ESA - Ersatz des vorhandenen DKIM-Schlüssels ohne Ausfallzeiten

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der vorhandene DKIM-Signaturschlüssel auf einem ESA- und DKIM-öffentlichen Schlüssel in DNS ohne Ausfallzeiten ersetzt wird.

Anforderungen

1. Zugriff auf die E-Mail Security Appliance (ESA).
2. Zugriff auf DNS zum Hinzufügen/Entfernen von TXT-Datensätzen
3. Die ESA muss bereits Nachrichten mit einem DKIM-Profil signieren.

Erstellen Sie einen neuen DKIM-Signaturschlüssel.

Sie müssen zuerst einen neuen DKIM-Signaturschlüssel auf der ESA erstellen:

1. Gehen Sie zu Mail-Policys > Signaturschlüssel, und wählen Sie "Schlüssel hinzufügen.." aus.
2. Nennen Sie den DKIM-Schlüssel, und generieren Sie entweder einen neuen privaten Schlüssel oder fügen Sie ihn in einen vorhandenen ein. **Hinweis**: *In den meisten Fällen wird empfohlen, eine private Schlüsselgröße von 2048 Bit zu wählen*.
3. Bestätigen Sie die Änderungen.
   Hinweis: Diese Änderung wirkt sich nicht auf die DKIM-Signierung oder den E-Mail-Fluss aus. Wir fügen nur einen DKIM-Signaturschlüssel hinzu und wenden ihn noch nicht auf ein DKIM-Signaturprofil an.

Erstellen Sie ein neues DKIM-Signaturprofil, und veröffentlichen Sie den DNS-Datensatz im DNS

Als Nächstes müssen Sie ein neues DKIM-Signaturprofil erstellen, einen DKIM-DNS-Datensatz aus diesem DKIM-Signaturprofil erstellen und diesen Datensatz auf DNS veröffentlichen:

1. Gehen Sie zu Mail-Policys > Signaturprofile, und klicken Sie auf "Profil hinzufügen..". Geben Sie dem Profil im Feld "Profilname" einen beschreibenden Namen.Geben Sie Ihre Domäne in das Feld "Domänenname" ein.Geben Sie eine neue Auswahlzeichenfolge in das Feld "Selector" ein.
   Hinweis: *Der Selektor ist eine beliebige Zeichenfolge, mit der mehrere DKIM-DNS-Datensätze für eine bestimmte Domäne zugelassen werden. Wir werden den Selektor verwenden, um mehr als einen DKIM DNS-Datensatz in DNS für Ihre Domäne zuzulassen. Es ist wichtig, einen neuen Selektor zu verwenden, der sich von dem bereits vorhandenen DKIM-Signaturprofil unterscheidet.*
   Wählen Sie im Feld "Signaturschlüssel" den im vorherigen Abschnitt erstellten DKIM-Signaturschlüssel aus.Fügen Sie ganz unten im Signaturprofil einen neuen "Benutzer" hinzu. Bei diesem Benutzer sollte es sich um eine nicht verwendete E-Mail-Adresse für Platzhalter handeln. Vorsicht: *Es ist wichtig, dass Sie diesem Signaturprofil als Benutzer eine nicht verwendete E-Mail-Adresse hinzufügen. Andernfalls kann dieses Profil ausgehende Nachrichten signieren, bevor der DKIM TXT-Datensatz veröffentlicht wird, was dazu führt, dass die DKIM-Überprüfung fehlschlägt. Durch Hinzufügen einer nicht verwendeten E-Mail-Adresse als Benutzer wird sichergestellt, dass dieses Signaturprofil keine ausgehenden Nachrichten signiert.*Klicken Sie auf Senden.
2. Klicken Sie hier in der Spalte "DNS-Textdatensatz" auf "Generate" (Generieren) für das Signaturprofil, das Sie gerade erstellt haben, und kopieren Sie den generierten DNS-Datensatz. Er sollte ähnlich wie folgt aussehen:

   ```
   selector2._domainkey.example.com. IN TXT "v=DKIM1;
   p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMaX6wMAk4iQoLNWiEkj0BrIRMDHXQ7743OQUOYZQqEXS
   s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTMdV0HWAi2AGsVOT8BdFHkyxg40
   oyGWgktzc1q7zIgWM8usHfKVWFzYgnattNzyEqHsfI7lGilz5gdHBOvmF8LrDSfN"
   "KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkrl9riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
   QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB;"
   ```
3. Bestätigen Sie die Änderungen.
4. Senden Sie den DKIM DNS TXT-Datensatz in Schritt 2 an DNS.
5. Warten Sie, bis der DKIM DNS TXT-Datensatz vollständig weitergegeben wurde.

Löschen Sie das alte Signaturprofil, und entfernen Sie den Platzhalter-Benutzer aus dem neuen Signaturprofil.

Nachdem der DKIM TXT-Datensatz an DNS gesendet wurde und Sie sichergestellt haben, dass er weitergegeben wurde, wird im nächsten Schritt das alte Signaturprofil gelöscht und der Platzhalter-Benutzer aus dem neuen Signaturprofil entfernt:

> Hinweis: *Es wird dringend empfohlen, die ESA-Konfigurationsdatei zu sichern, bevor Sie mit den folgenden Schritten fortfahren. Dies liegt daran, dass Sie die gesicherte Konfigurationsdatei einfach laden können, wenn Sie das alte DKIM-Signaturprofil löschen und die vorherige Konfiguration wiederherstellen müssen.*

1. Gehen Sie zu Mail-Policys > Signaturprofile, wählen Sie das alte DKIM-Signaturprofil aus, und klicken Sie auf "Löschen".
2. Wechseln Sie zum neuen DKIM-Signaturprofil, wählen Sie den aktuellen Platzhalterbenutzer aus, und klicken Sie auf "Entfernen".

3. Klicken Sie auf "Senden".
4. Klicken Sie unter der Spalte "Testprofil" auf "Test" für das neue DKIM-Signaturprofil. Wenn der Test erfolgreich ist, fahren Sie mit dem nächsten Schritt fort. Wenn nicht, stellen Sie sicher, dass der DKIM DNS TXT-Datensatz vollständig weitergegeben wurde.
5. Bestätigen Sie die vorgenommenen Änderungen.

Testen des E-Mail-Datenflusses zur Bestätigung der DKIM-Durchläufe

An dieser Stelle ist die weitere Konfiguration von DKIM abgeschlossen. Testen Sie jedoch die DKIM-Signierung, um sicherzustellen, dass die ausgehenden Nachrichten wie erwartet signiert und die DKIM-Verifizierung befolgt wird:

1. Senden Sie eine Nachricht über die ESA, um sicherzustellen, dass DKIM von der ESA signiert und DKIM von einem anderen Host verifiziert wird.
2. Wenn die Nachricht am anderen Ende empfangen wurde, überprüfen Sie die Kopfzeilen der Nachricht für den Header "Authentication-Results" (Authentifizierungsergebnisse). Suchen Sie im Abschnitt "DKIM" des Headers nach der Überprüfung, ob die DKIM-Überprüfung erfolgreich war. Der Header sollte ähnlich wie folgt aussehen:
   ```
   Authentication-Results: mx1.example.net; spf=SoftFail smtp.mailfrom=user1@example.net;
   dkim=pass header.i=none; dmarc=fail (p=none dis=none) d=example.net
   ```
3. Suchen Sie nach dem Header "DKIM-Signature", und stellen Sie sicher, dass die richtige Auswahl und Domäne verwendet wird:

   ```
   DKIM-Signature: a=rsa-sha256; d=example.net; s=selector2;
     c=simple; q=dns/txt; i=@example.net;
     t=1117574938; x=1118006938;
     h=from:to:subject:date;
     bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
     b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
              VoG4ZHRNiYzR
   ```
4. Wenn Sie davon überzeugt sind, dass DKIM wie vorgesehen funktioniert, warten Sie mindestens eine Woche, bevor Sie den alten DKIM TXT-Datensatz entfernen. Dadurch wird sichergestellt, dass alle Nachrichten, die mit dem alten DKIM-Schlüssel signiert wurden, verarbeitet wurden.