Brand Identity Protection: Zustellbarkeit Ihrer Mailings optimieren

Smart Guide

Dieser Smart Guide zeigt Ihnen, wie Sie die Zustellbarkeit Ihrer Mailings verbessern. Durch die richtigen Einstellungen im Agenten *Brand Identity Protection* [1] schaffen Sie die optimalen Voraussetzungen dafür, dass Ihre E-Mails tatsächlich beim Empfänger ankommen und nicht als Spam klassifiziert werden. Sie stärken Ihre Marke und Ihre Reputation als Versender.

Hinweis: Bevor Sie sich an die Einrichtung des passenden Szenarios machen, müssen Sie eine Subdomain authentifizieren, die Sie künftig für Ihren E-Mail-Versand in Inxmail Professional nutzen. Hier wird das Vorgehen beschrieben.

Die drei möglichen Einrichtungsszenarien

Es gibt drei verschiedene Umsetzungsszenarien, wie Sie Ihren Agenten *Brand Identity Protection* einrichten können. Die Szenarien hängen davon ab, ob Sie nur Ihre eigene Absenderdomain per DKIM signieren oder zusätzlich noch das Domain Alignment wählen und schließlich, ob Sie Ihre Absenderdomain an Inxmail delegieren.

Szenario 1 | Authentifizierung & Domain Alignment (mit Domain Delegation)

1. In Inxmail Professional den Agenten *Brand Identity Protection* starten.
2. Option *Optimale Zustellbarkeit (Domain Alignment)* auswählen.
3. Kontrollkästchen *Domain an Inxmail delegieren (empfohlen)* aktivieren.
4. Im Eingabefeld *Ihre Domain* die (Sub-)Domain erfassen, die als Absender- und Bouncedomain verwendet werden soll.
5. Im Eingabefeld *E-Mail-Adresse für die Weiterleitung von Antworten* eine E-Mail-Adresse hinterlegen, an die alle Antworten auf die versendeten Mailings weitergeleitet werden sollen.

   Die (Sub-)Domain der Antwortadresse darf nicht mit der zuvor erfassten Absender- bzw. Bouncedomain übereinstimmen.

   Sie müssen bei Ihrem ISP bzw. E-Mail-Provider ein gleichnamiges Postfach einrichten. Dort gehen die Antworten auf Ihre Mailings ein. Nach dem Einrichten von Szenario 1 werden die Antworten auf Ihre Mailings nicht mehr im Agenten Posteingang & Bounces in Inxmail Professional angezeigt. Sie erhalten die Antworten stattdessen direkt im Posteingang Ihrer hinterlegten Weiterleitungsadresse. Die Antwort- und Weiterleitungsadressen können im laufenden Betrieb jederzeit geändert werden. Details siehe hier.
6. Auf *Domain authentifizieren* klicken.
7. Die Seite *Domainauthentifizierung* erscheint.
8. Die erforderlichen Schritte sind in Inxmail Professional abgeschlossen. Sie müssen nun die DNS-Einträge beim ISP hinterlegen. Detaillierte Infos finden Sie hier.

Upgrade-Info für Kunden mit bereits hinterlegten Versanddomains

Wenn Sie bereits eine frühere Version des Agenten eingesetzt haben, dann ist ein Upgrade auf Domain Delegation nicht möglich. Falls Sie Domain Delegation verwenden möchten, verwenden Sie eine neue Absenderdomain. Wenn Sie die bisherige Subdomain für die Domain Delegation an Inxmail verwenden möchten, wenden Sie sich bitte an den Support.

---

[1] WIE HILFT DER AGENT KONKRET?

- Sorgen Sie mit *SPF (Sender Policy Framework)* dafür, dass nur berechtigte Versender E-Mails von Ihrer Domain versenden können.
- Authentifizieren Sie mit *DKIM (DomainKeys Identified Mail)* Ihre Versender, und sorgen Sie dafür, dass der Inhalt Ihrer E-Mails nicht manipuliert werden kann.
- Steuern Sie per *DMARC (Domain-based Message Authentication, Reporting and Conformance)*, was mit Versendungen Ihrer Domain geschehen soll, bei denen die Authentifizierung mittels SPF oder DKIM fehlschlägt.
- Nutzen Sie *BIMI (Brand Message Identification)*, damit der Empfänger authentifizierte Versendungen Ihrer Domain auf den ersten Blick an Ihrem Firmenlogo erkennen kann.

[I] VORTEILE SZENARIO 1

Hier haben Sie langfristig den geringsten Pflegeaufwand. Sie hinterlegen einmalig die DNS-Einträge und delegieren damit die Domain an Inxmail. Bei künftigen Änderungen an den Domain-Einträgen übernimmt Inxmail die Anpassungen und Sie haben keine Aufwände.

- Alle Technologien zur E-Mail-Authentifizierung (SPF, DKIM, DMARC) werden berücksichtigt. Die Domain ist so vor fremdem Missbrauch durch Cyberkrimelle geschützt. Dazu muss der empfangende Mailserver/ Spam-filter DMARC interpretieren.
- Übereinstimmung von Absender- und Bouncedomain ("Domain Alignment") wird von vielen

Szenario 2 | Authentifizierung & Domain Alignment (ohne Domain Delegation)

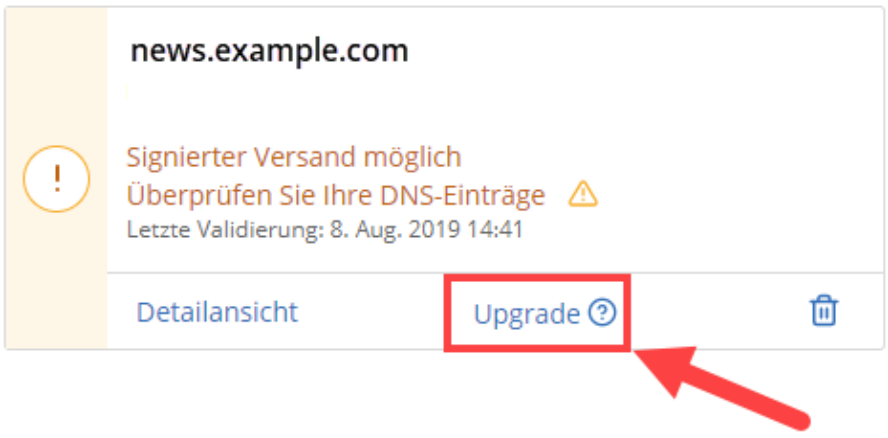
1. In Inxmail Professional den Agenten *Brand Identity Protection* starten.
2. Option *Optimale Zustellbarkeit (Domain Alignment)* auswählen.
3. Im Eingabefeld *Ihre Domain* die (Sub-)Domain erfassen, die als Absender- und Bouncedomain verwendet werden soll.
4. Im Eingabefeld *E-Mail-Adresse für die Weiterleitung von Antworten* eine E-Mail-Adresse hinterlegen, an die alle Antworten auf die versendeten Mailings weitergeleitet werden sollen.

   Die (Sub-)Domain der Antwortadresse darf nicht mit der zuvor erfassten Absender- bzw. Bouncedomain übereinstimmen.

   Sie müssen bei Ihrem ISP bzw. E-Mail-Provider ein gleichnamiges Postfach einrichten. Dort gehen die Antworten auf Ihre Mailings ein. Nach dem Einrichten von Szenario 2 werden die Antworten auf Ihre Mailings nicht mehr im Agenten Posteingang & Bounces in Inxmail Professional angezeigt. Sie erhalten die Antworten stattdessen direkt im Posteingang Ihrer hinterlegten Weiterleitungsadresse. Die Antwort- und Weiterleitungsadressen können im laufenden Betrieb jederzeit geändert werden. Details siehe hier.
5. Auf *Domain authentifizieren* klicken.
6. Die Seite *Domainauthentifizierung* erscheint.
7. Die erforderlichen Schritte sind in Inxmail Professional abgeschlossen. Sie müssen nun die DNS-Einträge beim ISP hinterlegen. Detaillierte Infos finden Sie hier.

Upgrade-Info für Kunden mit bereits hinterlegten Versanddomains

Wenn Sie bereits eine frühere Version des Agenten eingesetzt haben und keine Bouncedomain erfasst haben, können Sie Ihre Absenderdomain auf Domain Alignment upgraden. Falls diese Konstellation bei Ihnen gegeben ist, wird folgende Upgrade-Schaltfläche in der Domain-Übersicht angezeigt:



Ein Dialogfenster mit Anweisungen führt Sie durch die weitere Einrichtung.

Internet Service Providern (ISPs) als positives Merkmal bei der Einstufung von E-Mails bzgl. Spam bewertet.

- Mailing-Links zeigen auf dieselbe Domain (= "Full Domain Alignment").
- Durch das Authentifizieren Ihrer Absenderdomain entfällt die Anzeige der Inxmail-Absenderdomain.
- Die Domain Delegation erleichtert die Pflege Ihrer Domains. Sie brauchen nur einmalig so genannte NS-Einträge bei Ihrem ISP bzw. DNS zu hinterlegen. Alles Weitere, wie beispielsweise die Pflege der DKIM-Schlüssel, erledigt Inxmail für Sie.
- Sie können Ihr BIMI-Logo direkt über XPRO steuern, ohne dass Sie einen DNS-Eintrag bei Ihrem ISP vornehmen müssen.

[I] VORTEILE SZENARIO 2

Unterscheidet sich in der Art der DNS-Einträge von Szenario 1. Hier setzen Sie CNAME und TXT-Einträge ein. Somit sind Sie langfristig selbst verantwortlich für die Pflege und ggf. Aktualisierung Ihrer DNS-Einträge.

- Alle Technologien zur E-Mail-Authentifizierung (SPF, DKIM, DMARC) werden berücksichtigt. Die Domain ist so vor fremdem Missbrauch durch Cyberkrimelle geschützt. Dazu muss der empfangende Mailserver/ Spam-filter DMARC interpretieren.
- Übereinstimmung von Absender- und Bouncedomain ("Domain Alignment") wird von vielen Internet Service Providern (ISPs) als positives Merkmal bei der Einstufung von E-Mails bzgl. Spam bewertet.
- Mailing-Links zeigen auf dieselbe Domain (= "Full Domain Alignment").
- Durch das Authentifizieren Ihrer Absenderdomain entfällt die Anzeige der Inxmail-Absenderdomain.

Szenario 3 | Authentifizierung Ihrer Absenderdomain

Wichtig: In diesem Szenario müssen viele Einstellungen manuell vorgenommen werden. Diese Änderungen sollten nur von erfahrenen IT-/Mailserver-Administratoren durchgeführt werden. Bei falscher Einrichtung werden Reputationsprobleme riskiert, die Einfluss auf die eingesetzte Hauptdomain oder Subdomain haben.

Wie sollte ich nicht mit Szenario 3 arbeiten?

Wenn Sie mit Szenario 3 arbeiten, bedeutet dass, dass Sie Ihre E-Mails in Inxmail Professional über eine Hauptdomain versenden. Oder über eine Subdomain, die Sie außerhalb von Inxmail Professional anderweitig nutzen.

Das bedeutet, sie verwenden dieselbe Domain für verschiedene Versandquellen, z.B.: Newsletter, Transaktionsmails wie Bestellbestätigungen, Rechnungsbestätigungen und/oder Ihre alltäglichen Geschäftsmails.

Durch diese Vermischung kann es zu großen Reputationsproblemen kommen. Wenn z.B. aus Ihrem Newsletterversand Reputationsverluste entstehen, wirken sich diese Reputationsverluste auch auf ihre Alltags-E-Mails aus.

Differenziert man dagegen die Mailtypen voneinander, so baut jede Domain ihre eigene Reputation auf, und die Versandquellen stören sich gegenseitig nicht.

Wieso ist die Einrichtung von Szenario 3 so komplex und fehleranfällig?

Innerhalb einer Firma gibt es viele Systeme, die in Ihrem Namen E-Mails versenden. Das sind z.B. Job-Portale, Social Media-Dienste oder Akquise-Kanäle. Diese Kanäle existieren oft, ohne dass die IT-Abteilung in Ihrem Unternehmen überhaupt davon weiß. Man spricht auch von Schatten-IT. Nicht alle diese Dienste signieren Ihre E-Mails per DKIM – oder halten sich an die sonstigen technischen Zustellbarkeits-Standards.

Wenn Sie mit Szenario 3 arbeiten wollen, müssen Sie die DMARC-Policy Ihrer Hauptdomain auf "reject", mindestens aber auf "quarantine" setzen. Dazu müssen Sie sicherstellen, dass alle Systeme, die in Ihrem Namen E-Mails versenden, sich an Ihre Zustellbarkeits-Standards halten. In der Praxis bedeutet das: Sie müssen komplexe XML-Berichte generieren und auswerten, in denen Sie über IP-Adressen alle Programme und Dienste ermitteln, die in Ihrem Namen E-Mails versenden. Sie müssen mit fremden Dienstleistern kommunizieren und die Dienstleister dazu zwingen, Ihre E-Mails per DKIM zu signieren und sich an Ihre Zustellbarkeits-Standards zu halten. Dieser Prozess ist sehr aufwendig und kann je nach IT-Infrastruktur Jahre in Anspruch nehmen. Nutzen Sie daher Szenario 1 oder 2.

Falls Sie dennoch Szenario 3 einrichten wollen:

1. In Inxmail Professional den Agenten *Brand Identity Protection* starten.
2. Option *Verbesserte Zustellbarkeit (verschiedene Domains für Absenderdomain (From) und Bouncedomain (Return-Path) verwenden)* auswählen.
3. Im Eingabefeld *Absenderdomain (From)* die (Sub-)Domain erfassen, die als Absenderdomain verwendet werden soll.
4. Optional kann im Eingabefeld *Bouncedomain (Return-Path)* eine (Sub-)Domain erfasst werden, die als Bouncedomain verwendet wird. So wird vermieden, dass Inxmail-Absenderdomains wie inxserver.com oder inxserver.de im technischen E-Mail-Header zu sehen sind.
5. Auf *Domain authentifizieren* klicken.
6. Die Seite *Domainauthentifizierung* erscheint.
7. Die erforderlichen Schritte sind in Inxmail Professional abgeschlossen.
8. Nun müssen die DNS-Einträge beim ISP hinterlegt werden. Detaillierte Infos finden Sie hier.

[I] VORTEILE SZENARIO 3

Szenario 3 sollten Sie nur in absoluten Ausnahmefällen verwenden. Generell raten wir Ihnen davon ab. Bei falscher Einrichtung riskieren Sie Reputationsprobleme, die Einfluss auf Ihre eingesetzte Domain haben.

- Bei diesem Szenario ist gewährleistet, dass die Technologien SPF und DKIM zur E-Mail-Authentifizierung berücksichtigt werden. Je nachdem, wie die Domain außerhalb von Inxmail Professional per DMARC authentifiziert wurde, ist die DMARC-Authentifizierung unter bestimmten Umständen valide. Dies muss von einem erfahrenen IT-/ Mailserver-Administratoren geprüft werden. Bei korrekter Einrichtung ist die Domain vor fremdem Missbrauch durch Cyberkrimelle geschützt. Dazu muss der empfangende Mailserver/ Spam-filter DMARC interpretieren.
- Durch das Authentifizieren Ihrer Absenderdomain entfällt die Anzeige der Inxmail-Absenderdomain.
- Die Hauptdomain kann als Versanddomain genutzt werden.
- Die Versanddomain (Hauptdomain oder Subdomain) kann außerhalb von Inxmail Professional noch für andere Zwecke genutzt werden.