

Risoluzione degli errori di recapito dei messaggi di posta elettronica causati da problemi di configurazione dei record DNS invertiti (PTR)

Sommario

Problema

I messaggi di posta elettronica inviati a domini specifici vengono rifiutati con il messaggio di errore "Annullato dal server di destinazione con la risposta: 5.3.0 - Altri problemi del sistema di posta ('550', ['Ricerca inversa IP mittente rifiutata'])". Il rifiuto si verifica quando il server di posta elettronica ricevente tenta di eseguire una ricerca DNS inversa sull'indirizzo IP del mittente e non riesce a trovare un record PTR valido o trova un record PTR non configurato correttamente.

I messaggi di posta elettronica inviati al dominio example.com tornano in modo coerente con l'errore di rifiuto della ricerca DNS inversa. I log dell'appliance Cisco Cloud Email Security (CES) mostrano che l'elaborazione dei messaggi e-mail in uscita è stata completata correttamente, ma il server di posta di destinazione li ha rifiutati a causa di errori di convalida dei record PTR.

Ambiente

- Servizio Cisco Cloud Email Security (CES)
- Microsoft Exchange Server come sistema di posta di origine
- Recapito tramite e-mail a domini esterni (example.com)
- Non sono state segnalate modifiche di configurazione recenti in CES
- Impatto aziendale: Distribuzione di e-mail gravemente danneggiata per un dominio

Risoluzione

Configurare i record DNS inversi (PTR) corretti per gli indirizzi IP utilizzati dal server di Exchange quando si inviano messaggi di posta elettronica tramite il servizio Cisco Cloud Email Security.

1. Analizza i log di posta CES per identificare il modello di rifiuto

```
grep "Sender IP reverse lookup rejected" mail.current
```

I log hanno rivelato messaggi di salto consistenti:

```
Bounced: DCID 11205849 MID 14584716 to RID 0 - Bounced by destination server with response: 5.3.0 - Other
```

2. Verificare l'elaborazione dei messaggi tramite CES

```
grep "MID 14584701" mail.current
```

I log hanno confermato che il CES stava elaborando correttamente le e-mail:

```
MID 14584701 SPF: mailfrom identity example@example.com Pass (v=spf1)
MID 14584701 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
MID 14584701 queued for delivery
Message done DCID 11205836 MID 14584701 to RID [0]
```

3. Convalidare i record PTR esistenti. L'analisi tecnica conferma che i record PTR esistenti non sono configurati correttamente per gli indirizzi IP specifici utilizzati da Exchange Server per il recapito della posta in uscita.

4. Identificare gli indirizzi IP specifici utilizzati da Exchange Server per inviare messaggi di posta elettronica tramite il servizio CES.

5. Collaborare con il provider DNS o con l'amministratore DNS interno per creare o aggiornare i record PTR per gli indirizzi IP identificati. Questi record PTR dovevano essere risolti in nomi host corrispondenti o coerenti con l'infrastruttura di posta del dominio di invio.

6. Dopo aver implementato le modifiche ai record PTR, verificare che i record siano stati propagati correttamente e che possano essere risolti da server DNS esterni.

7. Dopo la configurazione del record PTR, inviare alcuni messaggi di prova al dominio interessato in precedenza (example.com) per confermare il recapito senza errori di rifiuto.

Causa

La causa principale è stata la mancanza o la configurazione non corretta dei record DNS invertiti (PTR) per gli indirizzi IP utilizzati dal server di Exchange durante l'invio di messaggi di posta elettronica tramite il servizio Cisco Cloud Email Security. Molti server di posta elettronica eseguono ricerche DNS inverse nell'ambito dei processi di convalida della protezione e della protezione da posta indesiderata. Quando un record PTR è mancante o non configurato correttamente, il server di posta ricevente può rifiutare l'e-mail come precauzione per la sicurezza, presupponendo che provenga da una fonte non autorizzata o compromessa.

Il problema era specificamente relativo alla configurazione DNS dal lato del mittente (infrastruttura di Exchange Server), non al servizio Cisco Cloud Email Security, che stava elaborando e tentando di recapitare i messaggi di posta elettronica correttamente.

Contenuto correlato

[Il destinatario rifiuta la posta da Microsoft 365 e il nome host non corrisponde all'errore dell'indirizzo IP](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).