Beheben von DMARC-Fehlern durch Korrigieren der SPF- und DKIM-Ausrichtung

Inhalt

Problem

E-Mails von bestimmten Domänen werden vom Cisco Secure Email Gateway (CES/ESA) aufgrund von DMARC-Verifizierungsfehlern blockiert. Die Analyse der Nachrichtenverfolgung weist darauf hin, dass diese E-Mails in der Arbeitswarteschlange gehalten und in Quarantäne gestellt oder abgelehnt werden. Dies verhindert, dass sie die beabsichtigten Empfänger erreichen.

Umwelt

- Cisco Secure Email Gateway (CES/ESA) Appliances
- SPF-, DKIM- und DMARC-Richtlinien werden konfiguriert und durchgesetzt

Auflösung

Zusammenfassende Tabelle der SPF/DKIM-Alignments (Beispiele)

Mechanismus	Ausrichtungsstatus	Umschlag-/Signaturdomäne	Von Header-Domäne	Logik
SPF	In Ausrichtung	sender@example.com	sender@example.com	Direkte Übereinstimmu

SPF	In Ausrichtung	sender@child.example.com	sender@example.com	Übergeordnete Domäne übereinstimme
SPF	Nicht ausgerichtet	sender@test.com	sender@example.com	Domänenkonfl
DKIM	In Ausrichtung	example.com	sender@example.com	Direkte Übereinstimmu
DKIM	In Ausrichtung	example.com	sender@child.example.com	Entspannter Modus
DKIM	Nicht ausgerichtet	example.com	sender@test.com	Domänenkonfl

Mit Absender abstimmen (empfohlen)

- Arbeiten Sie mit den Absender-Domänenadministratoren zusammen, um DMARC-Fehler zu beheben, indem Sie die richtige SPF- und DKIM-Ausrichtung auf der Kopfzeilenebene sicherstellen.
- Der Absender muss:
    - Stellen Sie sicher, dass die in der SPF-validierten MAIL FROM- oder HELO/EHLO-Identität verwendete Domäne mit der Domäne im From-Header der E-Mail übereinstimmt.
    - Implementieren Sie die DKIM-Signierung, wobei die im d=-Tag der DKIM-Signatur angegebene Domäne mit der From-Header-Domäne übereinstimmt.
    - Vergewissern Sie sich, dass die DMARC-Richtlinie korrekt konfiguriert ist, um den gewünschten Ausrichtungsmodus (strikt oder entspannt) und die gewünschten Reporting-Optionen durchzusetzen.
- Dieser Ansatz behebt die Ursachen von DMARC-Fehlern, indem er sich auf die Ausrichtung authentifizierter Domänen mit der sichtbaren From-Header-Domäne konzentriert, was für die langfristige Zustellung von E-Mails entscheidend ist.

DMARC-Ausnahme erstellen (alternativ)

- Wenn eine Problembehebung durch den Absender nicht möglich ist, erstellen Sie auf dem ESA-Gerät eine Ausnahme für die spezifische Absenderadresse, um DMARC-Prüfungen zu umgehen.
- Hierbei handelt es sich um einen vorübergehenden Workaround, der von einer Überwachung begleitet werden muss.

Überwachen und Validieren

- Nachdem Sie die Änderungen implementiert haben, überwachen Sie die Zustellung von Benachrichtigungs-E-Mails an die beabsichtigten Empfänger.
- Überprüfen Sie die Nachrichtenverfolgungsprotokolle, um sicherzustellen, dass DMARC-Fehler behoben wurden.
- Setzen Sie die Analyse aktualisierter Daten zur Nachrichtenverfolgung fort, wenn die Zustellungsprobleme fortbestehen.

Ursache

Die Hauptursache für die Quarantäne oder Ablehnung von E-Mails ist ein DMARC-Verifizierungsfehler aufgrund von SPF- und DKIM-Ausrichtungsproblemen. Diese Fehler weisen darauf hin, dass SPF- und DKIM-Datensätze zwar korrekt veröffentlicht werden können, die während des E-Mail-Austauschs authentifizierten Domänen jedoch nicht mit der Von-Header-Domäne übereinstimmen, was zu einer Quarantäne von E-Mails führt.

DMARC-, SPF- und DKIM-Ausrichtung:

- SPF authentifiziert die Domäne in den MAIL FROM- oder HELO/EHLO SMTP-Befehlen und erfordert, dass diese Domäne zur DMARC-Konformität mit der Domäne im From-Header übereinstimmt.
- DKIM verwendet kryptografische Signaturen mit einer im Tag d= angegebenen Signaturdomäne, die mit der Headerdomäne From übereinstimmen muss.
- DMARC baut auf SPF und DKIM auf, indem mindestens eine dieser authentifizierten Domänen mit der From-Header-Domäne übereinstimmen muss, entweder genau (strikter Modus) oder als Subdomäne (entspannter Modus).

Ein Ausfall dieser Domänenausrichtung führt zu DMARC-Ausfällen und anschließender Zurückweisung oder Quarantäne von E-Mails, selbst wenn die SPF- und DKIM-Datensätze selbst korrekt veröffentlicht und gültig sind.

Dieser Ausrichtungsfokus stellt sicher, dass die authentifizierte Identität mit der sichtbaren Absenderidentität übereinstimmt, verhindert Spoofing und verbessert die Vertrauenswürdigkeit von E-Mails.

Verwandte Inhalte

- Informationen zur SPF-Ausrichtung
- Informationen zur DKIM-Ausrichtung
- Best Practice für die E-Mail-Authentifizierung - optimale Möglichkeiten zur Bereitstellung von SPF, DKIM und DMARC - Cisco
- Konfigurieren des eingehenden Filters auf Basis der DKIM-Verifizierung in der ESA - Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.