E-Mail-Authentifizierung im Finanzsektor:

Schutz vor Cyber-Bedrohungen und Sicherstellung der Zustellbarkeit in den Posteingang

Herausgeber:
eco – Verband der Internetwirtschaft e. V.
Certified Senders Alliance

Autorin:
Sandra Schubert
Customer Success Manager, Certified Senders Alliance

CSA
Certified Senders Alliance

E-Mail-Authentifizierung im Finanzsektor

Schutz vor Cyber-Bedrohungen und Sicherstellung der Zustellbarkeit in den Posteingang

In der heutigen schnelllebigen und digitalisierten Welt ist die Sicherheit von Kommunikation von zentraler Bedeutung. E-Mails sind für viele Unternehmen ein zentrales Kommunikationsmittel, um Kunden zu informieren, mit ihnen in Kontakt zu bleiben und geschäftliche Abläufe zu steuern – auch im Finanzsektor.

Denn gerade im Finanzwesen, wie z.B. bei Banken und Versicherungen, birgt der Versand kommerzieller E-Mails erhebliche Risiken – sowohl für das Unternehmen als auch für ihre Kunden. Die besonders sensiblen Kundendaten machen diese Institutionen zu sehr attraktiven Zielen für raffinierte E-Mail-Phishing-Angriffe von Cyberkriminellen.

Eine umfangreiche und verlässliche E-Mail-Authentifizierung ist daher unerlässlich, um einer Vielzahl von Cyber-Bedrohungen, die über E-Mails erfolgen, vorzubeugen. Sie schützt nicht nur sensible Daten, sondern stellt auch die zuverlässige Zustellung von E-Mails sicher – ein wesentlicher Faktor für den Aufbau und Erhalt von Kundenvertrauen sowie für den Schutz des guten Rufs eines seriösen Unternehmens im Finanzsektor.

Diese Richtlinie beleuchtet die entscheidende Rolle, die Authentifizierung für die Sicherheit der E-Mail-Kommunikation spielt, und zeigt die Risiken auf, die bei unzureichender Umsetzung entstehen können. Zudem werden effektive Risikomanagement-Lösungen vorgestellt, um die Sicherheit zu erhöhen und eine zuverlässige E-Mail-Zustellung zu gewährleisten.

Viel Spaß beim Lesen.

1. E-Mail-Authentifizierung: Definition und Notwendigkeit

E-Mail-Authentifizierung umfasst Protokolle und Techniken, die sicherstellen, dass E-Mails tatsächlich vom angegebenen Absender stammen und während der Übertragung nicht manipuliert wurden. Im Finanzsektor, wo täglich mit sehr sensiblen Kundendaten gearbeitet wird, ist dies von besonderer Bedeutung, um Betrug wie Spoofing und Phishing effektiv vorzubeugen.

Auch im E-Mail-Marketing für Finanzprodukte ist die E-Mail-Authentifizierung zentrale Bestandteil und grundlegende Voraussetzung für eine gesicherte Zustellung in den Posteingang der Empfänger. Für Postfachbetreiber wie 1&1, Google, Yahoo oder Microsoft ist sie der wesentliche Faktor für Spam-Filter- und Blockierungsstrategien, um ihre Nutzer und die Infrastruktur zu schützen. Darüber hinaus sind die authentifizierten Bestandteile einer E-Mail - IP und Domain - entscheidend für den Aufbau einer Sender-Reputation. Wird eine Versand-Domain für Spam oder Phishing missbraucht, besteht große Gefahr, dass E-Mails dieser Domain gefiltert oder blockiert werden, was eine reibungslose Kommunikation mit Kunden erheblich beeinträchtigen kann.

Seit Anfang 2024 verschärfen Google, Yahoo und bald auch Microsoft ihre E-Mail-Authentifizierungsanforderungen, um die Sicherheit ihrer Nutzer zu erhöhen. Die neuen, strengeren Standards für SPF, DKIM und DMARC werden dazu führen, dass E-Mails, die den Anforderungen nicht entsprechen, im Spam-Ordner landen oder geblockt werden. Weitere Informationen zu diesen Änderungen und deren Auswirkungen auf die E-Mail-Zustellung finden Sie hier: *https://certified-senders.org/de/blog/die-einhaltung-der-csa-kriterien-zahlt-sich-aus-yahoo-und-gmail-verschaerfen-ihre-regeln*

2. Der Finanzsektor als bevorzugtes Ziel für Cyberattacken – die Gründe

Hoher Wert von Finanzinformationen

Finanzdaten wie Kontoinformationen, Transaktionshistorien und persönliche Identifikationsdaten sind äußerst sensibel und bei Cyberkriminellen sehr stark begehrt. Diese Daten bieten Angreifern schnellen Zugang zu Geld und Finanzinstitute oder Versicherungen sind daher besonders attraktive Ziele.

Vertrauen der Kunden in Finanzinstitutionen

Banken und Versicherungen genießen ein hohes Maß an Vertrauen und einen renommierten Ruf, da Kunden auf deren Sicherheit und Verlässlichkeit bei der Verwaltung ihrer sensiblen Daten zählen. Cyberkriminelle nutzen dieses Vertrauen aus, indem sie sich als diese Institutionen ausgeben und gefälschte E-Mails versenden, um Kunden zu täuschen.

Großer Kundenstamm und hohes E-Mail-Volumen

Die große Anzahl an Kunden im Finanzsektor erhöht die Wahrscheinlichkeit, dass Phishing-E-Mails relativ schnell und einfach viele potenzielle Opfer erreichen. Das hohe tägliche E-Mail-Aufkommen bietet Cyberkriminellen zahlreiche Gelegenheiten für Phishing-Angriffe. Mit zunehmender Raffinesse und täuschend echten E-Mails wird es für einen Empfänger ohne technisches Verständnis schwer, legitime E-Mails von betrügerischen zu unterscheiden.

3. Risiken bei fehlender Authentifizierung

Nachlässigkeit bei E-Mail-Authentifizierung kann schwerwiegende Folgen haben:

Verlust des Kundenvertrauens und Rufschädigung

Phishing-Angriffe können das Vertrauen der Kunden erheblich untergraben und zu einem massiven Imageverlust führen. Negative Berichterstattung über Sicherheitslücken oder Datenschutzverletzungen in den Medien oder sozialen Netzwerken verstärkt den Eindruck, dass das Unternehmen seine Kunden nicht ausreichend schützt oder nicht über die nötigen Sicherheitskompetenzen verfügt. Dies kann zu Kundenabwanderung und dem Verlust potenzieller Neukunden führen.

Zustellprobleme

Kunden erwarten von digitalisierten Unternehmen, vor allem in der Finanzbranche, dass wichtige E-Mails wie Kontoaktualisierungen, Vertrags- und Police Änderungen oder Konto-Warnungen und Benachrichtigungen zuverlässig in ihrem Posteingang landen. Fehlende oder fehlerhafte Authentifizierung kann jedoch dazu führen, dass diese E-Mails im Spam-Ordner enden oder sogar komplett von Postfachbetreiber zum Schutz ihrer Nutzer abgelehnt werden. Dies macht eine kontinuierliche Kommunikation mit Kunden unmöglich.

Verpasste Geschäftschancen

Wenn E-Mails im Spam-Ordner landen oder nicht zugestellt werden, verlieren Unternehmen potenzielle Umsatzchancen – diese Emails werden mit sehr hoher Wahrscheinlichkeit nicht gesehen.

Finanzielle und rechtliche Konsequenzen

Durch potenzielle Verstöße gegen Datenschutzgesetzte, Probleme bei der E-Mail-Zustellung oder möglicher Kundenentschädigungen bei Verlusten durch betrügerische E-Mails, operativen Beeinträchtigungen und erhöhten Rechtskosten durch rechtliche Maßnahmen von Kunden können sowohl erhebliche finanzielle also auch rechtliche Konsequenzen entstehen.

Gefährdung der Unternehmenssicherheit

Schwachstellen in der E-Mail-Authentifizierung können die gesamte IT-Architektur eines Unternehmens gefährden. Betrüger können gestohlene Informationen nutzen, um tiefer in die Unternehmenssysteme einzudringen und weiteren Schaden anzurichten, was die Integrität und Sicherheit des Unternehmens insgesamt bedroht.

4. Methoden der E-Mail-Authentifizierung

Es existieren verschiedene Mechanismen zur E-Mail-Authentifizierung, die alle vom Versender implementiert werden sollten:

SPF (Sender Policy Framework)

SPF ist ein Protokoll, das Domaininhabern ermöglicht, festzulegen, welche IP-Adressen berechtigt sind, E-Mails im Namen ihrer Domain zu versenden. Postfachbetreiber können dadurch prüfen, ob eine eingehende E-Mail von einer autorisierten Quelle stammt. E-Mails von Servern, die nicht im SPF-Eintrag aufgeführt sind, bestehen die SPF-Prüfung nicht, was die Wahrscheinlichkeit erhöht, dass sie im Spam-Ordner landen, da sie vom Postfachbetreiber als "nicht ganz vertrauenswürdig" eingestuft wurden.

DKIM (DomainKeys Identified Mail)

Eine DKIM-Signatur verwendet einen privaten und öffentlichen Schlüssel, um die Integrität einer E-Mail zu verifizieren. Diese Signaturen ermöglichen es dem Empfänger, zu überprüfen, ob die E-Mail während der Übertragung manipuliert wurde. Wurde die Nachricht unterwegs verändert, kann der Empfänger die Signatur mit Hilfe des öffentlichen Schlüssels nicht verifizieren und die E-Mail wird sehr

wahrscheinlich vom Postfachbetreiber oder Spamfilter als Spam markiert und in den Spam-Ordner geliefert.

DMARC (Domain-based Message Authentication, Reporting, and Conformance):

DMARC kombiniert die Protokolle SPF und DKIM und legt durch eine Richtlinie fest, wie der empfangende E-Mail-Server mit nicht- oder unkorrekt authentifizierten E-Mails einer Domain umgehen soll. Es gibt drei DMARC-Richtlinien, die Versender konfigurieren können:

"**None**": Es werden keine spezifischen Maßnahmen gegen E-Mails ergriffen, wenn die E-Mail-Authentifizierung fehlschlägt. Es obliegt dem Postfachbetreiber wie er das Risiko einschätzt und die E-Mails werden höchstwahrscheinlich wie gewohnt zugestellt. Es wird jedoch ein Bericht für den Versender erstellt, um verdächtige Aktivitäten für die Domain und potenzielle Bedrohungen durch eventuelle Konfigurierungslücken sichtbar zu machen.

"**Quarantine**": E-Mails, welche die Authentifizierungsprüfung nicht bestehen, sollen in den Spam-Ordner ausgefiltert werden. Dies reduziert das Risiko von Phishing, indem potenziell gefährliche E-Mails vom Posteingang ferngehalten werden und somit ein direkter Zugriff des Empfängers wesentlich eingeschränkt wird. Es bleibt ein Restrisiko, dass Empfänger die E-Mails im Spam-Ordner lesen und ggf. die schadhaften Links darin dennoch klicken.

"**Reject**": Bei Anwendung dieser Richtlinie werden E-Mails, welche die Authentifizierungsprüfung nicht bestehen, bereits vom empfangenden Server zurückgewiesen (Bounce-Nachricht) und gelangen somit nicht weiter in die Infrastruktur des Postfachbetreibers. Dies verringert das Risiko von potenziellen Phishing-Angriffen, da die E-Mails den Empfänger auf keinen Fall erreichen.
SPF, DKIM und DMARC sind essenziell für den Schutz vor Phishing-Angriffen, da sie die unbefugte Verwendung von Domains verhindern und somit den Zugang auf vertrauliche Informationen unterbinden oder zumindest erheblich erschweren.

5. Herausforderungen bei der Implementierung und Lösungsansätze

Mangelndes Bewusstsein

Im Banken- und Versicherungssektor fehlt oft das nötige Verständnis für die Wichtigkeit einer robusten E-Mail-Authentifizierung auch für die ausgehende E-Mail-

Kommunikation. Viele Entscheidungsträger sind sich der Risiken von Zustellbarkeitsproblemen und auch von Domainmissbrauch für E-Mail-Spoofing und Phishing sowie deren potenziell hohen finanziellen Folgen nicht bewusst.

Mangelndes Fachwissen und technische Komplexität

Viele Mitarbeiter im IT-Bereich verfügen oftmals nicht über das erforderliche Fachwissen und Verständnis für die Komplexität, um E-Mail-Authentifizierung effektiv umzusetzen und typische Fehler zu vermeiden.

Veraltete Systeme und komplexe IT-Infrastruktur

Altsysteme und eine zunehmend komplexe IT-Infrastruktur, bedingt durch Fusionen oder Weiterentwicklungen, erschweren es Unternehmen, moderne Sicherheitsmaßnahmen zu implementieren und E-Mail-Authentifizierungsmechanismen nahtlos ohne erheblichen Ressourcenaufwand zu integrieren.

Übermäßiges Vertrauen in traditionelle Sicherheitsmaßnahmen:

Firewalls und Verschlüsselung sind weiterhin wichtig sind, wehren allerdings nur die eingehenden Bedrohungen für das jeweilige Unternehmen selbst ab. Für den Schutz vor Missbrauch von den Domains der Unternehmen gegenüber den Endkunden schützt eine Firewall aber nicht. E-Mail-Sicherheit hat zwei Perspektiven und es sind zusätzliche Maßnahmen erforderlich, um einen umfassenderen Schutz in beide Richtungen zu gewährleisten.

Kooperationsmangel – Management von Drittanbietern:

Ineffiziente interne und externe Zusammenarbeit führt oft zu Interoperabilitätsproblemen und einem mangelnden ganzheitlichen Ansatz. Unterschiedliche Abteilungen wie IT, Marketing und Compliance setzen oft unterschiedliche Prioritäten oder kommunizieren nicht ausreichend miteinander.

6. Schritte zur Implementierung einer sicheren E-Mail-Authentifizierung:

Analyse der aktuellen E-Mail-Kommunikation und Systeme

Um effektiv absichern zu können muss zunächst ermittelt werden, wo welche E-Mails von welchen Systemen unter Nutzung welcher IPs und/oder Domains Verwendung finden. Eine gründliche Bestandaufnahme der bestehenden Sicherheitsmaßnahmen

für alle E-Mail-Server und Versand-Domains ist Grundlage. Dies ermöglicht erst die Bewertung und die effektive Planung der weiteren Maßnahmen.

Technische Implementierung und Herausforderungen

Für eine zuverlässige und sichere Authentifizierung ist die Implementierung von SPF-, DKIM- und DMARC-Einträgen in der DNS-aller Domains notwendig. Auch Domains, welche nicht für den E-Mail-Versand verwendet werden, müssen gegen den missbräuchlichen Versand von E-Mail abgesichert werden. Alle Einträge und Protokolle müssen vor Anwendung im E-Mail-Verkehr umfassend getestet werden und die E-Mail-Server sowie die Domains sollten kontinuierlich überwacht werden.

SPF:
Es muss festgelegt werden, welche Versand-Server (IP-Adressen) berechtigt sind, E-Mails im Namen einer Domain zu versenden. Ein entsprechender TXT-Eintrag im DNS listet diese autorisierten IP-Adressen auf.

Beispiel SPF Eintrag der Domain „firma.de“:

```
text "v=spf1 ip4:213.165.64.0/23 -all"
```

Dieser Eintrag erlaubt den Versand von E-Mails von allen Servern im Netzwerkbereich 213.165.64.0/23 im Namen der Domain „firma.de“.

Häufiger Fehler:
SPF-Einträge werden oft nicht regelmäßig aktualisiert, was dazu führt, dass neue Versandserver nicht korrekt authentifiziert werden und legitime E-Mails, die über diese neuen Mailserver versandt wurden, im Spam-Ordner landen oder vom Postfachbetreiber abgelehnt werden.

SPF-Einträge beinhalten oft sehr viele IP-Adressen oder ganze Netzbereiche, was eine potenzielle Sicherheitslücke darstellt.

Domains, welche nicht für den Versand von E-Mails vorgesehen sind, werden oft nicht gegen Missbrauch geschützt, sollten aber ebenfalls mit einem SPF-Eintrag versehen werden. *"v=spf1 -all"*

DKIM:
Für DKIM ist die Generierung eines öffentlichen und privaten Schlüsselpaares für die Domain notwendig, wobei der öffentliche Schlüssel im DNS-Eintrag hinterlegt wird. Der private Schlüssel wird zur Signierung jeder ausgehenden E-Mail verwendet. Der Empfangsserver vergleicht dann den privaten mit dem öffentlichen Schlüssel.

Beispiel:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=12dkim1;
d=emails.firma.com; h=From:To:Subject:Date:MIME-Version;
i=firma@emails.firma.com;
bh=LIHvJ+o6R8cJxg5BzQc0JiypsEb3u891LpwUMSgE6nY=;
b=dGh93t7sUgSqoyoBASeIdmnQuSM5iWU81wye+4tzVRpsQ5Tz4r7IvVVpnrfi+39+X
xx27bAvx6cXyPgp0GdRCLMCUi+72yAGEqQ5us755HLTgTbUjnTopHtv0r09TE1n9wKX
2iXAj8IBKJiC6oQg2GMRn3PgkyjrcR67S6UJmlHKcbjdxuv7JgBZr3PTOPWmDq9BrUU
eiAYrqO5mhGoT51GBi+btPkXYugkIQhL3/XhScf57InbxpMJsNAP1eXJG2viS989UAe
N+uvSv+rwR8EA2bhMhjdCqxcrNyo0t2MW3GJi1NuyAN6+ukQ9vgbYUfq3jJu6APkewj
hHFhQthbQ==
```

Häufiger Fehler:

- Unzureichende Domain-Konfiguration, wie falsche Schlüssellängen, fehlerhafte DNS-Einträge und veraltete DKIM-Schlüssel, kann es Cyberkriminellen ermöglichen, die Domain zu missbrauchen.
- Fehlende Rotation von Schlüsseln.
- Unzureichender Signaturumfang, welcher sich nur auf einzelne Header der E-Mail bezieht.
- Die Nutzung der Längenparameters (l=) beschränkt die Signatur auf einen bestimmten Teil der E-Mail und lässt Platz für Manipulation im nicht signierten Teil der E-Mail.
- Für die DKIM-Signatur wird eine zu allgemeine Domain verwendet, welche oft nicht mit der sichtbaren Versanddomain übereinstimmt oder Bezug hat.

DMARC:

Ein DMARC-Eintrag wird erstellt, um durch die Richtlinie festzulegen, wie E-Mails, die die SPF- und DKIM-Prüfungen nicht bestehen, vom Empfangsserver behandelt werden sollen. (E-Mails ablehnen „reject" Richtlinie, in den Spam Ordner liefern „quarantine" Richtlinie oder gar nichts tun „none" Richtlinie)

Beispiel:

```
v=DMARC1; p=quarantine; rua=mailto:beispiel@firma.de
```

Dieser Eintrag verwendet die Richtlinie „quarantine", und gemäß der Instruktion werden nicht-authentifizierte E-Mails in den Spam-Ordner geliefert. Der "rua"-Tag hier gibt an, wohin die täglichen verfügbaren DMARC-Berichte gesendet werden sollen.

Herausforderung:
Ein häufiger Fehler bei der DMARC-Konfiguration ist das voreilige Festlegen einer zu strengen Richtlinie ohne ausreichende Überwachung und Analyse der bestehenden Versandinfrastruktur. Dies kann dazu führen, dass legitime E-Mails blockiert oder gefiltert werden.

Eine DMARC Implementierung muss immer mit einem Monitoring der DMARC-Berichte eingehen. Nur so werden Konfigurationsfehler oder Missbrauchsfälle aufgedeckt und können behoben oder Maßnahmen zum Schutz ergriffen werden.

Die Implementierung von SPF, DKIM und DMARC ist oft komplex und erfordert fundierte Fachkenntnisse über DNS und E-Mail-Sicherheit. Es wird empfohlen, bei Bedarf Expertenhilfe in Anspruch zu nehmen.

7. Zugang zu Real-Daten & Monitoring – eine Notwendigkeit für Sicherheit und Risikomanagement

Der Zugriff auf Performance-Daten von Versand-Servern, Domains und E-Mail-Kampagnen, um Cyber-Bedrohungen und Zustellbarkeitsprobleme frühzeitig zu erkennen und zu beheben ist unerlässlich, aber auch eine der größten Herausforderungen. Ohne diese Real-Daten können Cyber-Bedrohungen und Probleme möglicherweise nicht rechtzeitig erkannt und angemessen adressiert werden, sie werden aber von den Postfachbetreibern auch nicht einfach so zur Verfügung gestellt und können sich in Art und Weise und von Betreiber zu Betreiber unterscheiden.

Nutzung von DMARC-Berichten

Zum Zweck eines einheitlichen Reporting ist der DMARC-Standard entwickelt und eingeführt worden. Es dient als effektives Monitoring-Instrument der Überwachung der Authentifizierungsprotokolle SPF und DKIM. DMARC-Berichte unterstützen Versender dabei, schnell unerlaubten Domain-Missbrauch und Sicherheitsverletzungen zu erkennen und zu reagieren. Regelmäßige Auswertung dieser Berichte ist entscheidend. Diese Berichte folgen einem einheitlichen Standard und werden von immer mehr Mailbox Providern versendet. Um diese Reports auszuwerten, benötigt man allerdings entsprechend Auswertungstools, um die technischen Berichte für einen Endanwender lesbar zu machen.

E-Mail-Performance-Monitoring

Die kontinuierliche Überwachung der E-Mail-Kampagnen ist entscheidend für die Sicherheit und Effizienz eines Unternehmens, um:

- Eine zuverlässige Zustellung von E-Mails in den Posteingang sicherzustellen.
- Eine positive Domain-Reputation aufzubauen und zu erhalten.
- Risiken zu erkennen und proaktiv zu managen, indem Schwachstellen frühzeitig identifiziert werden.

8. Die CSA als verlässlicher Partner für mehr E-Mail-Sicherheit und Qualität

Die Certified Senders Alliance (CSA) bietet zertifizierten Versendern umfassende Unterstützung durch einheitliche Standards, welche mit den Postfachbetreibern gemeinsam entwickelt und immer wieder aktualisiert werden und ein leistungsstarkes Überwachungstool, um die Einhaltung dieser Standards zu überwachen. Dieses Tool basiert auf realen Daten von Postfach- und Sicherheitsanbietern, die wertvolle Einblicke in die E-Mail-Authentifizierung und E-Mail-Performance gewähren.

Die korrekte Anwendung von Authentifizierungsprotokollen ist ein wesentlicher Bestandteil der CSA-Kriterien aber vor allem Grundlage für die E-Mail-Sicherheit eines Unternehmens.

Der CSA-Certification Monitor bietet:

- E-Mail-Performance-Daten: Zur frühzeitigen Erkennung und Behebung von Reputations- und Zustellungsproblemen, z. B. durch hohe Spamklickraten und Spamtraphits.
- Authentifizierungsdaten: Identifizierung von Authentifizierungslücken, wie DKIM-Fehlern.

Risikominderung durch gezielte Hinweise von CSA-Experten:
Zertifizierte Versender erhalten wertvolles individuelles Feedback zu nicht konformen E-Mails von Zustellbarkeits- und Rechtsexperten. Diese Rückmeldungen helfen, Mängel zu erkennen und potenzielle Schäden zu vermeiden, einschließlich:

- Benachrichtigungen über Nutzerbeschwerden
- Weiterleitung ernsthafter Beschwerden durch Postfachbetreiber
- Hinweise zu rechtlichen Anforderungen und technischen Unregelmäßigkeiten
- Expertenrat und Unterstützung bei der Fehlerbehebung

Die CSA-Gemeinschaft und Fortbildungsmöglichkeiten
Die CSA bringt E-Mail-Versender mit Postfachbetreibern zusammen, fördert den Austausch und bietet wertvolle Interaktionen innerhalb der Branche. Zertifizierte Versender profitieren von Fachwissen und Erfahrungsaustausch.

- CSA-Netzwerk: Austausch innerhalb der E-Mail-Community.
- Exklusive Weiterbildungsangebote: Rabatte für Webinare, Schulungen und Workshops, maßgeschneidert auf die Bedürfnisse der Mitglieder.
- CSA-Zertifikat: als anerkanntes Qualitätsmerkmal des Versenders in der Branche.

9. Fazit – E-Mail-Authentifizierung ist ein MUSS

Eine zuverlässige E-Mail-Authentifizierung ist heute unverzichtbar, um das Vertrauen der Kunden zu bewahren, den Ruf des Unternehmens zu schützen und finanzielle Risiken zu minimieren. Insbesondere in der Finanz- und Versicherungsbranche ist es unerlässlich, dem hohen Vertrauensvorschuss der Kunden gerecht zu werden und deren Sicherheit fortwährend aktiv zu gewährleisten. Unternehmen müssen sich kontinuierlich an die dynamische Bedrohungslage anpassen und die Verbesserung ihrer Sicherheitsmaßnahmen priorisieren und auch um sicherzustellen, dass ihre Emails auch im Posteingang ihrer Kunden landen.

E-Mail-Authentifizierung ist daher keine Option, sondern ein absolutes Muss.

Die Certified Senders Alliance bietet zertifizierten Versendern hierbei kontinuierliche und wertvolle Unterstützung.

10. Häufig gestellte Fragen

Was bedeutet E-Mail-Zustellbarkeit?

E-Mail-Zustellbarkeit bezieht sich darauf, dass eine E-Mail das Posteingangsfach des Empfängers erreicht, ohne im Spam-Ordner zu landen oder vom empfangenden Mailserver abgelehnt zu werden.

Was sind Betreiber von Postfächern?

Postfachbetreiber sind Unternehmen, die E-Mail-Dienste bereitstellen und den Empfang, Versand und die Speicherung von E-Mails ermöglichen. Sie bieten Nutzern E-Mail-Adressen an und kümmern sich um die Sicherheit der E-Mail-Kommunikation durch komplexe Filtertechnologien zur Verhinderung von Phishing und Spam.

Welche bekannten Postfachbetreiber gibt es?

Zu den beliebtesten Anbietern in Deutschland gehören:

- 1&1 (Web.de, GMX.de)
- Deutsche Telekom (T-Online)
- Google (gmail.com)
- Microsoft (outlook.com, hotmail.de,…..)
- Yahoo

Welche Schlüsselindikatoren (KPIs) für Performance sind im Bereich E-Mail-Marketing von Bedeutung?

- **Zustellungsrate**: Anteil der erfolgreich zugestellten E-Mails.
- **Zustellbarkeitsrate**: Anteil der E-Mails, die das Posteingangsfach erreichen.
- **Bounce-Rate**: Prozentsatz der abgelehnten E-Mails aufgrund von Zustellungsfehlern.
- **Beschwerderate**: Anteil der von Empfängern als Spam markierten E-Mails.
- **Öffnungsrate**: Prozentsatz der geöffneten E-Mails.
- **Klickrate**: Prozentsatz der Empfänger, die auf einen Link in der E-Mail geklickt haben.
- **Abmelderate**: Anteil der Empfänger, die auf den Abmeldelink in der geöffneten E-Mail geklickt haben.
- **Conversionsrate**: Anteil der Empfänger, die eine gewünschte Aktion durchgeführt haben.

Diese Performanceindikatoren sind entscheidend, um die E-Mail Performance zu überwachen und zu optimieren, die Reputation des Absenders zu schützen und das Engagement der Empfänger zu steigern.

Was ist DNS und wie wird es genutzt?

Das Domain Name System (DNS) ist das Telefonbuch des Internets. Es wird verwendet, um von Menschen lesbare Domainnamen wie z. B. "marke.com" in computerlesbare, numerische IP-Adressen wie "192.0.2.1" umzuwandeln, die von Computern verwendet werden können, um sich gegenseitig im Internet zu finden und zu kommunizieren.

Domaininhaber können über das Konto ihres Domain-Registrars auf das DNS ihrer Domain zugreifen und gegebenenfalls DNS-Einträge verfassen. Diese DNS-Einträge ermöglichen es, den Datenverkehr für eine Domain präzise zu steuern und zu konfigurieren, indem sie festlegen, wie und wohin Anfragen für diese Domain gerichtet werden.

Jeder DNS-Eintrag hat eine bestimmte Funktion und wird verwendet, um unterschiedliche Aspekte der Domainnamenverwaltung zu steuern wie z.B.:

- Verknüpfung einer IP-Adresse mit einem Domain-Namen (A-Eintrag)
- Definition der Zuständigkeit von Servern zugelassen für den Empfang von Emails (MX-Eintrag)
- Verifizierung von Domain-Inhaberschaften und zusätzliche Infos zur Domain (TXT-Eintrag)
- Info über den genutzten Verwaltungsdienst der Domain (NS-Eintrag)

Was ist der Unterschied zwischen Spoofing und Phishing?

Spoofing: Ist eine Technik von Cyberkriminellen, die sich als seriöser oder bekannten Absender einer E-Mail ausgeben möchten z.B. durch Domain-Missbrauch. Ziel ist es, Vertrauen zu gewinnen oder Identitäten zu verschleiern, um den Empfänger zu einer Interaktion zu bewegen.

Phishing: Bezieht sich auf den Versuch, den Empfänger durch gefälschte E-Mails dazu zu bringen, persönliche oder vertrauliche Informationen preiszugeben. Das Hauptziel ist der Diebstahl von sensiblen Daten durch Täuschung.

> **Beispiel**:
> Eine gefälschte E-Mail von einer Bank fordert den Empfänger auf, auf einen Link zu klicken, der zu einer gefälschten Login-Seite führt. Dort wird der Empfänger dann aufgefordert, seine Anmeldeinformationen einzugeben, die dann vom Angreifer gestohlen werden.

Was ist ein Bounce?

Ein Bounce im Zusammenhang mit Reputations- oder Authentifizierungsproblemen tritt auf, wenn eine E-Mail aufgrund von Zweifeln an der Seriosität des Absenders oder mangelnder Authentifizierung nicht zugestellt wird. In solchen Fällen verweigert der empfangende Mailserver die Annahme der E-Mail, weil er die Identität des Absenders nicht verifizieren kann oder der Absender eine schlechte Reputation aufweist, etwa durch viele Nutzerbeschwerden oder Spam- oder Phishing-Verdacht. Der Versender erhält einen sogenannten "Non-Delivery Report" (NDR) oder eine "Bounce Message" vom Mailserver des Empfängers, der den Grund der Ablehnung mit Hilfe eines Bounce-Codes angibt. Eine erhöhte Bounce-Rate kann die Reputation des Versenders noch weiter verschlechtern und zu noch schwerwiegenderen Zustellungsproblemen führen.

Über die Certified Senders Alliance

Die Certified Senders Alliance (CSA) ist ein Service des eco – Verband der Internetwirtschaft e.V. und ist in Kooperation mit dem Deutschen Dialogmarketing Verband (DDV) im Jahr 2004 entstanden. Die CSA bildet eine neutrale Schnittstelle zwischen Mailboxprovidern und Versendern kommerzieller E-Mails. Ziel der CSA ist es, die Qualität kommerzieller E-Mails (z.B. Newsletter, Rechnungen, Auftragsbestätigungen etc.) zu erhöhen. Um dieses Ziel zu erreichen, erstellt sie rechtliche und technische Qualitätsstandards. Die Qualitätsstandards ergeben sich aus geltendem Recht und technischen Anforderungen der Mailboxprovider. Sie werden entsprechend den aktuellen Gesetzgrundlagen und Marktanforderungen regelmäßig aktualisiert.

Über die Autorin

Sandra ist eine erfahrene E-Mail-Marketing- und Kundenservice-Expertin. Als E-Mail-Marketing-Beraterin bei Validity/Return Path in Frankreich arbeitete sie mit Marken zusammen, um Zustellbarkeitsprobleme zu lösen und E-Mail-Strategien zu verfeinern. Davor unterstützte sie Kunden in verschiedenen Funktionen in einem internationalen Umfeld, darunter Customer Success und Channel Support bei Return Path und Export Management bei Carl Zeiss. Seit August 2023 ist sie zurück im Kundensupport in ihrem Heimatland Deutschland, wo sie als Customer Success Managerin bei der CSA ihr Fachwissen und ihre Leidenschaft, anderen zu helfen, kombiniert.

Sandra Schubert
Customer Success Managerin
Certified Senders Alliance

eco – Verband der Internetwirtschaft e.V.
Certified Senders Alliance

Lichtstrasse 43h
50825 Köln

Tel: +49 221 – 70 00 48-0
E-Mail: info@certified-senders.org
https://certified-senders.org/

Vereinsregister Köln
Vereinsregisternummer: 14478
Umsatzsteueridentifikationsnummer: DE 182676944