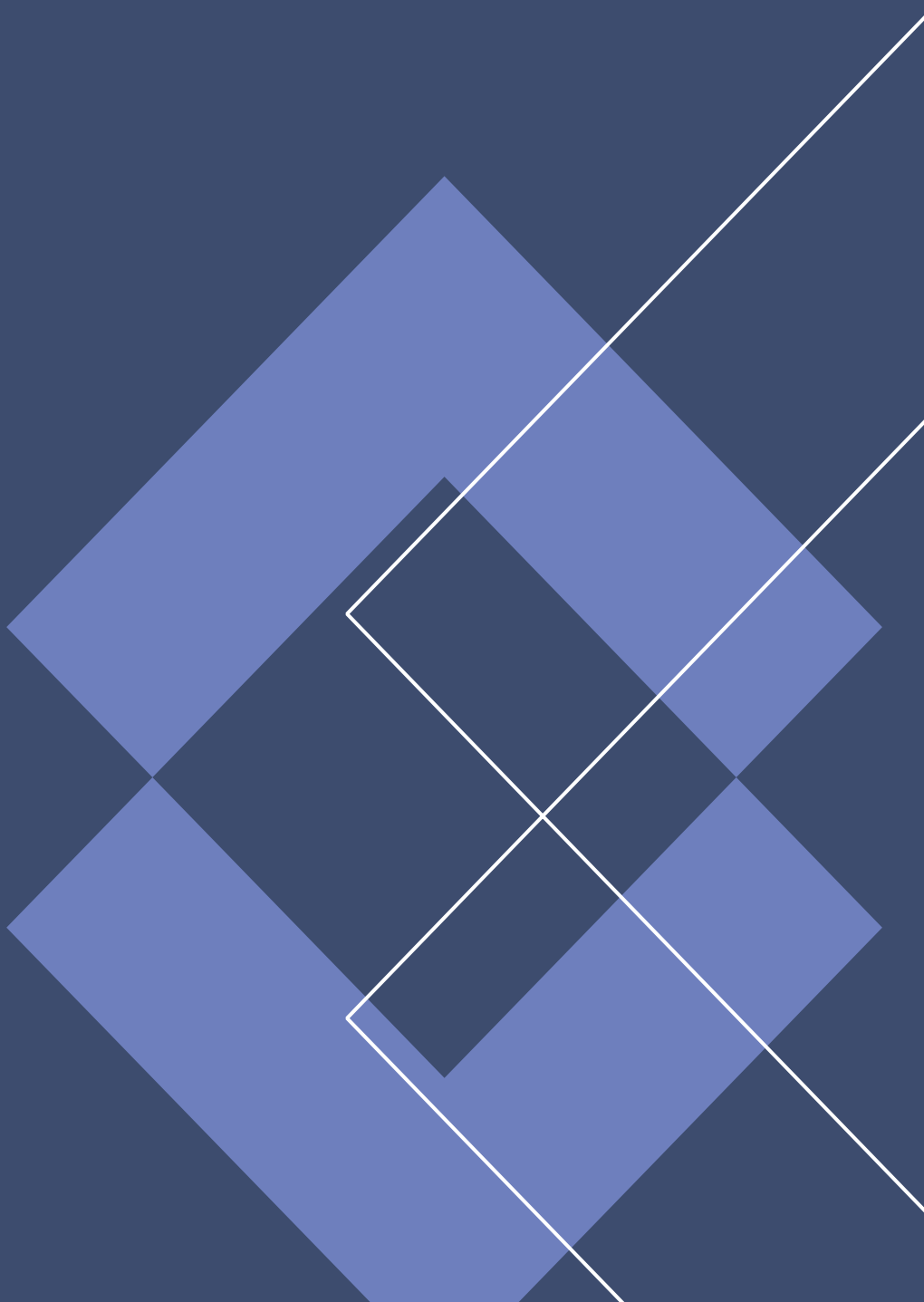
CSA
Certified Senders Alliance

Kriterien

für die IP-Plattformzertifizierung der Certified Senders Alliance (CSA)



Kriterien

für die IP-Plattformzertifizierung der Certified Senders Alliance (CSA)

Inhaltsverzeichnis

Kriterien

für die IP-Plattformzertifizierung der Certified Senders Alliance (CSA)

1. Verpflichtende Kriterien

1.1 Vertrauen und Transparenz

1.1.1 Unternehmensangaben und Kontaktmöglichkeiten

Das Unternehmen[1] muss auf seiner Website leicht auffindbar seine Postanschrift sowie eine digitale Kontaktmöglichkeit in Form einer E-Mail-Adresse oder eines Kontaktformulars angeben.

1.1.2 Datenschutzinformation

Das Unternehmen muss sicherstellen, dass auf der zugehörigen Webseite leicht auffindbare Datenschutzinformationen zur Verfügung stehen. Aus diesen muss hervorgehen, wann und in welchem Umfang personenbezogene Daten (sowohl von Kunden wie auch von Endnutzern) erhoben und verarbeitet werden. Zudem müssen Angaben enthalten sein, welche Maßnahmen zum Schutz personenbezogener Daten vor Missbrauch getroffen werden.

1.1.3 RFC-Konformität von E-Mails und Versand

Jede versendete E-Mail (Aufbau und Komposition) sowie der E-Mail-Versand (Envelope-Kommunikation im SMTP-Dialog) müssen konform zu den betreffenden Request for Comments (RFC) der IETF sein.

Maßgebend sind die jeweils aktuellen RFC. Zum Zeitpunkt der Erstellung dieses Dokuments sind das unter anderem RFC 6532, 2142, 2369, 5321,5322, 7208, 6376, 8058.

1.2 Abuse Prävention

1.2.1 Abuse-/Complaint-Adresse

Das Unternehmen ist verpflichtet, unter seiner organisations- bzw. unternehmensbezogenen Domain eine allgemeine Abuse- bzw. Complaint -Adresse einzurichten und diese im Certification Monitor der CSA zu hinterlegen. Diese Adresse muss ein Role-Account sein und hat bevorzugt die Struktur abuse@org-domain.tld. Auf Nachrichten der Beschwerdestelle an das Unternehmen muss werktags binnen 24h reagiert werden können.

1.2.2 Maßnahmen bei Plattformbetrieb für Dritte

Sofern das Unternehmen E-Mail-Technologie für den Versand kommerzieller Massen-E-Mails als Dienstleistung für Dritte anbietet, muss es geeignete Maßnahmen implementieren, um die Einhaltung der CSA Kriterien auch in Bezug auf einzelne Kunden zu gewährleisten. Dies umfasst zum Beispiel die Sperrung des Zugangs, die Begrenzung der Versandgeschwindigkeit, das maximal erlaubte Volumen oder die Beschränkung der maximalen Anzahl von Versanddomains.

[1] Der Begriff "Unternehmen" bezeichnet den Teilnehmer am Zertifizierungsverfahren für die IP-Plattform Zertifizierung bzw. das IP-Plattform zertifizierte Unternehmen.

1.2.3 Schutz von Kundenaccounts

Sofern das Unternehmen E-Mail-Technologie für den Versand kommerzieller Massen-E-Mails als Dienstleistung für Dritte anbietet, muss es geeignete Sicherheitsmaßnahmen implementieren, um die Accounts seiner Kunden vor einem Zugriff durch unberechtigte Dritte zu schützen (z.B. Zwei-Faktor-Authentifizierung).

1.2.4 Deaktivierung von Redirect-Links bei Missbrauch

Sofern in versendeten E-Mails Redirect-Links verwendet werden, muss das Unternehmen in der Lage sein, diese Links im Missbrauchsfall (z.B. beim Versand von Phishing-Mails) unverzüglich zu deaktivieren bzw. deaktivieren zu lassen, um einen Schaden durch diese Verlinkungen zu verhindern bzw. zu begrenzen.

Im Falle einer Benachrichtigung durch die eco Beschwerdestelle, dass Redirect-Links für Phishing oder dergleichen missbraucht werden, muss die Deaktivierung an Werktagen spätestens nach 24 Stunden erfolgt sein.

1.2.5 Implementierung des X-CSA-Complaints Headers

Ab erfolgter Zertifizierung muss ein „X-CSA-Complaints“-Header eingefügt und DKIM-signiert werden. Hierfür wird eine Umsetzungsfrist von vier Wochen gewährt, die mit der Benachrichtigung über die erfolgreiche Zertifizierung beginnt. Die Headerzeile lautet: „X-CSA-Complaints: csa-complaints@eco.de“ und darf nur beim zertifizierten E-Mail-Ausgangsserver implementiert werden. Das Erfüllen dieses Kriteriums ist der CSA durch eine Testaussendung zu bestätigen.

1.2.6 Technische Absicherung der E-Mail-Server

Die E-Mail-Ausgangsserver des Unternehmens müssen durch geeignete Maßnahmen technisch abgesichert sein (z.B. mit einer Firewall, kein Open Relay, kein Public Proxy, keine Backscatter, stetig überwachte Server etc.).

1.2.7 TLS-gesicherte Übertragung

E-Mails müssen über eine Transport Layer Security (TLS)-gesicherte Verbindung gemäß dem aktuellen Stand der Technik an den Empfänger zugestellt werden.

1.3 Authentifizierung

1.3.1 SPF für MAIL FROM

Für die MAIL FROM-Adresse, die in der SMTP-Kommunikation zwischen den E-Mail-Servern angegeben wird, muss ein SPF-Eintrag (RFC 7208) hinterlegt sein. Dies ermöglicht die Authentifizierung des E-Mail-Ausgangsservers gegenüber dem empfangenden E-Mail-Server. Der SPF-Eintrag muss mit „-all“ oder „~all“ enden.

1.3.2 DKIM-Signatur

Jede ausgehende E-Mail muss mindestens eine gültige DKIM-Signatur (Domain Keys Identified Mail) nach RFC 6376 enthalten.

Für Unternehmen, die eine technische Plattform für den Versand kommerzieller Massen-E-Mails als Dienstleistung für Dritte anbieten, gilt: Die im "d="-Tag verwendete Domain muss dem Kunden des Unternehmens zugeordnet werden können, d.h. der Versand-Domain des Kunden entsprechen. Zusätzliche DKIM-Signaturen für die Domains des Unternehmens (DKIM-Doppelsignatur) sind zulässig.

Für Unternehmen, die ihre eigene technische Plattform für den Versand kommerzieller Massen-E-Mails nutzen, gilt: Die im "d="-Tag verwendete Domain muss dem Unternehmen zugeordnet werden können, d.h. seine Versand-Domain betreffen.

In jedem Fall gilt: Die DKIM-Signatur muss mindestens die Header-Elemente "From", "X-CSA-Complaints", "Date" und "To" enthalten. Die Verwendung des Längenparameters "l=" ist nicht zulässig.

1.3.3 DKIM-Alignment

Jede ausgehende E-Mail muss ein DKIM-Alignment enthalten und dabei mindestens ein „relaxed alignment" vorsehen. Für ein „relaxed alignment" muss der organisatorische Domain -Teil der DKIM-Signatur („d="-Tag in der Signatur) mit der RFC5322.From (Header-From)-Domain übereinstimmen, um das geforderte Alignment zu erreichen.

Beispiel:

```
DKIM-Signatur: v=1; ...; d=brand.com; ...
From: „Friendly From“ local-part@subdomain.brand.com

oder

DKIM-Signatur: v=1; ...; d=subdomain.brand.com; ...
From: „Friendly From“ local-part@brand.com
```

Für Unternehmen, die eine technische Plattform für den Versand kommerzieller Massen-E-Mails als Dienstleistung für Dritte anbieten, ist eine Ausnahme vom DKIM-Alignment dann möglich, wenn keine markenbezogene, unternehmensbezogene oder organisationsbezogene Domain (oder Subdomain) des Kunden existiert.

1.4 Listen-Hygiene

1.4.1 List-Unsubscribe und List-Help Header

Das Unternehmen muss die Funktionalität bieten, in jeder E-Mail einen „List Unsubscribe"-Header und einen „List-Help"-Header einfügen zu können. Die anschließende Auswahl des geeigneten Headers hängt vom Inhalt der zu versendenden E-Mail ab und liegt nicht in der Verantwortung des IP-Plattform zertifizierten Unternehmens.

Der „List-Unsubscribe"-Header muss mittels der URL-Methode (entsprechend RFC 2369) mit einem „POST HTTPS"-Link eingefügt werden können. Dieser muss mit dem „List-Unsubscribe-Post"-Header kombiniert werden können, der die „One-Click-Unsubscribe"-Funktionalität (RFC 8058) unterstützt.

Der „List-Help"-Header muss mindestens eine „mailto:"-Adresse oder einen HTTPS-Link enthalten; HTTP-Links sind nicht erlaubt. Sowohl die Verwendung der „mailto:"-Adresse als auch des HTTPS-Links müssen dem Empfänger die Möglichkeit geben, Informationen zu erhalten, aus welchem Grund die E-Mail an ihn versendet wurde und weshalb eine Abmeldung auf Listenebene nicht möglich ist.

1.4.2 Abmeldemöglichkeit (Opt-Out)

Es muss dem Empfänger in jeder E-Mail mit werblichem Charakter möglich sein, die Zusendung weiterer E-Mails ohne separaten Login abzubestellen (Abmeldung/Opt-Out). Das Unternehmen muss daher sicherstellen, dass jede versendete E-Mail eine entsprechende funktionsfähige Abmeldemöglichkeit enthält. Für E-Mails mit nicht werblichem Charakter (insb. Transaktionsmails) besteht dieses Erfordernis nicht.

Als Abmeldemöglichkeit sollte bevorzugt ein Link verwendet werden, alternativ ist die Angabe einer E-Mail-Adresse zulässig.

1.4.3 Abmeldelink für Anbieter von E-Mail-Versandplattformen

Sofern das Unternehmen eine technische Plattform für den Versand kommerzieller Massen- E-Mails als Dienstleistung für Dritte anbietet, muss es seinen Kunden eine technische Funktionalität bereitstellen, in jeder E-Mail (im E-Mail-Body) einen leicht erkennbaren und funktionierenden Abmeldelink einfügen zu können. Es ist zulässig, dass der Abmeldelink zu einer Auswahlseite führt, auf welcher der Umfang der Abmeldung angegeben werden kann (z.B. Abmeldung von allen Newslettern des Unternehmens oder nur von einzelnen Newslettern, Abmeldung von Newslettern zu bestimmten Themen etc.).

1.4.4 Bounce-Handling

Das Unternehmen muss in der Lage sein, Bounce-Meldungen während der SMTP-Übertragung nach RFC 5321 zu empfangen und sie zum Zweck der Listenhygiene zu verarbeiten. Um dieses Bounce-Handling zu ermöglichen, muss es einen MX-Eintrag für die Envelope-From- (Mail-From-) Domain einrichten. Alternativ (als Fallback) ist auch ein A-Record zulässig.

1.4.5 Umgang mit nicht existierenden Postfächern

Das Unternehmen muss den weiteren Versand an E-Mail-Adressen unterbinden, bei denen nach dem Versand festgestellt wird, dass das Postfach nicht existiert.

1.5 Reputation und Performanceindikatoren

1.5.1 Spam Beschwerde Rate

Die Spam Beschwerde Rate pro Mail-Server (IP-Adresse) beziehungsweise pro Unternehmen darf innerhalb des Zeitraums von sieben Tagen (einer Woche) höchstens 0,3 Prozent betragen. Die Spam Beschwerde Rate ergibt sich aus dem Verhältnis der Anzahl von Spam-Beschwerden durch die Empfänger zu der Anzahl der E-Mails im Posteingang.

1.5.2 DKIM-Missing Rate

Die durchschnittliche DKIM-Missing Rate eines Unternehmens darf innerhalb des Zeitraums von sieben Tagen (einer Woche) höchstens 3,0 Prozent betragen. Die DKIM-Missing Rate errechnet sich aus dem Verhältnis der Anzahl der E-Mails mit DKIM-Missing zur Anzahl der insgesamt versendeten E-Mails. Dieser Schwellenwert umfasst nur Daten von Datenpartnern, die Daten zur DKIM-Validierung liefern.

1.5.3 Hard-Bounce-Rate

Die durchschnittliche Hard-Bounce-Rate pro Mail-Server (IP-Adresse) beziehungsweise pro Unternehmen darf innerhalb des Zeitraums von sieben Tagen (einer Woche) höchstens 1,0 Prozent betragen.

1.5.4 Weitere Reputationsindikatoren

Das Unternehmen soll auch darüber hinausgehend keine wesentlichen Reputationsprobleme (IP- oder DKIM-basiert) bei teilnehmenden Mailbox- oder Security-Providern (zum Beispiel basierend auf Spamtrap-Hits, Content-Scannern oder hohen Spamquoten) aufweisen.

2. Empfohlene Kriterien/Allgemeine Empfehlungen

2.1 Registrierung für Feedback-Loops und CFBL-Header

Das Unternehmen sollte sich für die öffentlich zugänglichen Feedback-Loops von Mailbox- und Security-Providern registrieren. Außerdem wird empfohlen, den CFBL-Header (RFC 9477) zu implementieren.

2.2 Multipart-E-Mails (HTML + Text)

HTML-formatierte E-Mails sollten generell mit einem Text-Part (MIME) erweitert werden. Dieser sollte Abmeldeinformationen und Hinweise zum Newsletter enthalten, da Empfänger HTML-formatierte E-Mails nicht immer korrekt empfangen können.

2.3 Einsatz von DMARC

Es wird empfohlen, Domain-based Message Authentication, Reporting and Conformance (DMARC) nach RFC 7489 einzusetzen, damit die Mailbox-Provider als Empfänger die empfangenen E-Mails nach den vorgegebenen Parametern überprüfen können. Beim Einsatz von DMARC müssen Reporting-E-Mail-Adressen so angegeben sein, dass durch Mailbox-Provider versendete Reports bei dem Unternehmen oder dessen Kunde(n) verarbeitet werden können. Es wird empfohlen, eine „Reject"-Policy zu verwenden.

2.4 Einsatz von DANE bzw. MTA-STS

Das Unternehmen sollte DANE nach RFC 7671 implementieren, um den sicheren Versand von E-Mails zu gewährleisten. Voraussetzung hierfür ist, dass DNSSEC nach RFC 9364 für die Absender- und Empfänger-Domains verfügbar ist. Sofern DNSSEC langfristig nicht verfügbar ist, sollte stattdessen MTA-STS nach RFC 8461 eingesetzt werden, um zumindest die Transportverschlüsselung abzusichern.

2.5 DKIM-Schlüssellänge und Signaturalgorithmus

Es wird empfohlen, DKIM-Schlüssel mit einer Länge von mindestens 2.048 Bit zu verwenden. Als Signaturalgorithmus sollte SHA-256 verwendet werden.

2.6 Double-Opt-In Verfahren

Es wird dringend empfohlen, dass Nutzerdaten über das so genannte Double-Opt-In (DOI)-Verfahren erhoben werden, um den strengen Anforderungen der DSGVO bezüglich der Nachweispflicht gerecht zu werden. Eine in diesem Zusammenhang versendete Bestätigungs-E-Mail darf keine werblichen oder sonstigen Inhalte umfassen.

2.7 Information über Versandfrequenz

Es wird empfohlen, dass schon bei der Erhebung der E-Mail-Adresse (zum Beispiel beim Abonnieren eines Newsletters) über die voraussichtliche Frequenz der Mailings informiert wird, sofern eine Frequenz vorliegt oder geplant ist.

2.8 Funktionsfähige Reply-To-Adresse

Es wird empfohlen, in jeder E-Mail eine funktionsfähige Reply-To-Adresse explizit anzugeben, alternativ sollte eine funktionsfähige Absenderadresse eingesetzt werden, sodass der Empfänger per „Antwort-Funktion" mit dem Absender Kontakt aufnehmen kann.

2.9 Trennung von Newsletter- und Transaktionsversand

Es wird empfohlen, Newsletter und Transaktions-Mails über unterschiedliche IPs zu versenden.

2.10 Verzicht auf URL-Shortener

Von der Verwendung von URL-Shortenern wird aus Transparenzgründen abgeraten.

2.11 Erweiterung des DKIM-Alignments

Es wird dringend empfohlen, das DKIM-Alignment (s.o., Kriterium 1.3.3) auf den Mail-From-Header (RFC5321) auszuweiten.

Beispiel:

```
DKIM-Signature: v=1; ...; d=example.com; ...
MAIL FROM: xyz@foo.example.com
```

```
From: "Example" <sender@child.example.com>
```

Darüber hinaus empfiehlt es sich, auch für die List-Header (RFC4021), Reply-To-Header (RFC5322) sowie, wenn vorhanden, Sender-Header (RFC5322), mit einer oder der gleichen DKIM-Signatur, ebenfalls auf organisatorischer Ebene, eine Übereinstimmung herbeizuführen.