Identificare e consentire server di posta con punteggio SBRS (SenderBase Reputation Score) inadeguato

Sommario

Introduzione

In questo articolo viene descritto come identificare e consentire temporaneamente ai server di posta con punteggio SBRS (SenderBase Reputation Score) basso tramite Email Security Appliance (ESA).

Premesse

Il filtro della reputazione del mittente è il primo livello di protezione dalla posta indesiderata, che consente di controllare i messaggi che passano attraverso il gateway di posta elettronica in base all'affidabilità del mittente, determinata da SBRS. Le connessioni dei server di posta elettronica con SBRS inadeguato possono essere rifiutate o i messaggi rimbalzati, in base alle preferenze dell'utente.

Problema

Un server di posta si connette all'ESA e viene segnalato come SBRS insufficiente e le e-mail sono ritardate a causa di una risposta SMTP 554 ricevuta dal server di connessione.

Esempio di risposta 554:

```
-----Original Message-----
From: Mail Delivery System [mailto:Mailer-Daemon@example.domain.com]
Sent: 25 April 2013 23:23
To: user@companyx.com
Subject: Mail delivery failed: returning message to sender

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:
```

```
person@example.domain.com
SMTP error from remote mail server after initial connection:
host gatekeeper.companyx.com [195.195.195.1]: 554-gatekeeper1.companyx.com
554 Your access to this mail system has been rejected due to the sending
MTA's poor reputation. If you believe that this failure is in error, please
contact the intended recipient via alternate means.
```

Soluzione

Identificazione del server di posta SBRS inadeguato

Utilizzare l'interfaccia della riga di comando (CLI) in quanto il rilevamento dei messaggi dell'interfaccia utente grafica (GUI) non registra le connessioni rifiutate per impostazione predefinita.

> **Nota:** La registrazione delle connessioni rifiutate può essere abilitata selezionando **GUI > Servizi di sicurezza > Verifica messaggi > Abilita gestione connessioni rifiutate**

Usare **grep** sul dominio per eseguire il pull di tutti i dati di registrazione correlati sul dominio. Per questo output, il dominio di esempio utilizzato è *test.com*:

```
myesa.local> grep "test.com" mail_logs

Info: New ICID 1512 to Management (10.0.0.1) from 198.51.100.1 connecting host reverse DNS
hostname: smtp1.

test.com


Info: MID 6531

ICID 1512 From: test@test.com
```

Quindi, **eliminare** l'ID connessione in ingresso (ICID) per estrarre le informazioni sull'host della posta. La registrazione di ICID viene utilizzata per rivelare tutte le informazioni, ad esempio l'indirizzo IP dell'host di invio, il nome host verificato dal DNS (se disponibile), la corrispondenza del gruppo di mittenti e il punteggio SBRS associato:

```
myesa.local> grep "ICID 1512" mail_logs


Tue Mar 10 12:04:29 2015 Info: New SMTP ICID 1512 interface Management (10.0.0.1) address
198.51.100.1 reverse dns host unknown verified smtp1.test.com
Tue Mar 10 12:04:29 2015 Info: ICID 1512 REJECT SG BLACKLIST match sbrs[-10:-3] SBRS -4.0
```

Consenti al server di posta SBRS scadente di utilizzare l'ESA

1. Dalla GUI, selezionare **Mail Policies > HAT overview** (Policy di posta > Panoramica HAT).
2. Clic **Aggiungi gruppo di mittenti...**
3. Assegnare al gruppo di mittenti un nome significativo.
4. Selezionare l'ordine in modo che si trovi al di sopra del gruppo Mittenti BLACKLIST.
5. Selezionare Criterio posta, **ACCETTATO** o **LIMITATO**.
6. Lasciare vuoti tutti gli altri campi.
7. Fare clic su Submit and Add Senders (Invia e aggiungi mittenti).
8. Aggiungere l'indirizzo IP o il nome host DNS degli host interessati come indicato dal

comando grep.

9. Fare clic su **Submit (Invia).**
10. Controllare la panoramica HAT e verificare che il nuovo gruppo di mittenti sia ordinato correttamente.
11. Infine, fare clic su **Commit** per salvare tutte le modifiche alla configurazione.

Per l'indirizzo del mittente sono consentiti i formati seguenti:

- Indirizzi IPv6 come 2001:420:80:1::5
- indirizzi IPv4, ad esempio 10.1.1.0
- Subnet IPv4 o IPv6, ad esempio 10.1.1.0/24, 2001:db8::/32
- Intervalli di indirizzi IPv4 o IPv6, ad esempio 10.1.1.10-20, 10.1.1-5 o 2001:db8::1-2001:db8::10
- Nomi host come example.com
- Nomi host parziali, ad esempio .example.com.

Nell'esempio riportato sopra, per consentire l'accesso a qualsiasi altra informazione sul server di posta che termina con *test.com*, questa sarebbe stata configurata come:

```
198.51.100.1
smtp1.test.com
.test.com
```

Informazioni correlate

Informazioni su Cisco SenderBase