Elenco di controllo per l'efficacia della protezione dalla posta indesiderata di Cisco Email Security Appliance (ESA)

Sommario

Introduzione

Le procedure e le raccomandazioni che seguono sono "best practice" per ridurre la quantità di spam che passa attraverso l'ESA. Tenere presente che ogni cliente è diverso e che alcune di queste raccomandazioni possono aumentare il numero di e-mail legittime classificate come spam (falsi positivi).

Configurazione di base

1. Verificare che la protezione da posta indesiderata sia attivata:

   Verificare che tutti i record MX (inclusa la priorità più bassa) stiano inoltrando la posta attraverso le ESA.Verificare che gli accessori dispongano di una chiave valida per la funzionalità di protezione dalla posta indesiderata.Assicurarsi che la protezione da posta indesiderata sia abilitata per tutti i criteri di posta in arrivo appropriati.

2. Verificare di aver ricevuto gli aggiornamenti delle regole per la posta indesiderata. Verificare che i timestamp **più recenti** per gli aggiornamenti in Servizi di sicurezza > Anti-Spam siano stati rilevati nelle ultime 2 ore.

3. Verificare che i messaggi vengano analizzati da Anti-Spam:

   Controlla un esempio di messaggi di posta indesiderata mancanti per la seguente intestazione: Risultato X-IronPort-Anti-Spam:Se l'intestazione è mancante:

   Verificare di non avere voci dell'elenco di indirizzi consentiti o filtri che impediscano alla posta indesiderata di ignorare la scansione (vedere di seguito).Verificare che i messaggi non vengano ignorati perché superano le dimensioni massime consentite per l'analisi dei messaggi (il valore predefinito è 262144 byte). La riduzione di questa impostazione non migliora in modo significativo le prestazioni e può causare la perdita di SPAM. Durante una valutazione, è anche importante assicurarsi che l'impostazione IPAS sia la stessa di tutti gli altri prodotti testati.Esaminare ogni voce HAT e confermare che "spam_check=on" per tutti i criteri di flusso della posta in arrivo. Se il valore predefinito è "spam_check= on" e nessuno

dei criteri di flusso della posta lo disattiva esplicitamente, la configurazione è corretta. Prestare particolare attenzione alle impostazioni TRUSTED/allowLIST. Spesso i clienti aggiungono inavvertitamente un mittente all'elenco dei mittenti autorizzati che inoltra spam, ad esempio aggiungendo il dominio di un ISP o di un partner che inoltra sia spam che e-mail legittime al gruppo di mittenti allowLIST.

Controllare rapidamente i filtri messaggi per verificare che non siano presenti filtri che consentono di ignorare lo spamcheck. In caso affermativo, accertarsi che il destinatario stia eseguendo le operazioni desiderate, tenendo presente che la corrispondenza con un solo destinatario può essere applicata anche ai messaggi con più di 30 destinatari.

Trovare un esempio di SPAM recente (ora, data, ricezione e così via) e fare riferimento ai log di posta per verificare cosa è successo. Confermare che Anti-Spam ha restituito un verdetto negativo.

4. Accertarsi di eseguire le azioni desiderate sui messaggi di posta indesiderata positivi. Per informazioni sulla gestione dei verdetti antispam, vedere Criteri posta in arrivo. Verificare che i messaggi di posta indesiderata positivi e sospetti vengano eliminati o messi in quarantena nel criterio predefinito e che tutti gli altri criteri utilizzino il comportamento predefinito o sostituiscano deliberatamente quello predefinito.

5. Applicare soglie di posta indesiderata più aggressive se i falsi positivi destano meno preoccupazioni rispetto alla posta indesiderata persa:

   Ridurre la soglia di posta indesiderata positiva a 80 (il valore predefinito è 90) se i falsi positivi non rappresentano un problema per la soglia "certa".

   Ridurre la soglia di possibile posta indesiderata a 40 (il valore predefinito è 50) se i falsi positivi non rappresentano un problema per la soglia "sospetto".

   Se la maggior parte dei reclami relativi alla posta indesiderata proviene da un sottoinsieme di destinatari, è possibile creare un criterio di posta separato per questi utenti con soglie di posta indesiderata più basse in modo da filtrare in modo più efficace solo i destinatari.

   Le modifiche a questi valori non devono essere prese alla leggera, né devono essere attuate senza dati concreti per accertare quali saranno gli effetti riduttivi.

   Inoltre, non regolare necessariamente i valori nella direzione opposta solo per evitare falsi positivi.Assicurarsi che i falsi positivi e i falsi negativi siano inviati a TAC.

6. Ottimizza le impostazioni SBRS e i criteri HAT:

   La maggior parte delle organizzazioni aggiunge SBRS da -10 a -3.0 al proprio elenco di blocco e SBRS da -3.0 a -1.0 al proprio ELENCO DI SOSPETTI. I clienti più aggressivi possono bloccare le porte SBRS da -10 a -2.0 e aggiungere da -2.0 a -0.6 all'elenco dei sospetti.

   In alcuni casi, il fatto che un mittente non disponga ancora di un punteggio di reputazione

SenderBase è la prova che il mittente potrebbe essere uno spammer. È possibile aggiungere SBRS "none" direttamente a un gruppo di mittenti che ottiene il criterio "Throttled", ad esempio al gruppo di mittenti con stato SUSPECT.

Modificare il numero massimo di destinatari all'ora in 5 per il criterio "Limitato".

Valutare la possibilità di creare più criteri di limitazione per applicare limiti orari diversi per ogni destinatario, ad esempio per limitare la frequenza di mittenti con una SBRS compresa tra -2 e -1 e 5 destinatari all'ora e mittenti con una SBRS compresa tra -1 e 0 e 20 destinatari all'ora.

7. Abilita verifica mittente per il criterio di flusso di posta "limitato":

   I clienti possono scegliere di aggiungere mittenti con DNS inesistente o configurato in modo non corretto al gruppo di mittenti SUSPECTLIST.

   Il record PTR dell'host connesso non esiste nel DNS.La connessione della ricerca dei record PTR dell'host non è riuscita a causa di un errore DNS temporaneo.

   La connessione della ricerca DNS inversa dell'host (PTR) non corrisponde alla ricerca DNS diretta (A).

   Esiste il rischio di falsi positivi da parte di mittenti con DNS non configurato correttamente, pertanto i clienti potrebbero voler impostare un criterio di flusso di posta separato che restituisce una risposta 4xx personalizzata indicante il motivo per cui i messaggi vengono rifiutati.

   Per ulteriori informazioni sulla verifica del mittente, consultare la Guida in linea o la Guida dell'utente di AsyncOS

8. Abilitare l'accettazione LDAP e la protezione dagli attacchi di tipo Raccolto directory:

   Molti spammer inviano e-mail a un numero elevato di indirizzi non validi, pertanto bloccare i mittenti che inviano a destinatari non validi può anche ridurre la posta indesiderata.

   Se l'accettazione LDAP è già attiva, verificare che anche la protezione DAP (Directory Harvest Protection) sia configurata per ciascun listener in ingresso con un numero massimo di tentativi non validi compreso tra 5 e 10 per IP.

9. Abilita dizionari contenuto:

   L'ESA viene fornita con due dizionari di contenuti: profanity.txt e sex_content.txt. Anche se l'utilizzo di questi dizionari può generare falsi positivi, alcuni clienti hanno scoperto che filtrare il flusso di posta per individuare parole inappropriate può ridurre il rischio che la "persona sbagliata" riceva le "e-mail sbagliate". Questi filtri possono essere applicati solo alle "rotelle stridulate" abilitandole per un gruppo di utenti in una policy di posta specifica.

10. Segnala i messaggi non classificati a Cisco TAC.

11. Per evitare un numero elevato di falsi positivi, è consigliabile disabilitare SBRS per la scansione in uscita. Questo perché SBRS considera la reputazione degli IP in ingresso, e in una rete interna, la maggior parte di questi IP sono dinamici. Attenersi alla procedura descritta nella sezione successiva.

Abilita SBNP

1. Assicurarsi che la posta in entrata e in uscita si trovino su listener separati.

2. Disabilita le ricerche SenderBase per la posta in uscita per ogni indirizzo di seguito. Per eseguire questa operazione dalla GUI, selezionare Rete > Listener, selezionare i listener in uscita, scegliere "Avanzate" e deselezionare la casella accanto a "Usa profilo IP SenderBase".

   SenderBase Network Participation (SBNP) può aumentare significativamente l'efficacia dei filtri reputazione, antispam ed epidemie di virus. Inoltre, se abilitata durante l'utilizzo della protezione antispam e altamente sicura, la SBNP non ha alcun impatto significativo sulle prestazioni.

   Nota: Il volume di posta indesiderata ricevuto dall'organizzazione cambierà nel tempo. È possibile che l'ESA abbia ricevuto più posta indesiderata semplicemente perché il numero di messaggi indesiderati è superiore a quello del passato. È possibile tenere traccia di questo comportamento nel tempo esaminando la pagina Panoramica della posta in arrivo e aggiungendo le voci "interrotto dal filtro reputazione" e "messaggi di posta indesiderata rilevati".

Motivazione SBRS

La grande preoccupazione dei falsi positivi è che importanti e-mail possano andare perdute. In questo contesto, la pratica di mettere in quarantena o eliminare i messaggi di posta indesiderata positivi è problematica. Se un'e-mail autentica viene inviata a una cartella di quarantena o spam, è necessario eseguire una ricerca proattiva per accedere e "notare" che il messaggio è stato erroneamente classificato come spam.

Al contrario, i messaggi di posta elettronica bloccati e con limitazioni di velocità vengono bloccati in modo che il mittente venga informato immediatamente. Se il mittente NON è uno spammer, probabilmente troverà un altro modo per contattare l'utente. In effetti, come regola generale, il blocco per impostazione predefinita e l'accettazione successiva di partner di fiducia su richiesta rappresentano una posizione migliore per alcune aziende.

La limitazione, se impostata correttamente, deve raramente o mai colpire i partner, ma fornisce protezione dai domini che vengono infettati da virus. La limitazione sarà anche off-put per gli spammer. Siamo a conoscenza di una tecnica spammer per acquistare grandi numeri di IP, generare abbastanza "buona" e-mail per ottenere un punteggio SBRS decente e quindi iniziare lo spamming. Un intervallo più ampio di elenchi di sospetti dovrebbe intercettarli, limitare i danni che possono causare l'interruzione dell'invio di spam al tuo dominio.