Wie können Sie die LDAP Accept-Abfrage verwenden, um den Absender der weitergeleiteten Nachrichten zu überprüfen?

Inhalt

Frage

Wie können Sie die LDAP Accept-Abfrage verwenden, um den Absender der weitergeleiteten Nachrichten zu überprüfen?

WARNUNG: Sie können eine LDAP Accept-Abfrage nur für die Umschlagadresse *'mail from'* ausführen, wenn die Nachricht in einem öffentlichen Listener eingeht. Der private Listener lässt die Verwendung von LDAP Accept-Abfragen nicht zu. LDAP Accept-Abfrage wird nur auf eingehende Verbindungen angewendet. Aus diesem Grund darf das 'Connection Behavior' der Mail Flow Policy NICHT auf Relay gesetzt werden, damit diese Konfiguration funktioniert.

Im Folgenden finden Sie die erforderlichen Schritte zum Einrichten der LDAP Accept Query Sender Validation:

1. Um es internen Absendern zu gestatten/verweigern, im Internet zu kommunizieren, muss Ihr privater Listener durch einen öffentlichen Listener ersetzt werden, je nachdem, ob seine E-Mail-Adresse im LDAP vorhanden ist. In diesem Beispiel erhält der neue öffentliche Listener den Namen "Outbound_Sender_Validation".

2. Erstellen Sie ein neues LDAP-Serverprofil, und richten Sie eine LDAP Accept-Abfrage für dieses Profil ein. Um die LDAP Accept-Abfrage zur Validierung der E-Mail-Absenderadresse zu erhalten, müssen Sie {a} durch {f} in der Abfragezeichenfolge ersetzen. Weitere Informationen zur Konfiguration und Verwendung von LDAP finden Sie im erweiterten Benutzerhandbuch.

   Beispiel: *(mail={a}) => (mail={f})*

3. Aktivieren Sie die konfigurierte LDAP Accept-Abfrage im Listener "Outbound_Sender_Validation".

4. Gehen Sie zu "**Mail Policies > Recipient Access Table (RAT)**", und wechseln Sie zum neuen öffentlichen Listener "Outbound_Sender_Validation". Um die Weiterleitung zuzulassen, setzen Sie "Alle anderen Empfänger" auf "Akzeptieren", und stellen Sie sicher, dass dies der einzige Eintrag im RAT ist.

5. Gehen Sie zu "HAT Overview" und wechseln Sie zum Listener "Outbound_Sender_Validation". Hier benötigen Sie nur eine Absendergruppe. Um das Risiko eines offenen Mail-Relays zu vermeiden, empfiehlt es sich, diese Absendergruppe so einzurichten, dass sie nur die IP-Adressen der MTA(s) abgleicht, die weitergeleitet werden dürfen.
   Es ist wichtig, dass das 'Connection Behavior' der zugewiesenen Mail Flow Policy NICHT auf Relay festgelegt ist, da andernfalls die Verwendung der LDAP Accept-Abfrage deaktiviert würde. Um sicherzustellen, dass keine anderen MTA(s) über "Outbound_Sender_Validation" eine Verbindung herstellen können, legen Sie die Richtlinie der Standardabsendergruppe "ALL" auf BLOCKED fest.

Was wird in den Protokollen angezeigt?

WARNUNG: Basierend auf dieser Konfiguration erfolgt die Ablehnung nicht vor dem Empfang der Rcpt-To-Umschlagadresse. Der Grund hierfür ist, dass die LDAP Accept-Abfrage ursprünglich für die Überprüfung durch den Empfänger statt für die Überprüfung durch den Absender vorgesehen war. Dies wird auch in den Mail-Protokollen angezeigt, in denen die LDAP-Ablehnung in derselben Protokollzeile wie die Empfängeradresse angegeben wird:

```
Wed Feb 18 16:16:19 2009 Info: New SMTP ICID 2643 interface Management
(10.0.0.100) address 10.0.0.200 reverse dns host unknown verified no
Wed Feb 18 16:16:19 2009 Info: ICID 2643 ACCEPT SG RELAY_HOSTS match 10.0.0.200
rfc1918
Wed Feb 18 16:16:32 2009 Info: Start MID 2554 ICID 2643
Wed Feb 18 16:16:32 2009 Info: MID 2554 ICID 2643
From: <do_not_exist@example.test>
Wed Feb 18 16:16:39 2009 Info: MID 2554 ICID 2643 To: <good_user@example.com>
Rejected by LDAPACCEPT
Wed Feb 18 16:17:14 2009 Info: ICID 2643 close
```

Wenn Sie sich diesen Protokolleintrag ansehen, glauben Sie, dass die abgelehnte Adresse 'good_user@example.com' ist, obwohl es sich um 'do_not_exist@example.test' handelt, das abgelehnt wird.