Gemeenschappelijke fouten in de configuratie van de ESA's

Inhoud

Inleiding

Dit document beschrijft gemeenschappelijke configuratiefouten in e-mail security applicatie (ESA).

Wat zijn de gemeenschappelijke configuratiefouten in de ESA?

Of u een nieuwe evaluatie opstelt of over een bestaande configuratie kijkt, kunt u naar deze controlelijst van algemene configuratiefouten verwijzen.

HAT

- Plaats geen positieve SBRS-scores zoals +5 of +7 in de ALLOWLIST. Een bereik van 9.0-10.0 zou OK zijn, maar als je lagere scores opneemt is het alleen maar waarschijnlijker dat spam er door zal komen.
- Schakel de UNKNOWNLIST-, Envelope Sender DNS-verificatie en Connecting Host DNS-verificatie uit, tenzij u deze echt nodig hebt en begrijpt.
- In plaats van de berichtgrootte en andere beleidsinstellingen in elk beleid van de Mail Flow te veranderen, ga naar het menu Mail Flow Policy en kies de laatste optie, "Default Policy parameters".
- Beperk maximale verbindingen tot drie voor de meeste zenders, en maak dit de standaard voor het nieuwe beleid van de Stroom van de Post.
- Controleer of SenderBase scores van -10.0 tot -2.0 in de BLOCKLIST zijn opgenomen. De documentatie en setup-kaarten zijn te conservatief. op dit ogenblik hebben wij geen valse positieve resultaten .

Beleidsbeleid

- Geef beleid aan wie ze krijgt en niet wat ze doen. Naam van elke inhoud filters na wat ze

doen en gebruik afkortingen zoals Q_basic_attachments, D_spoofers, Strip_Multi-Media, waar Q quarantaine en D neerzetten betekent.
- Non-default beleid moet "Default Settings" gebruiken voor anti-spam, animatievirus, contentfilters en Outbreak filters, behalve wanneer u echt speciale instellingen nodig hebt. Herstel deze instellingen niet in elk beleid als dit niet nodig is.
- Vul "Verbonden bijlagen neerzetten" in of anders geeft u veel lege e-mails door waar het virus is verwijderd.
- Antivirusinstellingen voor uitzending moeten de zender en niet de ontvanger op de hoogte stellen
- Uitbraakfilters en anti-Spam moeten bij uitstek worden uitgeschakeld

Inkomende relais

Als "Monitor > Overzicht" verbindingen van uw eigen servers en domeinen toont, moet u ze aan de inkomende versies van Relay toevoegen. Een zeer vaak voorkomende fout, bij gebruik van de GUI, is om te denken dat u de functie Inkomend Relay hebt ingeschakeld wanneer u alleen de items aan de tabel hebt toegevoegd. Daarnaast:

- Voeg voor rapportagedoeleinden een speciale HAT - verzendgroep voor deze groepen toe, boven ALLOWLIST. Kies geen snelheidsbeperking of DHAP, maar spam en virusdetectie zijn OK.
- Voeg een berichtfilter toe om uw BLOCKLIST beleidsactie aan te passen. Bijvoorbeeld:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

In zeldzame gevallen waarin u e-mail opnieuw injecteert (bijvoorbeeld door intersubscriber-mail opnieuw te verwerken via het inkomende e-mailbeleid), zal uw filter ook de herinjectieinterface moeten vrijstellen. Normaal gesproken is dit niet nodig.

DNS

Veel klanten dwingen de ESA om hun interne DNS-servers ongebruikelijk te vragen. In de meeste installaties zijn 100% van de DNS-records die we nodig hebben op het internet en niet op de interne DNS-site. Het is logischer om de Internet root servers te vragen, waardoor de verzendbelasting op de interne DNS wordt verminderd.

Bericht- en contentfilters

De meest voorkomende fout is om matchomstandigheden in contentfilters te plaatsen waar deze niet nodig zijn. De meeste filters moeten een lijst van bepaalde handelingen maken, maar de voorwaarde moet leeg zijn. Het filter zal altijd *waar* zijn en zal altijd actief zijn. U controleert welke gebruikers/beleid deze acties ontvangen door nieuwe Inkomende of Uitgaande Post Beleid te creëren zoals nodig, en deze filter op het beleid toe te passen. Hier zijn onjuiste en correcte voorbeelden:

- Het is bijna altijd een fout om de rcpt-to-conditie in een berichtfilter te gebruiken. De juiste

procedure is om een inkomend contentfilter te schrijven en het voor een bepaalde gebruiker specifiek te maken door een op een ontvanger gebaseerd Inkomend Mail-beleid toe te voegen.
- Het is vrijwel altijd een fout om een contentfiltertest te hebben voor de aanwezigheid van een bijlage en dan de bijlage te laten vallen. De juiste methode is om deze bevestiging altijd te laten vallen, zonder te testen op de aanwezigheid ervan.
- Het is bijna altijd een fout om de resultaten() te gebruiken. Levering betekent overslaan van resterende filters en dan afleveren. Als u gewoon wilt leveren zonder de rest van de filters te overslaan, is geen expliciete actie vereist (impliciete levering).

Open Relay-preventie

Sommige services zullen controleren of uw Message Transfer Agent (MTA) adressen accepteert die mogelijk kunnen resulteren in open relais voorwaarden. Aangezien het verlaten van uw MTA als functionerend open relais slecht is, kunnen deze plaatsen u aan een BLOCKLIST toevoegen tenzij u deze gevaarlijke adressen in het gesprek mtp. afwijst.

Voeg voor rapportagedoeleinden een speciale HAT - verzendgroep voor deze groepen toe, boven ALLOWLIST. Kies geen snelheidsbeperking of DHAP, maar laat spam en virusdetectie toe.

- Verandering in Streng Adres Parsing (Los is de standaard). Dit is nodig om dubbele @ borden in adressen te voorkomen.
- Ongeldige tekens afwijzen (niet verwijderen). Dit is ook nodig om dubbele @ borden in adressen te voorkomen.
- Afwijzen (niet accepteren) van lettertypen en de volgende tekens invoeren: *%!\\/?

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems