchiffrer des blocs d'emails.

AES est une méthode open-source utilisée dans le monde entier. Elle est considérée comme efficace pour prévenir les attaques par force brute. C'est ce qu'utilisent les agences gouvernementales telles que la NSA pour le chiffrement de ses données. Les principaux fournisseurs de services de cloud computing publics tels que GCP, AWS et Azure utilisent également le cryptage AES-256.

La plupart des expéditeurs de volumes importants d'emails se sont tournés vers des solutions basées sur le cloud pour l'emailing. Si vous optez pour des partenaires stockant des adresses email ou toute autre donnée sensible en votre nom, il existe d'autres mesures de sécurité qui permettront de protéger ces informations à l'intérieur de leurs centres de données. Cela comprend des mesures telles que le contrôle de l'accès aux centres de données avec une surveillance 24 heures sur 24 et des systèmes de contrôle biométrique.

Sécurité des emails et réputation d'expéditeur

Lorsque vous utilisez un service d'emailing comme Mailgun, vous aurez normalement la possibilité de choisir des abonnements qui utilisent des adresses IP dédiées ou partagées pour l'envoi des emails.

À moins que vous ne soyez un expéditeur de gros volumes, une adresse IP partagée est généralement suffisante. Mais que se passe-t-il si vous envoyez des emails à partir de la même adresse IP qu'un mauvais acteur ? **Cela pourrait compromettre votre réputation d'expéditeur**.

Les services de messagerie utilisent divers facteurs pour évaluer la réputation d'expéditeur. Deux des facteurs les plus importants sont la réputation de l'adresse IP et la réputation du domaine.

Les services de messagerie comme Gmail ont commencé à accorder une plus grande importance à la réputation du domaine. La raison en est qu'elle est beaucoup plus ciblée sur des expéditeurs spécifiques. De nombreux domaines peuvent envoyer à partir d'une seule adresse IP. Ainsi, la réputation d'un domaine est plus étroitement liée à une certaine entreprise ou marque. La réputation de l'adresse IP, cependant, est toujours un facteur, en particulier avec le client de messagerie Outlook, ce qui signifie que **réputation de l'adresse IP pourrait avoir un effet démesuré sur les emails B2B**.

Pour cette raison (entre autres), l'équipe de Mailgun travaille dur pour empêcher les mauvais acteurs d'utiliser notre plateforme pour envoyer des emails à partir d'adresses IP partagées. Nick Schafer et l'équipe de délivrabilité et de conformité examinent et vérifient systématiquement les nouveaux utilisateurs avant qu'ils ne soient autorisés à utiliser la plateforme.

« Si de mauvais expéditeurs se connectent à l'une de nos IP partagées, les services de messagerie le remarqueront. La réputation d'expéditeur d'autres clients sur la même adresse IP peut être affectée négativement. Les services de messagerie voient désormais l'adresse IP partagée comme un endroit où les expéditeurs font des choses peu nettes. Nous devons donc arrêter les mauvais acteurs rapidement et protéger les clients. Cette solution protège la réputation de Mailgun en tant qu'expéditeur, ce qui est vraiment important pour les utilisateurs sur des adresses IP partagées. »

Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

Les clients de Mailgun sont également tenus de respecter notre Politique d'Utilisation Acceptable (PUA). C'est une autre façon de protéger la réputation d'expéditeur de tous les utilisateurs. **Notre PUA comprend (entre autres) les stipulations suivantes** :

- Un taux de rebond inférieur ou égal à 5 %
- Un taux de désinscription inférieur ou égal à 1,4 %
- Un taux de plaintes pour spam inférieur ou égal à 0,8 %
- Aucune liste de contacts achetée, louée ou récupérée
- L'obtention du consentement explicite avant l'envoi d'emails non transactionnels
- Un lien de désinscription dans chaque email
- Pas de stockage, de transmission ou de publication de contenu interdit (prêts sur salaire, jeux d'argent illégaux, contenu diffamatoire, contenu faisant la promotion de la violence, etc)
- Utilisation réduite des ressources partagées de la plateforme

La PUA garantit que nous travaillons tous ensemble pour suivre les bonnes pratiques, en tant qu'expéditeurs, dans un environnement numérique partagé. Elle n'est pas destinée à menacer qui que ce soit. La PUA ressemble davantage à un code de conduite.

> *« Nous surveillons le bon respect de ces directives par les clients de Mailgun. Si quelqu'un franchit l'un de ces seuils, nous n'allons pas nécessairement lu interdire l'accès à la plateforme. On sait que des écarts peuvent arriver de temps en temps. Donc, nous allons d'abord leur recommander de revoir leurs pratiques. »*
>
> Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

Le chiffrement des emails en transit

Le protocole simple de transfert de courrier (SMTP) est le protocole standard pour la transmission d'emails. Les serveurs SMTP traitent le message, l'envoi, la réception et le relais d'emails d'un serveur à un autre. Mais, SMTP a un problème assez important... il n'est pas sécurisé.

SMTP sous sa forme de base ne prend pas en charge le chiffrement ou les algorithmes d'authentification. C'est une des raisons pour lesquelles les spammeurs et les escrocs utilisent les emails et pourquoi des protocoles d'authentification séparés, comme SPF et DKIM, ont été créés.

Les spammeurs et les hameçonneurs ont souvent exploité les serveurs SMTP configurés avec des relais ouverts. Mais, les serveurs SMTP protégés par mot de passe peuvent également être piratés, exposant les données contenues dans les emails. Les mauvais acteurs peuvent utiliser le protocole SMTP pour diffuser

des virus et des logiciels malveillants, ainsi que pour mener des attaques DoS. Il est même possible de modifier un email en route vers un destinataire. Les données doivent donc également être protégées pendant que les emails sont en transit.

C'est pourquoi les expéditeurs et les services d'emailing ajoutent des protocoles de chiffrement tels que TLS et SSL au protocole SMTP. Mailgun a cessé de prendre en charge SSL en 2014, en raison d'une vulnérabilité connue sous le nom de POODLE, qui a permis des attaques.

TLS utilise un chiffrement asymétrique pour établir une session sécurisée entre un client et un serveur. Ensuite, il utilise un chiffrement symétrique pour échanger des données au sein de la session sécurisée. C'est ce que l'on appelle la négociation TLS : le processus par lequel la communication entre un client et un serveur est établie et définie.

Par défaut, Mailgun utilise désormais ce qu'on appelle le **chiffrement opportuniste via TLS** (TLS version 1.2) pour les emails. Ce dernier essaiera de mettre à niveau les serveurs de réception vers TLS si nécessaire, mais passe au protocole SMTP en texte brut si TLS n'est pas pris en charge, ce qui garantit la délivrabilité.

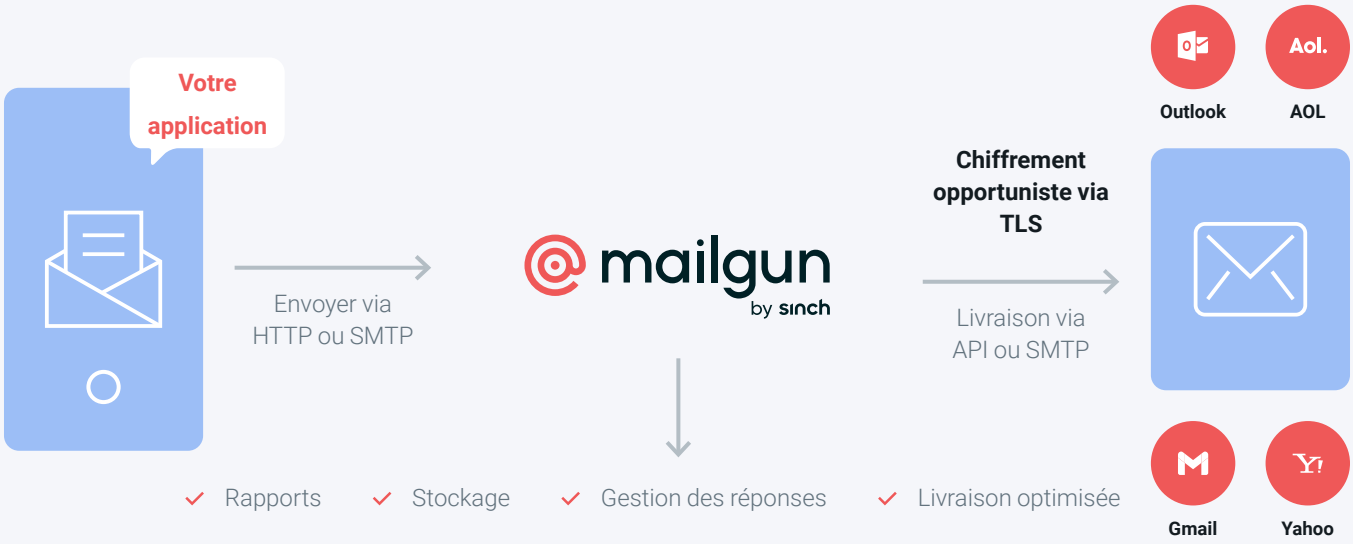
Vous pouvez également ajouter des indicateurs au chiffrement opportuniste via TLS pour personnaliser les paramètres de connexion pour l'envoi des emails. Il s'agit de `require tls` et `skip verification`.

- `require tls :`
  - Lorsqu'il est défini sur TRUE, le serveur de réception envoie un email uniquement si le serveur de réception prend en charge le TLS.
  - Lorsqu'il est défini sur FALSE, nous tenterons de procéder à la mise à niveau, puis d'envoyer un SMTP en texte brut en cas d'échec.
- `skip verification :`
  - Lorsque la valeur est TRUE, nous n'essayons pas de vérifier le certificat et le nom d'hôte lorsque nous tentons d'établir une connexion TLS.
  - Lorsqu'il est défini sur FALSE, nous essayons de vérifier le certificat et, si nous ne pouvons pas le faire, une connexion TLS ne sera pas établie.

En savoir plus sur TLS et l'emailing.

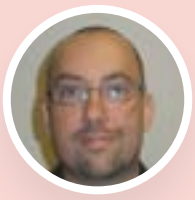
Des informations complémentaires essentielles sur le chiffrement des communications par email et le fonctionnement du contrôle des connexions TLS sur mailgun.com. Article en anglais. ›

Mailgun recommande souvent d'utiliser notre Email API au lieu du SMTP. L'API est jusqu'à trois fois plus rapide, facile à utiliser et idéale pour les envois par lots de gros volumes. De plus, Mailgun permet d'utiliser différentes clés d'envoi de domaine lors de la gestion de plusieurs expéditeurs. Cependant, les pirates peuvent accéder à la fois aux identifiants SMTP et aux clés API.



Il est donc important de renouveler régulièrement les clés API et de protéger vos mots de passe SMTP. Jonathan Torres de Mailgun affirme que l'exposition accidentelle des clés API et des identifiants SMTP est l'une des méthodes les plus courantes de compromettre la sécurité de l'email.

Dan Ross souligne que les données de l'email nécessitent également une protection lorsque vous déplacez des listes de contacts d'une plateforme à l'autre. C'est une autre situation dans laquelle les données sensibles sont en danger durant le transit.



« Il est important de comprendre comment les adresses email et les contacts arrivent dans les outils que vous utilisez pour envoyer des emails. Mailgun dispose d'une API sécurisée, ce qui nous distingue dans le milieu. Nos clients utilisent l'API pour importer des emails et des adresses email à une vitesse incroyable. Si vous disposez d'un tunnel sécurisé, cela réduit le risque que ces données soient interceptées pendant le transit. »

Dan Ross, Responsable de la gouvernance, du risque et de la conformité senior chez Mailgun

Sécurité et authentification des emails

Si de mauvais acteurs tentent d'usurper votre marque à l'aide d'emails de hameçonnage, il existe des moyens très efficaces d'empêcher ces emails d'atteindre la boîte de réception. **Les protocoles d'authentification des emails aident les services de messagerie à décider si les emails peuvent être faux ou falsifiés** avant qu'ils ne soient livrés aux destinataires.

Les protocoles d'authentification de l'email sont apparus au début des années 2000 comme un moyen d'améliorer la sécurité du SMTP et de contrecarrer l'augmentation des spams. Les protocoles SPF et DKIM ont été les premières méthodes largement adoptées. DMARC a rapidement suivi en tant que politique visant à confirmer et à étendre SPF et DKIM. La section suivante traite en détail de ces protocoles.

Chez Mailgun, nous demandons aux utilisateurs de configurer des enregistrements SPF et DKIM sur leurs serveurs DNS. Si vous ne l'avez pas fait ou si vous avez besoin d'aide, nous pouvons vous aider. Nous recommandons également d'appliquer une politique DMARC et pouvons orienter nos clients vers des fournisseurs de services dignes de confiance si nécessaire. **La configuration des enregistrements DNS pour l'authentification améliorera également la réputation d'expéditeur et la délivrabilité des emails.**

> *« Les services de messagerie ont besoin de moyens pour identifier qui est vraiment un expéditeur. Sans authentification par email, il est difficile de dire d'où vient réellement le trafic. Grâce à l'authentification, les expéditeurs peuvent indiquer que cet email a été envoyé par eux, qu'il s'agit de leur email et qu'ils sont autorisés à l'envoyer. »*
>
> Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

S'informer sur la sécurité des emails

En matière de sécurité de l'email, ce que les destinataires ignorent peut *certainement nuire* à leur réputation. Mais, une équipe bien formée et des abonnés avertis seront beaucoup plus susceptibles de repérer les spammeurs et les escrocs avant de comettre une grosse erreur.

Dan Ross de Mailgun affirme qu'un programme de sensibilisation des employés **est essentiel pour la sécurité des emails**. N'oubliez pas à quel point le harponnage professionnel est devenu répandu. Ces attaques ciblent les employés au sein de votre organisation. Dans une situation idéale, la formation et les tests devraient avoir lieu chaque année et avec toutes les nouvelles recrues.

Tout au long de l'année, vous pouvez également mettre cette formation à l'épreuve en envoyant vos propres emails de harponnage aux employés comme test (de faux emails en un sens). Cela vous permet d'évaluer le degré de vigilance des utilisateurs, de garder les employés sur le qui-vive et de rappeler à chacun ce à quoi il faut faire attention en cas de tentative de harponnage.

« Chez Mailgun, nous envoyons des tests de harponnage. Si une personne clique dessus, nous avons une conversation avec les employés pour expliquer pourquoi ils doivent être plus prudents. Nous suivons ces indicateurs et faisons tout notre possible pour tenir nos employés informés sur le harponnage. »

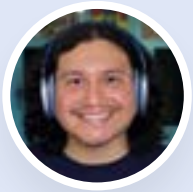
Dan Ross, Responsable de la gouvernance, du risque et de la conformité senior chez Mailgun

Ainsi, la sécurité de vos emails est répartie également entre tous les maillons. Chaque maillon supporte le même poids. Par conséquent, si l'un des maillons est plus faible, il sera le premier à casser, ce qui brisera la chaîne en entier. Et, dans presque toutes les organisations, le maillon le plus faible est l'être humain, et non un outil technologique.

Selon le rapport State of Email Security 2022 de Mimecast, **les employés bénéficiant d'une formation de sensibilisation aux cybermenaces sont cinq fois plus susceptibles de repérer et d'éviter de cliquer sur des liens malveillants**. Cependant, même si la quasi-totalité des organisations interrogées disposent d'une formation, seuls 34 % la proposent régulièrement. Et ce malgré le fait que quatre répondants sur dix ont cité la naïveté des employés comme un défi majeur pour la sécurité des emails en 2022.

La sensibilisation des clients et des abonnés est également importante. Si votre entreprise est exposée à des attaques par hameçonnage et d'usurpation d'identité, ou si vous avez connaissance d'emails frauduleux qui détournent votre marque, soyez proactif dans cette situation. N'attendez pas que ces messages frauduleux fassent des victimes. Informez-les et avertissez-les de ces programmes. Indiquez clairement les types d'informations que vous allez demander et que vous ne demanderez pas par email.

Malheureusement, la plupart des entreprises ne pensent pas à informer leurs clients sur les risques d'usurpation de marque tant qu'elles ne rencontrent pas ces problèmes. Pourtant, Jonathan Torres dit qu'un incident d'usurpation de marque est une occasion d'être transparent et de regagner la confiance de vos utilisateurs.



« La dernière chose que vous voulez, c'est que le nom de votre entreprise soit utilisé dans un email qui semble légitime, mais qui met le destinataire en situation périlleuse. Je pense que c'est une chose dont les expéditeurs se rendent souvent compte après qu'il soit trop tard. Alors ils doivent faire marche arrière. Donc, si votre identité a été usurpée, soyez transparent avec vos abonnés. Une bonne communication est essentielle. Expliquez aux abonnés ce qui s'est passé et ce que vous faites pour consolider vos systèmes, afin que cela ne se reproduise pas. »

Jonathan Torres, Responsable des chargés de compte chez Mailgun

Alors, comment pouvez-vous exactement « consolider les systèmes », comme le dit Jonathan ? Si vos identifiants sont accidentellement divulgués, et qu'une personne commence à envoyer du spam à partir de votre compte, il est probable que Mailgun le saura avant vous, et nous y mettrons un terme. Mailgun aide également les expéditeurs à restreindre l'accès aux clés API et aux identifiants SMTP vous permettant d'attribuer des rôles d'utilisateur au sein de la plateforme.

Quelle que soit la plateforme d'envoi d'emails que vous utilisez, nous vous recommandons vivement de réinitialiser les clés API et les mots de passe SMTP immédiatement, ainsi que de vérifier si votre domaine d'envoi a été bloqué en raison d'une fuite. Configurer l'authentification à deux facteurs permettra également d'éviter que ce problème ne se reproduise.

Mais y a-t-il autre chose que les expéditeurs peuvent faire pour lutter contre l'usurpation de marque ? Il y en a. **Tout est une question d'authentification par email**. Nous aborderons ce sujet important dans la prochaine section.

PARTIE 5

L'authentification, la meilleure protection des emails

Le moment clé dans la transmission des emails survient lorsqu'un service de messagerie, comme Gmail ou Outlook, doit décider comment filtrer un email. L'expéditeur de cet email est-il vraiment celui qu'il prétend être ? Est-ce du spam ? Est-ce dangereux ? Devrions-nous bloquer ce message, l'envoyer dans le dossier du spam ou en boîte de réception ?

Comme Kate Nowrouzi l'a mentionné plus tôt dans ce guide, il n'est pas toujours facile de répondre à ces questions, même si vous êtes un spécialiste de l'anti-spam. C'est pourquoi le secteur d'emailing a développé des **protocoles d'authentification** et d'autres spécifications techniques pour demander concrètement aux expéditeurs de prouver leur identité avant d'être autorisés à accéder à la boîte de réception.

Pour chaque protocole ou spécification, il existe un enregistrement TXT du DNS qui doit être ajouté et correctement formaté sur les serveurs du nom de domaine. Examinons quatre points clés de l'authentification des emails, notamment leur utilité, leur fonctionnement et leur interaction.

1. Le protocole SPF

Sender Policy Framework (SPF) est un protocole qui répertorie les adresses IP des serveurs de messagerie et des noms de domaine autorisés à envoyer des emails en votre nom. L'enregistrement SPF agit comme le videur d'une boîte de nuit. Si vous n'êtes pas sur la liste, vous n'entrez pas.

Par exemple, si vous envoyez des emails transactionnels via Mailgun, un service d'emailing différent pour les emails marketing, et que vous utilisez Google Workspace pour les emails internes, les trois doivent être identifiés sur votre enregistrement SPF. Ainsi, si les services de messagerie remarquent des messages provenant d'un expéditeur non autorisé, ils peuvent choisir de bloquer ces messages ou de les envoyer dans le dossier du spam.

Quelques détails techniques

Voici un exemple d'enregistrement DNS du protocole SPF :

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

Voici un exemple d'enregistrement TXT du DNS pour le protocole SPF ci-dessus :

La version du protocole SPF utilisée :

Cela devrait toujours être « `v=spf1` » (la première version), car toutes les autres ont été abandonnées.

Liste des expéditeurs autorisés :

Tout domaine qui envoie des emails en votre nom doit être répertorié à l'aide de mécanismes tels que des adresses IP, des noms d'hôte ou des enregistrements « `a` ». Vous pouvez choisir d'utiliser le même type de mécanisme ou d'appariement.

Vous avez le choix entre plusieurs mécanismes :

1. Le mécanisme `ip4` ou `ip6` répertorie les adresses IP autorisées à envoyer en votre nom.
2. Le mécanisme de **« a** » permet au serveur entrant de référencer les enregistrements « `un` » d'un domaine, au lieu d'une adresse IP spécifique. Tant que l'adresse IP d'où provient l'email se trouve parmi les enregistrements « `a` » , l'email passera l'authentification SPF.
3. Le mécanisme `MX` indique les adresses IP que votre domaine utilise pour recevoir des emails. Si un email est envoyé à partir de l'une de ces adresses IP, le serveur de courrier entrant doit l'accepter.
4. Le mécanisme « `include` » est également utilisé pour inclure l'enregistrement SPF du domaine donné. C'est ce que Mailgun utilise comme moyen pour les clients d'ajouter toutes les adresses IP Mailgun à leur SPF.

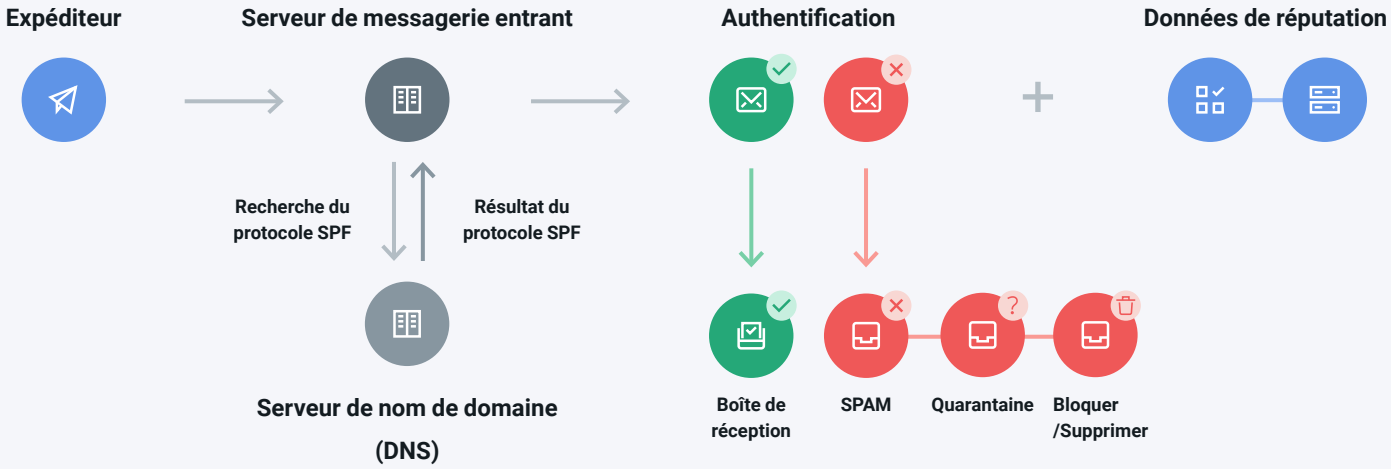
Le mécanisme « all » ou la qualification d'échec :

Un mécanisme « all » se trouve à la fin de chaque enregistrement SPF. Il informe les serveurs de courrier entrant sur ce qu'il faut faire si l'authentification de l'email échoue.

- `-all` : si aucune correspondance exacte n'est trouvée, l'email a échoué. L'email sera bloqué et n'arrivera pas dans la boîte de réception, de quelque manière que ce soit. C'est la meilleure façon d'utiliser le protocole SPF pour éviter l'usurpation d'identité.
- `~all` : si aucune correspondance exacte n'est trouvée, l'email échoue, mais sera toujours envoyé. Cependant, il sera marqué comme suspect et sera probablement envoyé dans le dossier du spam.
- `+all` : cela permet à n'importe quel serveur d'envoyer à partir de votre domaine. Il devrait rarement être utilisé, car chaque email réussira l'authentification SPF. Cela signifie que n'importe qui pourrait usurper votre identité en tant qu'expéditeur.
- `?all` : c'est un paramètre par défaut. Les emails ne réussissent pas ou échouent l'authentification SPF si l'adresse IP n'est pas répertoriée. C'est le service de messagerie qui prend la décision.

> ***Notez qu'un domaine ne peut avoir qu'un seul enregistrement SPF.*** *Si un domaine possède plusieurs enregistrements SPF, l'authentification des emails échouera. Bien que les services de messagerie ne prennent pas toujours des mesures en cas de défaillance du protocole SPF, il s'agit d'une partie importante de l'alignement du protocole DMARC, que nous explorerons plus tard.*

Fonctionnement de l'authentification SPF



Lorsque les services de messagerie utilisent l'authentification SPF, le serveur de courrier entrant vérifie le chemin de retour dans l'en-tête de l'email. Il vérifie ensuite que l'email provient de l'une des adresses IP répertoriées dans l'enregistrement TXT du DNS.

Si le serveur de courrier entrant authentifie l'expéditeur, il livre l'email en boîte de réception. Si l'authentification échoue, l'email sera bloqué ou envoyé dans le dossier du spam en fonction de la définition de la qualification d'échec (les mécanismes `all`).

Le protocole SPF présente quelques inconvénients. D'une part, il s'interrompt lorsqu'un email est transféré, car il est maintenant envoyé depuis une IP qui ne figure pas dans l'enregistrement. **Ensuite, le protocole SPF est limité à 10 mécanismes (ou adresses IP approuvées)**, ce qui peut ne pas être suffisant pour les grandes organisations et les expéditeurs de gros volumes avec de nombreuses branches envoyant au nom du domaine principal.

2. Le protocole DKIM

Le protocole DKIM (DomainKeys Identified Mail) est un protocole d'authentification qui combine deux méthodes conçues pour empêcher la falsification d'emails : « DomainKeys » de Yahoo et « Identified Internet Mail » de Cisco.

Comme pour le protocole SPF, l'authentification DKIM implique un enregistrement TXT du DNS auquel les serveurs de courrier entrant se réfèrent lors de la vérification de l'authenticité d'un expéditeur, mais c'est un peu plus avancé. Le protocole DKIM permet également de déterminer si un email a été modifié pendant le transit. Aujourd'hui, tous les principaux services de messagerie vérifient les emails selon le protocole DKIM.

Comme son nom l'indique, le protocole DKIM implique l'utilisation de clés chiffrées, également connues sous le nom de signatures numériques. La clé secrète est ajoutée à un en-tête d'email afin d'associer l'email à un certain domaine et de vérifier l'expéditeur. La clé DKIM chiffrée est appariée à une clé publique localisée dans l'enregistrement TXT du DNS.

Quelques détails techniques

Voici un exemple d'enregistrement DNS du protocole DKIM :

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

Voici un exemple d'enregistrement TXT du DNS pour la signature DKIM :

- `v=` La version du protocole utilisée
- `t=` Balise facultative. Elle indique que le domaine d'envoi *teste* le protocole DKIM
- `k=` Type de clé (généralement rsa)
- `p=` Clé publique associée à la signature DKIM chiffrée
- La seule balise obligatoire dans l'enregistrement DNS est la clé publique (`p=`). L'enregistrement DKIM inclut également le domaine d'envoi et le sélecteur. Ce dernier est un nom ou un numéro que l'expéditeur utilise pour indiquer aux serveurs de messagerie de réception où trouver la clé publique. **L'en-tête de signature DKIM** est ajouté aux emails et comprend les informations dont les serveurs de messagerie ont besoin pour vérifier l'authenticité d'un email.

Voici un exemple d'en-tête DKIM :

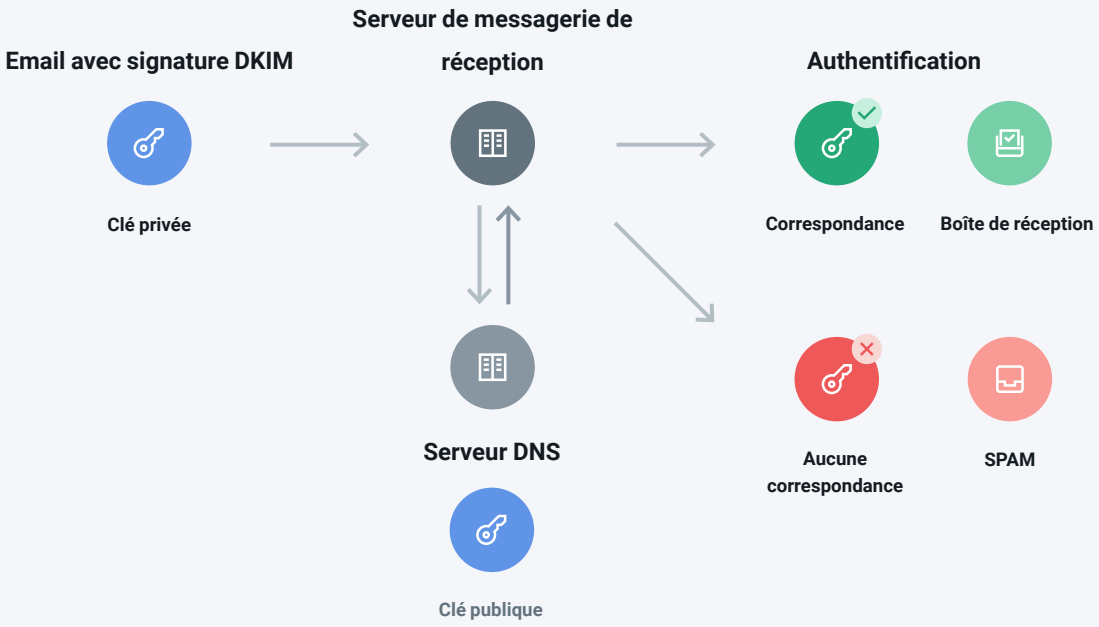
```
DKIM-Signature v=1; a=rsa-sha256; q=dns;
d=exemple.com;
s= dk1024-2012; t=1117574938; x=1118006938;
h=Content-Type: Mime Version: Subject: From: To: Sender; Date: List-
Unsubscribe
bh=PV3AoaeTApQYJwe3qgbuUFFTVhjwhv1q2gGNBL+KHU=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

Voici un aperçu des balises trouvées dans l'exemple d'en-tête DKIM ci-dessus :

- `v=` La version de DKIM
- `a=` L'algorithme de signature
- `q=` La méthode de requête par défaut
- `d=` Le domaine de signature associé à un enregistrement de sélecteur pour localiser une clé publique
- `s=` Le sélecteur utilisé pour rechercher la clé publique et autoriser plusieurs clés sur un domaine
- `t=` L'horodatage de la signature
- `x=` Le délai d'expiration
- `h=` La liste des en-têtes utilisés dans l'algorithme de signature
- `bh=` Le hachage du corps après avoir été canonicalisé par Base64, qui transforme le code binaire en texte
- `b=` La signature DKIM réelle des en-têtes et du corps, encodée avec Base64

Certaines balises DKIM facultatives peuvent également être ajoutées aux informations d'en-tête. D'autres balises d'en-tête DKIM sont requises : `v`, `a`, `d`, `s`, `h`, `bh` et `b`. D'autres encore, comme `t` et `x`, sont facultatives, mais recommandées.

Fonctionnement de l'authentification DKIM



Une signature DKIM permet aux services de messagerie et aux Mail Transfer Agents (MTA) de savoir où récupérer la clé publique. Si la clé publique est associée à la signature chiffrée, les services de messagerie sont plus susceptibles de la livrer en boîte de réception. S'il n'y a pas de correspondance, ou s'il n'y a pas de signature DKIM du tout, l'email est plus susceptible d'être rejeté ou redirigé vers le dossier du spam.

Le protocole DKIM ne filtre pas les emails. Cependant, il aide les serveurs de messagerie de réception à décider de la meilleure façon de filtrer les emails entrants. Une vérification du protocole DKIM réussie signifie souvent un score de spam réduit pour un email.

3. Le protocole DMARC

Strictement parlant, le rapport d'authentification des messages de domaine (DMARC) n'est pas un protocole d'authentification. Il s'agit d'une spécification technique qui définit une politique d'authentification des emails. DMARC aide les expéditeurs et les services de messagerie à tirer le meilleur parti de SPF et DKIM tout en fournissant des rapports qui fournissent des informations stratégiques sur qui essaie d'envoyer depuis le domaine.

L'objectif principal d'une politique DMARC est de vérifier l'alignement SPF et DKIM. Il est ainsi considéré comme le moyen le plus efficace d'empêcher les mauvais acteurs d'usurper l'identité de votre marque par email. Lorsque DMARC est implémenté, les services de messagerie vérifient à la fois SPF et DKIM, puis se réfèrent à la politique que l'expéditeur définit dans l'enregistrement DNS du protocole DMARC.

Les options de la politique DMARC sont :

- **Reject :** il s'agit des emails qui échouent le protocole DMARC et ne seront pas remis (`p=reject`).
- **Quarantine :** les emails qui échouent le protocole DMARC seront filtrés dans le dossier du spam (`p=quarantine`).
- **None :** les emails sont autorisés à transiter indépendamment du succès ou de l'échec du protocole DMARC. Cette option est utilisée uniquement pour les rapports ou lors de la configuration et des tests DMARC (`p=none`).

Quelques détails techniques

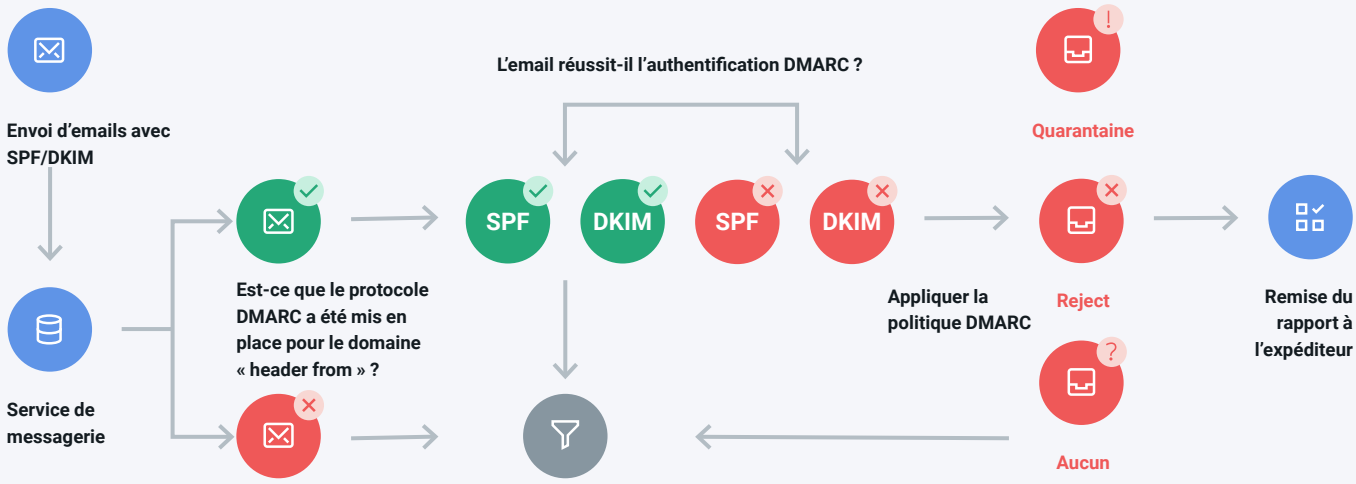
```
1  v=DMARC1; p=quarantine; sp=none; rua=mailto:dmarc-reports@example.
   com; pct=100; aspf=s; adkim=s
```

Les enregistrements DMARC peuvent sembler un peu plus simples que cela, mais aussi plus compliqués, selon le nombre de balises qu'un expéditeur décide d'utiliser. Voici une liste complète des balises du protocole DMARC possibles avec leurs explications :

- `v=` est la version de DMARC utilisée.
- `p=` est la politique d'application du protocole DMARC : none, quarantine, ou reject.
- `rua=` est la liste des adresses électroniques où les rapports agrégés du protocole DMARC sont envoyés.
- `pct=` est le pourcentage d'emails soumis à la politique d'application. La valeur par défaut est pct=100.
- `aspf=` définit le mode d'alignement pour le protocole SPF, qui peut être strict ou détendu avec des scénarios de réussite/échec.
- `adkim=` définit le mode d'alignement pour le protocole DKIM, qui peut être strict ou détendu avec des scénarios de réussite/échec.
- `sp=` représente différentes stratégies d'application pour les sous-domaines.
- `ruf=` répertorie les adresses email pour l'envoi de rapports d'échec/d'analyse du protocole DMARC, qui sont plus détaillées que les rapports agrégés.
- `fo=` indique les options de création d'un rapport d'échec/d'analyse du protocole DMARC.
- `rf=` déclare le format de rapport d'analyse pour les rapports d'échec spécifiques aux emails.
- `ri=` définit l'intervalle d'envoi des rapports du protocole DMARC, défini en secondes, mais est généralement de 24 heures ou plus.

Ainsi, dans notre exemple d'enregistrement TXT du DNS, l'expéditeur dispose d'une politique DMARC définie sur quarantaine, sans différence pour les sous-domaines. Il y a une adresse email pour recevoir des rapports agrégés. 100 % des messages sont soumis à la politique DMARC, et les modes d'alignement SPF et DKIM sont définis sur « strict ». Lorsqu'ils sont définis sur « strict », si SPF ou DKIM échouent à l'authentification, l'ensemble de la vérification du protocole DMARC échoue.

Fonctionnement d'une politique DMARC



Lorsqu'un expéditeur a implémenté le protocole DMARC, le service de messagerie vérifie si l'email passe l'authentification SPF et DKIM. Ensuite, il applique la stratégie répertoriée dans l'enregistrement DNS et filtre l'email en conséquence. Enfin, un rapport est envoyé à l'expéditeur avec des informations sur le trafic de messagerie envoyé au nom du domaine et sur la façon dont il a été traité.

Rapports DMARC

Les rapports du protocole DMARC fournissent des informations stratégiques sur la façon dont les emails circulent dans l'écosystème des emails, ainsi que sur la fréquence à laquelle les mauvais acteurs essaient de contrefaire vos emails et d'usurper l'identité de votre marque. Comme vous l'avez peut-être remarqué, il existe deux types de rapports DMARC : agrégés et détaillé.

Les rapports DMARC agrégés sont envoyés quotidiennement, sauf indication contraire. Cela inclut :

- tous les domaines qui envoient des emails en utilisant votre domaine dans le champ « De »
- Les adresses IP d'envoi pour chaque domaine du rapport
- Les résultats de l'authentification SPF et DKIM
- Les emails mis en quarantaine (si votre politique est `p=quarantine`)
- Les emails bloqués (si vous avez utilisé `p=reject`)
- Les informations sur le trafic quotidien global des emails

> ***Remarque :*** *vous souhaiterez probablement configurer une adresse email dédiée pour recevoir vos rapports DMARC. En effet, des emails sont envoyés quotidiennement par chaque fournisseur d'accès à Internet qui reçoit des messages avec votre domaine dans le champ « De ». Cela peut représenter beaucoup d'emails pour certains expéditeurs.*

Les rapports DMARC détaillés sont envoyés chaque fois qu'un email échoue à l'authentification DMARC car SPF et/ou DKIM ne sont pas alignés. Également connus sous le nom de rapports d'échec , ils sont très utiles lorsque vous enquêtez sur des cas d'usurpation d'identité et que vous avez besoin de détails supplémentaires sur des messages spécifiques. Par exemple, les rapports DMARC détaillés incluront l'objet d'email des messages ayant échoué, les champs « `À` » et « `De` », ainsi que des informations sur les pièces jointes et les URL de ces emails.

Si votre équipe supervise la sécurité des emails, les rapports DMARC sont comme des briefings réguliers qui vous aident à détecter et à résoudre les problèmes avant qu'ils ne deviennent hors de contrôle.

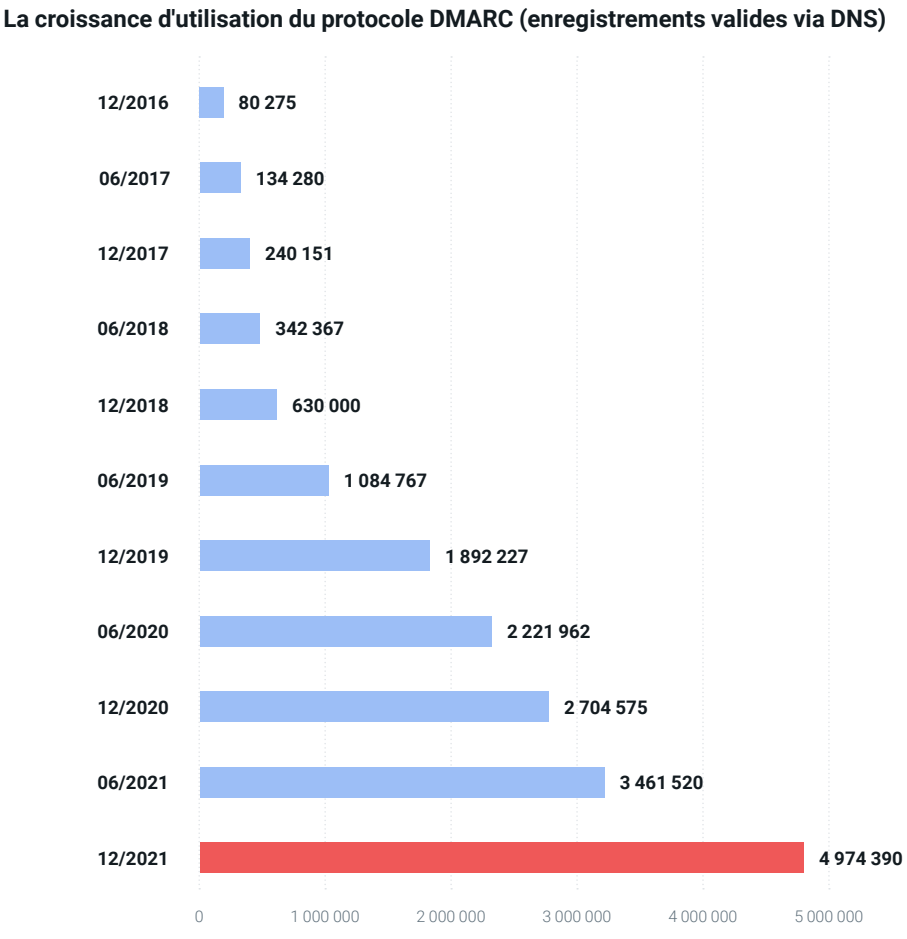
Si votre équipe supervise la sécurité des emails, les rapports DMARC sont comme des briefings réguliers qui vous aident à détecter et à résoudre les problèmes avant qu'ils ne deviennent hors de contrôle.

« Quand nous avons configuré pour la première fois des politiques DMARC pour Mailgun, c'était vraiment intéressant d'obtenir ces rapports et de voir tout le trafic. Nous avons commencé à remarquer toutes les personnes et structures utilisant Mailgun.com comme domaine d'envoi. Une grande partie de ce trafic était en fait le nôtre, mais nous ne le savions tout simplement pas. Par exemple, notre équipe marketing pourrait essayer un nouveau service et les protocoles ne seraient pas alignés. Mais, au moins, avec les rapports du protocole DMARC, nous savons ce qui se passe. »

Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

Quelle est la meilleure politique DMARC ?

De plus en plus d'expéditeurs s'intéressent à la valeur du protocole DMARC. Les chiffres récents de DMARC.org indiquent que l'adoption du protocole a bondi de 84 % en 2021, avec près de 5 millions d'enregistrements uniques à la fin de l'année.



DMARC.org affirme également que **près des deux tiers de ces enregistrements (65,6 %) ont des politiques détendues définies sur `p=none`**. Cela peut être dû au fait que certains expéditeurs veulent uniquement voir leurs rapports DMARC, et qu'ils hésitent à appliquer une politique stricte qui rejette ou met en quarantaine les emails échoués. Une politique p=none vous donnera les avantages de la déclaration. Cependant, elle ne servira à rien pour arrêter les attaques par hameçonnage et l'usurpation de marque.

Selon Kate Nowrouzi, Mailgun encourage ses utilisateurs à appliquer des politiques DMARC plus strictes. Bien qu'il soit parfaitement acceptable de commencer avec une politique détendue, à un moment donné, les expéditeurs doivent passer à l'étape suivante pour améliorer la sécurité de leurs emails.

La balise `pct=` dans votre enregistrement DMARC vous permet de **spécifier un pourcentage d'emails auxquels votre politique doit être appliquée**. Cela signifie que vous pouvez évaluer l'impact qu'une politique `p=quarantine` ou `p=reject` peut avoir sur la délivrabilité des emails sans que DMARC n'affecte l'ensemble de vos emails sortants. Vous pouvez ensuite résoudre tout problème en utilisant les rapports DMARC et augmenter progressivement le pourcentage auquel la politique est appliquée.

Kate estime que le but ultime du protocole DMARC est de mettre en œuvre une politique qui aide réellement les services de messagerie à vérifier les expéditeurs légitimes. De plus, elle protège les destinataires contre ceux qui tentent de se faire passer pour votre entreprise. Mais d'abord, les expéditeurs doivent surmonter leur peur de mettre en place le protocole DMARC.

« Beaucoup de marques traditionnelles reconnaissables considèrent encore le protocole DMARC comme nouveau, ce qui conduit à quelques inquiétudes de leur part. Elles craignent, par exemple, que si la politique est définie sur p=reject, leurs emails seront bloqués parce que DMARC n'est pas configuré correctement. Je vois beaucoup de marques se vanter d'avoir mis en œuvre le protocole DMARC. Mais, si leur politique est définie sur p=none, cela revient à ne rien faire.

Kate Nowrouzi, VP de la délivrabilité et du développement de produit chez Mailgun

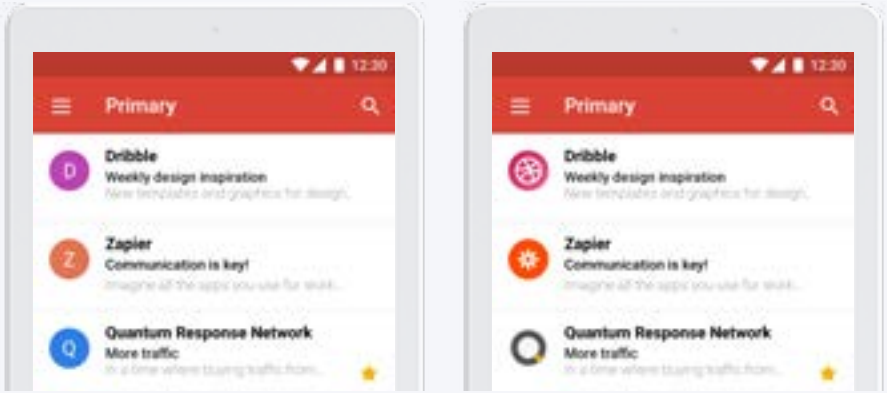
4. BIMI

Une autre raison pour laquelle certains expéditeurs hésitent à appliquer une politique DMARC est le manque d'avantages probants en leur faveur. Il est facile de supposer que seuls les emails légitimes sont bloqués ou envoyés au spam, car vos enregistrements d'authentification par email ne sont pas parfaitement configurés.

Afin d'encourager une meilleure adoption de la politique DMARC, le secteur de l'emailing a introduit le Brand Indicators for Message Identification (BIMI). Le résultat de la mise en œuvre de BIMI est un logo de marque qui apparaît dans la boîte de réception et au niveau du message. Mais, pour être « prêt pour le BIMI », vous devez avoir recours au protocole DMARC avec une politique définie pour rejeter ou mettre en quarantaine.

Voici un exemple de ce à quoi ressemblent ces logos avec BIMI :

Avant BIMI **Après BIMI**



Lorsqu'un service de messagerie reçoit un email de votre marque, il utilise d'abord l'enregistrement DMARC pour rechercher l'authentification SPF et DKIM. S'il réussit cette authentification DMARC, le service de messagerie peut rechercher un enregistrement DNS du BIMI, où est stocké un fichier image SVG du logo de la marque.

Les logos BIMI intéressent les marketeurs et tous ceux qui se soucient de l'image de marque. Cependant, ce sont les équipes techniques qui doivent mettre en place les enregistrements BIMI. La première étape consiste à s'assurer que tous les autres protocoles d'authentification des emails sont correctement configurés, y compris une politique DMARC appliquée.

Pour cette raison, vous pourriez considérer BIMI comme une sorte de récompense pour les expéditeurs qui prennent au sérieux l'authentification des emails. Jonathan Torres, de Mailgun, affirme que le secteur de l'emailing est « à la pointe » avec BIMI comme motivation pour la mise en œuvre de DMARC.

Gmail a commencé à prendre en charge la norme en 2021, ce qui la rend encore plus attrayante. Et Apple prévoit d'introduire le support de BIMI pour Apple Mail lorsque les prochaines versions de ses systèmes d'exploitation seront disponibles. (Ventura devrait arriver en octobre 2022).

Toutefois, Jonathan estime que l'on peut envisager que les services de messagerie passent de l'idée de récompenser les expéditeurs avec l'authentification DMARC, à celle d'en faire une exigence pour le placement en boîte de réception.

> *« À un moment donné, les services de messagerie peuvent décider de hiérarchiser les emails provenant d'expéditeurs dont les stratégies DMARC sont définies pour être rejetées ou mises en quarantaine, car ce sont celles qu'ils peuvent vérifier et auxquelles ils peuvent faire confiance. Pour l'instant, personne n'a franchit ce cap, mais il est possible de demander aux expéditeurs de définir une politique DMARC sur autre chose que p=none. C'est peut-être ce qu'il faut pour qu'il soit adopté. »*
>
> Jonathan Torres, Responsable des chargés de compte chez Mailgun

Authentification et réputation des emails

Avouons-le ! Si les logos en boîtes de réception sont sympathiques, ils ne sont guère plus qu'une symbole de fierté pour les directeurs marketing et les marketeurs par email. Vous devriez faire attention à l'authentification des emails pour d'autres raisons plus importantes : **la réputation d'expéditeur et la réputation de marque**.

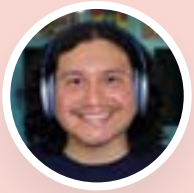
La réputation d'expéditeur est comme un score de crédit pour les organisations qui envoient des emails. Il s'agit essentiellement d'une mesure de votre fiabilité et de la qualité de vos communications par email.

Les services de messagerie sont très attentifs et comptent ces points. Ils utilisent des pièges à spam pour identifier les expéditeurs qui acquièrent des contacts de manière suspicieuse. Ils savent à quelle fréquence les abonnés ouvrent et interagissent avec le contenu que vous envoyez. De plus, ils savent si les emails sont ignorés, supprimés ou marqués comme spam. C'est pourquoi, **plus votre réputation d'expéditeur est bonne, meilleure sera la délivrabilité de vos emails**.

Dans cette optique, Mailgun inclut des actions telles que les désabonnements et les plaintes pour spam dans sa PUA. De plus, notre plateforme comprend des outils et des services de surveillance de la réputation d'expéditeur. Nous voulons que des expéditeurs dignes de confiance utilisent notre plateforme, et nous voulons aider les utilisateurs à améliorer leur réputation d'expéditeur.

L'utilisation ou le manque d'authentification des emails affectera également la réputation d'expéditeur et la délivrabilité. Si vous ne vous souciez pas de l'authentification, les services de messageries seront moins susceptibles de vous considérer comme un expéditeur digne de confiance. C'est l'une des raisons pour lesquelles Mailgun exige les authentifications SPF et DKIM, et nous recommandons fortement la mise en œuvre du protocole DMARC.

Les équipes techniques peuvent croire que **la réputation de marque** n'est pas de leur responsabilité, créant une déconnexion entre mise en place de protocoles (ou absence de mise en place) et usurpation de marque. Toutefois, si votre rôle touche de quelque manière que ce soit à la cybersécurité, l'une des principales choses que vous protégez est la réputation de marque. Vous n'avez pas besoin d'être un marketeur pour vous soucier de la marque.



« Je pense que l'importance de protéger la marque d'un expéditeur devient un sujet plus important dans le monde de l'emailing en raison de la façon dont le secteur évolue. La marque englobe tout. Si les utilisateurs perdent confiance en votre entreprise parce qu'ils ne savent pas si les emails que vous semblez envoyer sont sûrs, cela peut nuire définitivement à votre réputation. »

Jonathan Torres, Responsable des chargés de compte chez Mailgun

PARTIE 6

Choisir les bons partenaires

La confiance est un facteur crucial en matière de sécurité. De fait, la confiance est cruciale dans le cadre de toutes sortes de relations et de partenariats. Tout comme les services de messagerie ont besoin de moyens pour identifier les expéditeurs de confiance, vous devez également identifier des fournisseurs d'emailing de confiance.

Les experts en sécurité et en conformité des emails de Mailgun offrent leur point de vue sur ce qu'il faut rechercher chez un partenaire SaaS qui suit les bonnes pratiques.

Audits et certifications

L'une des façons les plus évidentes d'évaluer un partenaire potentiel est d'examiner les normes suivies et les certifications obtenues. Il se trouve que Dan Ross, Responsable de la gouvernance, du risque et de la conformité senior chez Mailgun, collaborait à la tenue d'audits majeurs au moment de la rédaction de ce guide.

Dan a un bon aperçu de ce que sont ces audits et certifications, ainsi que de ce qu'ils signifient pour vous en tant qu'expéditeur d'email.

Audits SOC 2 Type I et II

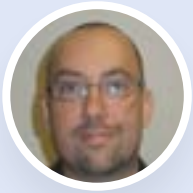
Un rapport SOC 2 vous garantira de la sécurité, de la disponibilité, de l'intégrité du traitement, de la confidentialité et des contrôles de confidentialité d'une organisation. Il est basé sur la conformité aux Trust Services Criteria (TSC, ou critères de confiance aux services) de l'American Institute of Certified Public Accountants (AICPA).

- **L'audit SOC 2 Type I évalue** la conception des processus de sécurité et examine si des contrôles de sécurité sont en place à un moment précis.
- **L'audit SOC 2 Type II évalue** le fonctionnement de ces contrôles de sécurité tout en observant les opérations sur une période de six à douze mois.

Par exemple, lorsque les auditeurs ont rédigé le rapport SOC 2 Type II sur Mailgun, ils ont évalué des éléments tels que la formation et la sensibilisation des employés à la cybersécurité. Les auditeurs ont pris 25 noms et ont vérifié si ces employés avaient suivi une formation et terminé le test.

Les auditeurs ont également examiné 25 changements de code sur la plateforme Mailgun pour voir si chacun de ces changements suivait les bonnes pratiques, notamment si Mailgun avait effectué des vérifications d'assurance qualité, et si le nouveau code avait été examiné pour détecter les failles de sécurité.

Un autre aspect de la norme SOC 2 Type II est la possibilité d'ajouter des contrôles HIPAA à l'audit. C'est ce que fait Mailgun. Nous savons qu'il est relativement rare de trouver un fournisseur de services email doté d'un rapport SOC 2 Type II. Cependant, selon Dan, ce rapport est ce dont vous avez vraiment besoin si vous souhaitez trouver des partenaires qui respectent les lois relatives à la protection de la vie privée. Son équipe est d'ailleurs assaillie de questions par les auditeurs lors de l'élaboration du rapport complet.



« Le SOC 2 Type II vérifie si les contrôles de sécurité fonctionnent efficacement. Lorsque Mailgun doit passer un audit SOC 2 Type II, cela signifie des journées de travail de 12 heures pendant quelques semaines. Ça peut être assez intense ! »

Dan Ross, Responsable de la gouvernance, du risque et de la conformité senior chez Mailgun

Certifications ISO 27001 et 27701

Les normes internationales aident les consommateurs et les clients B2B à évaluer la sécurité, la qualité et, dans ce cas, la sécurité des produits et services. ISO 27001 et ISO 27701 sont des normes internationales qui évaluent la sécurité des données et l'accès à ces données.

Si un partenaire potentiel dispose d'une **certification ISO 27001**, cela montre que son équipe a établi, mis en œuvre, maintient et améliore continuellement un système de gestion de la sécurité de l'information. La norme certifie qu'un partenaire a les bons processus et politiques en place, et avec une amélioration constante de ces processus d'année en année. Dans un partenariat SaaS, cela signifie que la plateforme est toujours plus sécurisée pour les clients et les utilisateurs.

Selon Dan, cela inclut des facteurs tels qu'un budget et une équipe de sécurité dédiés, qui continuent de croître chaque année plutôt que d'être réduits.

Une **certification ISO 27701** va plus loin que la norme ISO 27001 en couvrant les domaines des contrôles d'accès aux données sur la vie privée dans un système de gestion des informations confidentielles. Cette norme a été introduite en 2019 pour aider à évaluer la conformité d'une organisation à des lois telles que le RGPD et la CCPA. Elle établit une correspondance avec ces réglementations et d'autres réglementations sur la vie privée.

Bien que ces deux certifications ISO ne garantissent pas la conformité totale d'un partenaire potentiel, il est fort probable que l'organisation fasse tout son possible pour protéger les données client. Et trouver un partenaire d'emailing conforme est très important, car cela est directement lié à la conformité de votre propre organisation.

« Il n'y a pas de certification RGPD spécifique, parce que c'est une loi. Aussi, vous ne pouvez pas être certifié pour le RGPD, parce que vous devez de fait respecter la loi. Toutefois, la façon dont nous prouvons que nous respectons bien cette loi est d'avoir des certifications comme ISO 27701, que nous pouvons montrer à nos clients, pour prouver que nous faisons réellement ce que nous disons faire. »

Dan Ross, Responsable de la gouvernance, du risque et de la conformité senior chez Mailgun

Autres certifications et politiques de sécurité

Au-delà des principaux audits et normes de sécurité, vous devez poser d'autres questions à vos partenaires potentiels. Dan dit que cela peut inclure des éléments tels que la façon dont ils gèrent l'accès à vos données, la façon dont ils réagissent aux violations de cybersécurité, ainsi que les sauvegardes de données, la redondance géographique et la reprise après sinistre.

Vous pouvez également avoir des questions sur la sécurité des utilisateurs, notamment sur l'authentification unique et l'authentification multifacteurs. Vous pouvez rencontrer des problèmes spécifiques avec la certification PCI, avoir des questions sur la sécurité à l'intérieur des bureaux physiques, ou peut-être voulez-vous examiner un diagramme de réseau. **Un partenaire fiable répondra à toutes vos questions de sécurité et vous fournira toute la documentation dont vous avez besoin.**

En savoir plus sur la sécurité Mailgun.

Chez Mailgun, nous mettons à disposition un portail de sécurité complet contenant toutes sortes de documents que nos clients et prospects peuvent nous demander. Page en anglais.

Protection des produits

Steve Proud est directeur de l'ingénierie de sécurité chez Mailgun, ce qui signifie qu'il est chargé de protéger notre plateforme et de la garder sûre pour l'ensemble des expéditeurs. Selon Steve, les contrôles que nous avons abordés dans la section précédente (ISO 27701 et SOC 2 Type II) sont des facteurs importants, quel que soit le type de partenaire technologique que vous évaluez. Tout simplement parce que les cybercriminels ne s'arrêtent jamais.

« Les pirates attaquent en permanence les applications exposées à Internet. Qu'il s'agisse d'une plateforme d'envoi d'emails ou d'un réseau social, les organisations devraient s'appuyer sur des partenaires qui ont mis en place un programme de sécurité robuste. Cela permet de s'assurer qu'il existe une gouvernance et une structure dans la manière dont la sécurité est mise en œuvre, avec des personnes, processus et technologies dédiés. »

Steve Proud, Directeur de l'ingénierie de sécurité chez Mailgun

Avant de signer un contrat avec un partenaire qui fournit des solutions d'emailing, demandez des détails sur la manière dont son équipe protège son application contre les menaces de cybersécurité. L'équipe de sécurité de Mailgun applique une stratégie en trois volets pour protéger notre plateforme.

Approche « triple menace » de la sécurité des produits

1. **Tests de sécurité internes :** le partenaire potentiel dispose-t-il d'experts en sécurité internes qui testent les mises à jour de produits avant le déploiement ?
2. **Audit externe :** le partenaire potentiel utilise-t-il un service de test de cybersécurité tiers qui va au-delà des audits et des rapports standard ?
3. **Programmes de chasse aux bugs :** des spécialistes en sécurité ou « white hats » recherchent-ils des failles de sécurité inconnues dans la plateforme du partenaire potentiel ?

Dans ce guide, vous avez déjà fait la connaissance de certaines des personnes impliquées dans la sécurité des produits Mailgun. Parmi elles, Dan Ross affirme que s'enquérir de la « gestion du changement » est une partie importante de l'évaluation d'un partenaire technologique potentiel. **Les équipes produit et sécurité tentent-elles de tester de nouveaux codes pour détecter les vulnérabilités avant que les produits ne soient mis en ligne ?** Chez Mailgun, c'est toujours le cas.

Steve Proud affirme qu'une vigilance constante est nécessaire dans son travail. Tout aussi important, vos partenaires potentiels doivent avoir un plan pour remédier aux situations de sécurité de manière rapide et efficace.

« Les expéditeurs d'emails doivent attentivement examiner avec qui ils choisissent de s'associer lorsqu'ils évaluent les outils d'email marketing et de délivrabilité. Il ne s'agit pas de savoir si des vulnérabilités et des erreurs de configuration seront découvertes, mais simplement de savoir quand. Il est ainsi important de s'assurer que vos partenaires ont mis en place une méthodologie permettant une action rapide pour pousser un nouveau code sécurisé dans l'environnement, atténuant par conséquent l'effet de cette vulnérabilité. »

Steve Proud, Directeur de l'ingénierie de sécurité chez Mailgun

Sécurité et automatisation

Même avec l'équipe de sécurité la plus compétente et la plus brillante, il est difficile de rester au fait des tendances et de garder une longueur d'avance sur les mauvais acteurs. C'est pourquoi un partenaire efficace **automatise également les mesures de sécurité afin de pouvoir réagir rapidement et efficacement aux menaces**.

Dan Ross souligne que même si Mailgun dispose d'une équipe talentueuse, nous sommes tous humains et parfois les humains ratent des choses que les machines ne ratent pas. Ainsi, Dan et ses collègues ont travaillé pour « éliminer les hésitations sur la sécurité ». Cela peut sembler étrange, mais cela signifie simplement qu'il existe des outils automatisés en place pour alerter l'équipe de sécurité d'un problème presque instantanément.

Mailgun utilise des outils de sécurité internes qui nous permettent de surveiller les menaces sur le réseau et sur les points de terminaison en temps réel avec un personnel dédié enquêtant sur chaque alerte qui arrive. Par exemple, si l'ordinateur d'un employé distant présente un comportement étrange, l'équipe de sécurité le sait et y remédie avant que l'employé n'ait la moindre idée que quelque chose ne va pas.

Nick Schafer dit que ce type d'automatisation s'étend à ce qui se passe à l'intérieur de l'application Mailgun, car nous voulons nous assurer que les emails qui partent de notre plateforme sont sûrs, sécurisés et légitimes.

« Si nous devions uniquement compter sur des actions humaines manuelles, nous serions trop lents. Même si nous pensons agir rapidement, des milliers de messages potentiellement dangereux pourraient partir. Nous avons donc toutes sortes d'alertes et d'automatisations en place pour nous avertir et empêcher les actes malveillants de se produire. »

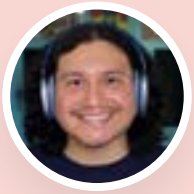
Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

Éducation des clients

Enfin, un bon partenaire en matière de sécurité des emails partagera ses connaissances et son expertise avec vous. Comme nous l'avons vu, les menaces de cybersécurité évoluent constamment et l'email est au cœur de l'action. Ainsi, un fournisseur d'emailing qui vous permet, à vous et à votre organisation, de rester informé est très précieux.

Chez Mailgun, nous mettons tout en œuvre pour nous assurer que nos clients ne font pas accidentellement quelque chose qui va à l'encontre de bonnes pratiques ou qui enfreint potentiellement la loi.

Jonathan Torres explique que nous agissons de manière proactive en veillant à ce que les problèmes de sécurité des emails soient abordés lors de l'intégration, ainsi qu'avec le chargé de compte client sur une base continue.



« Tous les prestataires ne s'intéressent pas aux sujets de la sécurité et de la conformité. Nous parlons à nos clients de ces questions, et nous sommes plus que prêts à les conseiller sur les bonnes pratiques, même lorsqu'un problème n'est pas directement lié à notre produit. »

Jonathan Torres, Responsable des chargés de compte chez Mailgun

PARTIE 7

Comment Mailgun peut vous aider

J'espère que nous vous avons convaincu qu'une plateforme sécurisée pour l'envoi des emails est d'une extrême importance. De la mise en place de mesures de sécurité des utilisateurs à l'arrêt des mauvais acteurs en passant par notre strict respect des normes de conformité, c'est le quotidien chez Mailgun by Sinch. Vous pouvez nous traiter de « gens bizarres » si vous voulez, mais nous aimons ce que nous faisons.

« Notre équipe est vraiment passionnée et expérimentée. Nous apprécions à juste titre le travail consistant à écarter les mauvais acteurs de la plateforme Mailgun. C'est amusant parce que c'est comme jouer aux gendarmes et aux voleurs. J'aime dire à mes enfants que nous sommes les gentils, ceux qui protègent la plateforme. »

Nick Schafer, Responsable de la délivrabilité et de la conformité chez Mailgun

À l'heure actuelle, vous devez également comprendre comment le fait d'avoir un partenaire qui place la sécurité et la conformité des emails en tête de ses priorités est un atout précieux pour toute organisation. Mailgun by Sinch se tient à votre disposition pour être ce partenaire.

Voici un récapitulatif de la façon dont nous travaillons en partenariat avec nos utilisateurs en matière de sécurité et de conformité des emails :

- **Centres de données sécurisés :** les services cloud de Mailgun reposent sur une infrastructure GCP de pointe. Tous les centres de données sont équipés de systèmes de surveillance 24h/24 et de contrôle d'accès biométrique.
- **Redondance, restauration des données et sauvegardes :** les centres de données sont équipés d'une redondance de niveau N+1 minimum pour l'alimentation, le réseau et l'infrastructure de refroidissement. Dans chaque région, le traitement des données se fait dans au moins trois zones de disponibilité distinctes. Des sauvegardes quotidiennes des données de compte avec restauration chiffrée incrémentielle/point-à-temps ont lieu sur toutes les bases de données primaires.
- **Chiffrement :** Mailgun utilise le chiffrement AES-256 pour protéger les données des clients et applique un chiffrement via TLS opportuniste pour protéger les emails envoyés depuis la plateforme en transit.
- **Conformité réglementaire :** Mailgun respecte et dépasse même la conformité au RGPD et à la CCPA pour protéger la confidentialité et l'intégrité des données des clients. Les droits et responsabilités en matière de conformité HIPAA sont définis dans un code de conduite pour les partenaires commerciaux. Stripe sert de processeur de paiement conforme à la norme PCI.
- **Rapports et certifications :** nous sommes certifiés ISO 27001 et 27701. Mailgun dispose également de rapports SOC 2 Type I et SOC 2 Type II, ce qui signifie que nos contrôles de sécurité sont mis en correspondance avec l'essentiel des réglementations, notamment RGPD, CCPA et HIPAA. De plus, tous les fournisseurs sont certifiés SOC Type II et ISO 27001.
- **Accès et sensibilisation des employés :** Mailgun limite l'accès aux données et aux systèmes en fonction des rôles. L'accès administratif aux systèmes et services Mailgun suit le principe du moindre privilège. Tous les employés doivent suivre une formation annuelle de sensibilisation aux cybermenaces, y compris une évaluation annuelle individuelle.
- **Sécurité des applications :** SAML et 2FA sont disponibles pour les connexions des clients. Un système de détection d'intrusion est en place pour détecter les accès non autorisés au compte. Des changements de code produit sont testés pour détecter les failles de sécurité, et un programme tiers de chasse aux bugs aide Mailgun à identifier les problèmes inconnus.
- **Protection de la plateforme :** Mailgun dispose d'outils, de systèmes automatisés et d'employés dédiés à la protection des mauvais acteurs de la plateforme et à la surveillance de notre réseau pour détecter toute activité suspecte. Une Politique d'Utilisation Acceptable (PUA) décrit les attentes des utilisateurs.
- **Authentification par email :** les authentifications SPF et DKIM sont requises lors de l'utilisation de la plateforme Mailgun. En outre, il est fortement recommandé d'appliquer une politique DMARC.

La sécurité, la conformité et l'authentification des emails sont des problèmes complexes. C'est pourquoi Mailgun met à votre disposition des chargés de compte pour vous aider lors de l'accompagnement initial et tout au long de votre contrat. Nous pouvons même vous aider avec des tâches telles que la mise en œuvre des protocoles SPF et DKIM. En outre, nous serons toujours heureux de pouvoir discuter de ces sujets avec vous et de vous donner des conseils utiles.

« Nous entretenons une relation très étroite avec nos clients, ce qui inclut une formation approfondie sur les bonnes pratiques pour toutes les questions liées à l'authentification et à la conformité des emails. Chaque année, nous rencontrons nos clients pour les éduquer et également donner des informations aux nouvelles personnes qui ont rejoint l'équipe. Nous faisons tout cela parce que nous nous soucions vraiment de leur réussite en tant qu'expéditeur et nous nous assurons qu'ils connaissent les risques. »

Kate Nowrouzi, VP de la délivrabilité et du développement de produit chez Mailgun

Vous avez encore des questions ? Renseignez-vous sur la sécurité et la conformité chez Mailgun by Sinch en visitant notre portail dédié à la sécurité . N'hésitez pas à nous contacter si vous avez des questions sur la sécurité, la conformité ou toute autre question. Nous sommes toujours heureux de vous expliquer comment Mailgun protège les emails.

PARTIE 8

Ressources

Explorez plus en détail la sécurité, la conformité et l'authentification des emails avec des informations détaillées, des articles du blog Mailgun, des études citées dans ce guide et d'autres ressources externes utiles.

Ressources sur Mailgun.com

- Le portail de sécurité Mailgun : consultez ou demandez l'accès à nos politiques, certifications et rapports. Cela inclut les rapports ISO 27001, ISO 27701 et SOC 2 Type I et II.
- Centre RGPD : découvrez comment Mailgun se conforme à la législation européenne sur la protection de la vie privée des consommateurs.
- Code de conduite pour les partenaires commerciaux pour conformité HIPAA : toutes les informations sur les droits et responsabilités concernant la protection des informations de santé privées.
- Accord sur le traitement des données : découvrez comment Mailgun gère les données client.
- Politique d'Utilisation Acceptable : consultez les lignes directrices requises pour les utilisateurs sur la plateforme Mailgun.

Contenu Mailgun utile

- Email security best practices: How to keep your email program safe (article en anglais)
- Email scams glossary (article en anglais)
- How does Mailgun keep your emails protected? (article en anglais)
- Vulnerability management: Working with the community to patch security threats (article en anglais)
- TLS basics: What is TLS connection control? (article en anglais)
- Understanding DKIM: How it works and why it's necessary (article en anglais)
- Implementing DMARC: A step-by-step guide (article en anglais)
- Which SMTP port should I use? (article en anglais)
- Phishing emails: How to identify them and protect yourself (article en anglais)
- Case Study: Optimizing data privacy for scalable and secure email (article en anglais)

Ressources sur l'authentification des emails

- Open-SPF.org : en savoir plus sur le projet Sender Policy Framework.
- DKIM.org : en savoir plus sur l'authentification DKIM.
- DMARC.org : en savoir plus sur l'authentification DMARC.
- BIMIGroup.org : en savoir plus sur le BIMI.
- The path to BIMI implementation : en savoir plus sur la configuration de BIMI à partir d'Email on Acid by Sinch (en anglais).

Sources externes de ce guide

- IBM : Combien coûte une violation de données en 2022 ?
- Cisco : Étude de 2021 sur les résultats de sécurité
- Mimecast : State of Email Security 2022
- Proofpoint : Rapport 2022 sur l'état du phishing
- GreatHorn : 2021 Email Security Benchmark Report

Plus de 100 000 entreprises dans le monde utilisent Mailgun by Sinch pour créer des expériences d'email marquantes pour leurs clients, grâce à une infrastructure de niveau mondial. Des marques comme Vodafone, la NHL, Etsy et McKinsey font confiance à Mailgun, ses technologies innovantes et son infrastructure fiable pour envoyer des milliards d'emails chaque année. D'abord conçu pour les équipes de développement, Mailgun simplifie l'envoi, la réception et le suivi d'emails pour les expéditeurs de toutes tailles.

Mailgun a été fondé en 2010 pour répondre à un manque de services d'envoi d'emails pensés pour les développeurs et basés sur les API. En 2021, Mailgun a rejoint **Sinch**, un des leaders dans le secteur des plateformes de communications en tant que service (CPaaS), et devient le service d'emailing à destination des développeurs pour leur clientèle internationale. Respectant le RGPD, HIPAA ainsi que SOC I et II, Mailgun veut vous offrir le meilleur service d'emailing possible avec les plus hauts niveaux de sécurité et de confidentialité des données.

Pour plus d'informations, visitez **mailgun.com/fr**.