WHITE PAPER

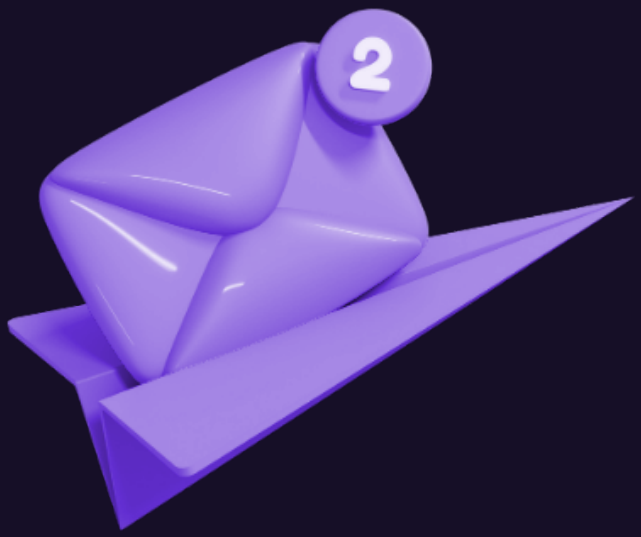
DKIM E-MAIL AUTHENTIFIZIERUNG

Alles, was Sie zur DKIM-PLICHT wissen müssen, um ihre E-Mails 2024 vor der Spam-Einstufung zu schützen.

INVICTUS
LEAD GENERATION

INHALTE DES WHITE PAPERS

01 DKIM-Pflicht 2024 3
02 Wer ist betroffen? 3
03 DKIM einfach erklärt 4
04 Welche Zusatzmaßnahmen sind zu beachten? 5
05 Chancen für Versender & Empfänger 5
06 Von welchen Vorteilen können Sie profitieren? 6
07 So gelingt die Implementierung 7
08 Ausblick auf zukünftige Entwicklungen 9
09 Die Takeaways im Überblick 10
About Invictus 11



01 DKIM-PFLICHT 2024

In unserer digitalisierten Welt ist der Schutz vor Spam, Phishing und Identitätsdiebstahl ein absolutes Muss. Und genau hier kommt **DKIM**, kurz für **„Domain Keys Identified Mail“**, ins Spiel.

Die Pflicht zu DKIM trat im Februar dieses Jahres in Kraft. Die E-Mail Authentifizierungsmethode wurde von Postfach-Anbietern wie Google, Yahoo und Co. **weltweit als verbindliche Voraussetzung für den sicheren Versand und Empfang von E-Mails eingeführt**.

02 WER IST BETROFFEN?

- Absender, die täglich mehr als **5000 E-Mails** an Gmail- oder Yahoo-Adressen versenden.
- Unternehmen und Einzelpersonen, die auf E-Mail-Kommunikation angewiesen sind, u.a. Plattformen für den elektronischen Handel, Newsletter und Abonnementdienste oder Marketing-Agenturen.

Um zu garantieren, dass Ihre E-Mails weiterhin zugestellt und nicht als Spam eingestuft werden, ist es notwendig, DKIM in Ihrem Account einzurichten!

TIPP

Auch bei einem Versand von weniger als 5000 E-Mails pro Tag lohnt es sich, DKIM einzurichten, um eine **erhöhte Zustellbarkeit** der E-Mails zu erreichen.

03 DKIM EINFACH ERKLÄRT

DKIM dient als digitales Siegel für E-Mails, das ihre **Authentizität und Unversehrtheit** gewährleistet

Wie funktioniert das?

DKIM basiert auf **asymmetrischer Verschlüsselung**, um sicherzustellen, dass eine E-Mail tatsächlich von dem angegebenen Absender stammt und ihr Inhalt während der Übertragung unverändert bleibt. Dies geschieht durch Hinzufügen einer **eindeutigen digitalen Signatur** (dem privaten Schlüssel) durch den sendenden Mailserver. Der Empfangsserver überprüft diese Signatur mithilfe des im **DNS** (Domain Name System) - **Eintrag** des Absenders hinterlegten öffentlichen Schlüssels.

Es handelt sich also um die Signierung von Mails mittels zwei miteinander korrespondierender digitaler Schlüssel, welche die Zustellbarkeit von Mailings verbessert. Der Empfangsserver überprüft hierbei, ob die jeweilige E-Mail zugestellt werden darf oder nicht.

- Der **erste Schlüssel** wird auf dem Empfangs-DNS-Server hinterlegt und veröffentlicht (Public Key).
- Der **zweite Schlüssel**L ist nur dem Versender bekannt (Private Key).

Der **erste öffentliche Teil des Schlüssels** wird als TXT-Datensatz in die Domain des DNS-Servers des Hosts gesetzt (Absenderadresse).

Der **zweite private Teil des Schlüssels** wird genutzt, um für jede E-Mail eine individuelle DKIM-Signatur zu generieren. Diese Signatur wird automatisch in den E-Mail-Header eingefügt.

Erkennt der Empfangsserver die Signatur im E-Mail-Header, sucht er den öffentlichen Teil des Schlüssels. Hierfür erfragt er beim DNS-Server den TXT-Datensatz.

Wenn beide Schlüssel passen, können die E-Mails zugestellt werden.

04 WELCHE ZUSATZ-MASSNAHMEN SIND ZU BEACHTEN?

Zusätzlich zur DKIM-Anforderung ist es für Versender entscheidend, sicherstellen, dass sie ausschließlich E-Mails an Personen versenden, die **explizit ihr Einverständnis** zum Empfang von Newslettern gegeben haben. Es ist ebenso wichtig, **einfache Möglichkeiten zur Abmeldung** von E-Mail-Listen anzubieten.

DKIM allein bietet zwar eine gewisse Sicherheit, möglicherweise aber keinen ausreichenden Schutz. Es empfiehlt sich daher, DKIM mit **SPF** (Sender Policy Framework) und **DMARC** (Domain-based Message Authentication, Reporting, and Conformance) zu kombinieren.

SPF ermöglicht die **Überprüfung des Absenders**, während DMARC Richtlinien für die **Behandlung von nicht authentifizierten E-Mails** festlegt. Die gemeinsame Anwendung von DKIM, SPF und DMARC bildet ein **robustes Sicherheitsnetz**, das die Integrität und Authentizität von E-Mails gewährleistet.

05 CHANCEN FÜR VERSENDER UND EMPFÄNGER

Durch die Implementierung von DKIM ergeben sich für VERSENDER die Chancen auf eine **verbesserte Zustellbarkeit** ihrer E-Mails sowie eine **gestärkte Absender-Reputation**.

EMPFÄNGER schützt DKIM vor **unerwünschten E-Mails**, **verbessert** deren **Qualität** und **reduziert Spam**.

06 VON WELCHEN VORTEILEN KÖNNEN SIE PROFITIEREN?

01 **SICHERHEIT**

- DKIM minimiert Phishing-Angriffe und E-Mail-Spoofing.

02 **INTEGRITÄT**

- Die Authentifizierungsmethode liefert die Gewährleistung, dass der Inhalt der E-Mails unverändert bleibt.

03 **REPUTATIONSGEWINN**

- Ihre authentifizierten E-Mails genießen eine verbesserte Zustellbarkeit.

04 **VERTRAUENSBILDUNG**

- Ihre Empfänger können sich darauf verlassen, dass die E-Mail tatsächlich von der angegebenen Domain stammt.

07 SO GELINGT DIE IMPLEMENTIERUNG

Die Integration von DKIM erfordert ein gründliches Verständnis der technischen Anforderungen sowie entsprechende Ressourcen. Um einen reibungslosen Ablauf zu gewährleisten, ist es entscheidend, bewährte Verfahren zu befolgen. Dies beinhaltet:

- die präzise **Generierung von Schlüsselpaaren**
- die korrekte **Integration in bestehende E-Mail-Infrastrukturen**
- regelmäßige **Überprüfungen der DKIM-Konfiguration**

Es empfiehlt sich außerdem, E-Mails von einer **privaten Domain** zu versenden, die beispielsweise für geschäftliche Zwecke oder die vorhandene Webseite genutzt wird, anstatt kostenloser E-Mail-Dienste wie Gmail oder Yahoo. In dieser privaten Domain sollte der DKIM-Eintrag eingerichtet werden.

Step by Step zum DKIM-Eintrag

01 SCHLÜSSELPAAR GENERIEREN

- Überprüfen Sie zunächst, ob Ihr E-Mail-Dienstanbieter bereits ein DKIM-Schlüsselpaar für Ihre Domain bereitgestellt hat. Falls ja, verwenden Sie diese Schlüssel.
- Falls nicht, können Sie ein Schlüsselpaar mithilfe von Open-Source-Tools wie OpenDKIM oder OpenSSL generieren. Beachten Sie dabei die Anweisungen des jeweiligen Tools.

02 DKIM-SELEKTOR WÄHLEN

- Entscheiden Sie sich für einen DKIM-Selektornamen, der Ihrem Schlüsselpaar zugeordnet werden soll. Dieser Name sollte eindeutig sein und in Ihrer Domain noch nicht verwendet werdent.
- BEISPIEL: „dkim“ oder ein spezifischer Name wie „sales_dkim“ je nach Verwendungszweck

03 DKIM-EINTRAG IM DNS ERSTELLEN

- Melden Sie sich bei Ihrem DNS-Provider an und navigieren Sie zum Bereich für die DNS-Einstellungen Ihrer Domain.
- Fügen Sie einen TXT-Eintrag hinzu, der den öffentlichen DKIM-Schlüssel enthält. Der Eintrag sollte den DKIM-Selektor und Ihre Domain enthalten.
- BEISPIEL: „dkim._domainkey.beispiel.de“

04 DKIM-EINTRAG TESTEN

- Senden Sie eine Test-E-Mail von Ihrem Server und überprüfen Sie, ob der DKIM-Signaturheader korrekt hinzugefügt wurde.
- Verwenden Sie DKIM-Testtools oder Dienste wie „DKIM Validator“, um die Gültigkeit Ihrer DKIM-Signatur zu überprüfen.

05 ÜBERPRÜFUNG UND WARTUNG

- Überwachen Sie regelmäßig die DKIM-Authentifizierung Ihrer E-Mails, um sicherzustellen, dass der DKIM-Eintrag ordnungsgemäß funktioniert.
- Aktualisieren Sie den DKIM-Eintrag bei Bedarf, z. B. wenn sich Schlüssel ändern oder neue DKIM-Selektoren erforderlich sind.

TIPP

Fallstudien erfolgreicher DKIM-Implementierungen bieten praxisnahe Einblicke und können als Leitfaden für eine erfolgreiche Umsetzung dienen.

Viele private Domain-Anbieter geben bei der Einrichtung eine Hilfestellung, indem sie Informationen in Form einer Schritt-für-Schritt-Anleitung zur Verfügung stellen.

08 AUSBLICK AUF ZUKÜNFTIGE ENTWICKLUNGEN

Die zukünftige Entwicklung der E-Mail-Sicherheitsstandards lässt auf einen **kontinuierlichen Anstieg der Anforderungen** schließen. Faktoren wie die Pandemie und der damit etablierte Trend zum Arbeitsmodell Remote Work haben die E-Mail-Kommunikation verstärkt, was das Risiko von E-Mail-basierten Angriffen erhöht hat.

In diesem Zusammenhang könnten sich neue Möglichkeiten und Standards in der Authentifizierungstechnologie abzeichnen, um eine **noch sicherere digitale Kommunikation** zu gewährleisten.

Im Bereich der E-Mail-Sicherheit zeichnen sich folgende Trends und Vorhersagen ab:

01 EINSATZ VON KI-TECHNOLOGIEN

- Künstliche Intelligenz wird zunehmend genutzt, um E-Mail-Bedrohungen effektiver zu erkennen und zu bekämpfen. Durch die Fähigkeit, aus Mustern zu lernen, verbessern diese Technologien kontinuierlich ihre Erkennungsrate.

02 VERSCHÄRFUNG DER COMPLIANCE-ANFORDERUNGEN

- Angesichts steigender Cyberbedrohungen werden strengere Datenschutzvorschriften erwartet. Unternehmen werden zunehmend dazu gedrängt, ihre E-Mail-Sicherheitsstrategien anzupassen, um den neuen Anforderungen gerecht zu werden.

03 IMPLEMENTIERUNG VON SECURE EMAIL GATEWAYS (SEGS)

- Umfassender Schutz gegen eine Vielzahl von E-Mail-Bedrohungen wird durch die verstärkte Implementierung von Secure Email Gateways angestrebt.

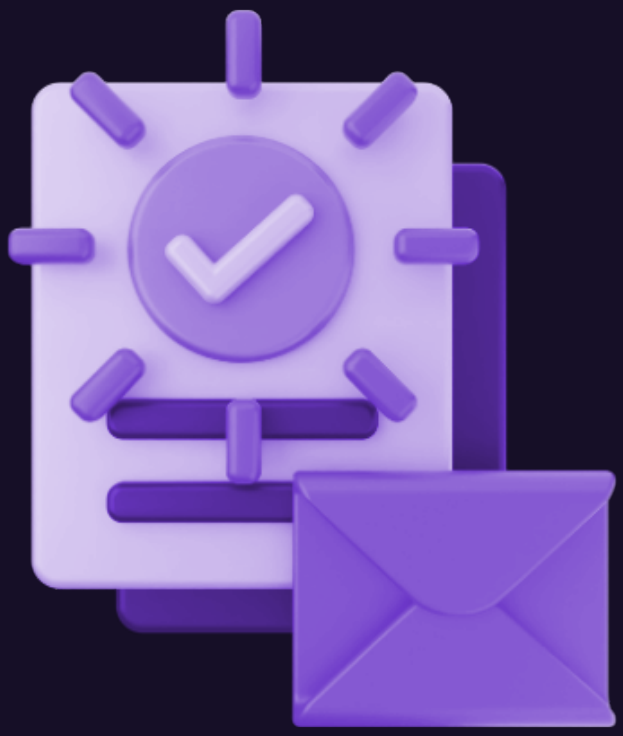
04 ENTWICKLUNG FORTGESCHRITTENER PHISHING-ABWEHRTECHNIKEN

- Angesichts der anhaltenden Bedrohung durch Phishing werden zukünftige Abwehrstrategien auf fortgeschrittene Erkennungs- und Neutralisierungs-technologien sowie auf verstärkte Nutzer-Schulungen im Bereich Sicherheitsbewusstsein setzen.

09 DIE TAKEAWAYS IM ÜBERBLICK

Im **Februar 2024** trat die Pflicht zu DKIM für Newsletter-Versender diverser Postfach-Anbieter in Kraft. DKIM spielt eine entscheidende Rolle bei der Gewährleistung von **Authentizität, Integrität und Vertrauen** von übermittelten, digitalen Inhalten.

Obwohl die Implementierung technische Fachkenntnisse erfordert, bietet sie nicht nur eine **Grundvoraussetzung für den E-Mail-Versand**, sondern auch eine Chance, das Vertrauen in digitale Kommunikation zu stärken und den Schutz vor unerwünschten E-Mails zu verbessern.



ABOUT INVICTUS

Als Agentur unterstützen wir Unternehmen auf dem Weg zum Erfolg und sind mit unserer langjährigen Erfahrung Spezialisten für Kommunikation im Bereich **B2B Lead Generation**.

Sie wollen zielorientiertes Marketing?
Starten sie ihr Projekt mit uns!

Invictus Lead Generation

invictus.lead.gen

invictus.lead.gen

invictus.leadgen

www.invictus-lead-generation.de
info@invictus-lead-generation.de
030 311 6989 150

INVICTUS
LEAD GENERATION