Warum behandelt die ESA das DKIM-Authentifizierungsergebnis "permfail" als "hardfail"?

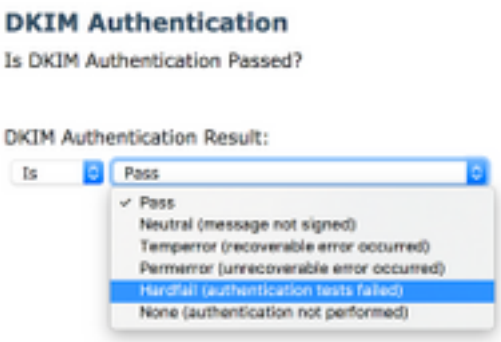
Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die E-Mail Security Appliance (ESA) die DKIM-Authentifizierungsergebnisse (DomainKeys Identified Mail) verarbeitet.

Warum behandelt die ESA das DKIM-Authentifizierungsergebnis "permfail" als "hardfail"?

Die ESA-Inhaltsfilterbedingung DKIM-Authentifizierung verfügt über mehrere Optionen, wie in diesem Bild gezeigt:



Wenn die Bedingung DKIM Authentication Result auf **Hardfail** gesetzt ist, werden permfail-Nachrichten in der E-Mail-Protokolldatei und verfolgte Nachrichten angezeigt, wie in diesem Beispiel gezeigt:

Message 815204 DKIM: permfail body hash did not verify [final] (d=sub.example.com s=selector1-sub-com i=@sub.example.com)

Die ESA betrachtet "permfail" als dasselbe wie "hardfail" und fügt das Ergebnis als "dkim=hardfail" in den Header "Authentication-Results" ein. Die ESA-Namen für DKIM-Ereignisse unterscheiden sich von RFC6376-Namen. In Headern für Authentifizierungsergebnisse (und verfolgten Nachrichten) muss die ESA die richtigen RFC6376-Zeichenfolgen anzeigen, während der Content-Filter unterschiedliche Ereignisnamen verwendet.

Diese Ereignisse werden zugeordnet: RFC6376.PERMFAIL == ESA Content-Filter - Fehler

Fehler bei der Signatur- und Nachrichtentext-Hash-Verifizierung stellen die Mehrzahl der Überprüfungsfehler dar. Body-Hash-Überprüfungsfehler weisen darauf hin, dass der Nachrichtentext nicht mit dem Hash-(Digest-)Wert in der Signatur übereinstimmt.

Signaturüberprüfungsfehler weisen darauf hin, dass der Signaturwert die signierten Headerfelder (die die Signatur selbst enthalten) in der Nachricht nicht ordnungsgemäß überprüft.

Es gibt mehrere mögliche Ursachen für diese beiden Fehler. Die Nachricht wurde möglicherweise während der Übertragung geändert (möglicherweise von einer Mailingliste oder einem Spediteur). die Signatur- oder Hashwerte wurden möglicherweise vom Unterzeichner falsch berechnet oder angewendet; Möglicherweise wurde der falsche öffentliche Schlüsselwert im DNS (Domain Name System) veröffentlicht. oder die Nachricht von einer Entität getäuscht wurde, die nicht über den privaten Schlüssel verfügt, der zur Berechnung der richtigen Signatur erforderlich ist.

Es ist sehr schwierig, diese Ursachen durch Analyse der Nachricht zu unterscheiden, obwohl die Ursprungs-IP-Adresse im Fall einer gefälschten Nachricht hilfreiche Forensik bieten kann. Aus Datenschutzgründen haben wir jedoch keinen Zugriff auf die Nachrichten selbst, sodass eine solche Analyse nicht möglich ist.

Es gibt Nachrichten, deren Signaturen aus anderen Gründen nicht überprüft werden, häufig aufgrund leicht vermeidbarer Konfigurationsfehler in den im DNS veröffentlichten Datensätzen mit öffentlichem Schlüssel (Selektor).

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.