La posta indesiderata ricevuta da Cisco Email Security Appliance (ESA) nell'organizzazione

Sommario

[Introduzione](#)
[Metodi](#)
[1. Messaggio legittimo/Posta commerciale](#)
[2. Aggiornamento Dell'Antispam Non Corretto](#)
[3. Criterio di posta o filtro messaggi](#)
[4. Criteri flusso di posta](#)
[5. Il messaggio è indesiderato](#)

Introduzione

In questo documento vengono descritti cinque metodi per inviare e-mail indesiderate all'organizzazione.

Metodi

1. Messaggio legittimo/Posta commerciale

Il messaggio legittimo è stato scelto dall'utente o il suo nome è stato venduto a un'altra organizzazione. Nel primo caso, l'utente dovrà eseguire delle operazioni per annullare la sottoscrizione all'elenco. Se si tratta di quest'ultimo, inviare nuovamente il messaggio a spam@access.ironport.com in modo che le definizioni antispam possano essere aggiornate globalmente, migliorando la percentuale complessiva di acquisizione della posta indesiderata dell'ESA. L'attivazione della posta di marketing nei criteri di posta in arrivo può contribuire a modificare la percezione di questo messaggio come "Marketing" anziché "Spam".

2. Aggiornamento Dell'Antispam Non Corretto

La protezione dalla posta indesiderata è disabilitata oppure la chiave della funzionalità è scaduta. Per verificare se è in corso l'aggiornamento di Anti-Spam, selezionare **GUI > Servizi di sicurezza > IronPort Anti-Spam**. In questo riquadro vengono visualizzati gli aggiornamenti ai set di regole o al motore nelle ultime 6 ore. Inoltre, da questa scheda nella parte superiore è possibile verificare che il servizio antispam sia abilitato. Per verificare lo stato della chiave della funzionalità, andare alla scheda Amministrazione del sistema > Chiave della funzionalità per controllare lo stato della chiave antispam.

3. Criterio di posta o filtro messaggi

La posta indesiderata può raggiungere l'organizzazione se il motore di protezione antispam è disabilitato per un mittente o un destinatario specifico in base ai criteri di posta elettronica del cliente. Un altro modo per ignorare il filtro antispam è tramite i filtri messaggi (CLI: **filters**).

4. Criteri flusso di posta

Un messaggio viene classificato utilizzando l'ICID del messaggio. In questa situazione è probabile che la funzionalità di protezione dalla posta indesiderata sia disattivata, ignorando i criteri di posta elettronica. È possibile determinare questa condizione esaminando i log di posta, all'interno dei log sarà necessario esaminare prima l'ICID per capire in quale SenderGroup il messaggio è stato classificato. Da qui la revisione dei criteri del flusso di posta associati. Se l'elenco AllowList contiene un numero elevato di voci, potrebbe essere necessario esaminare alcuni dei messaggi ricevuti per verificare se sono stati analizzati dal motore AntiSpam. Aprire le intestazioni di un messaggio e cercare l'intestazione X-IronPort-Spam. La presenza di questa intestazione indica che il messaggio è passato attraverso il motore.

5. Il messaggio è indesiderato

Il messaggio è effettivamente indesiderato. Conferma che il messaggio è stato analizzato dal modulo antispam utilizzando la funzionalità di verifica dei messaggi (nella verifica dei messaggi cercare "CASE"). Se il verdetto della richiesta è negativo e il messaggio viene considerato indesiderato, inviare il messaggio originale a spam@access.ironport.com. Potrebbe trattarsi di una nuova minaccia di posta indesiderata che è appena stata rilasciata o di una minaccia precedente che è stata riprogettata.

L'elaborazione degli invii di posta indesiderata è automatica e manuale e non è disponibile alcun feedback per l'invio specifico. In qualsiasi momento è possibile contattare Cisco TAC e richiedere una valutazione e una risposta.