Erreurs de configuration courantes sur l'ESA

Contenu

Introduction

Ce document décrit les erreurs de configuration courantes sur le dispositif de sécurité de la messagerie électronique (ESA).

Quelles sont les erreurs de configuration courantes sur le ESA ?

Que vous configuriez une nouvelle évaluation ou que vous examiniez une configuration existante, vous pouvez vous reporter à cette liste de contrôle des erreurs de configuration courantes.

CHAT

- N'inscrivez pas les scores positifs SBRS comme +5 ou +7 dans ALLOWLIST. Une plage de 9.0 à 10.0 serait correcte, mais l'inclusion de scores plus faibles ne fera qu'augmenter la probabilité que le spam passe.
- Désactivez la vérification DNS UNKNOWNLIST, Envelope Sender et la vérification DNS de l'hôte de connexion, sauf si vous en avez vraiment besoin et que vous les comprenez.
- Au lieu de modifier la taille des messages et d'autres paramètres de stratégie dans chaque stratégie de flux de courrier, accédez au menu Stratégies de flux de courrier et choisissez la dernière option, « Paramètres de stratégie par défaut ».
- Limitez le nombre maximal de connexions à trois pour la plupart des expéditeurs, et faites de ce nombre la valeur par défaut pour les nouvelles stratégies de flux de messages.
- Vérifiez que les scores SenderBase de -10.0 à -2.0 sont inclus dans la liste BLOCKLIST. Les assistants de documentation et de configuration sont trop prudents ; à l'heure actuelle, il n'y a pas de faux positifs dans cette fourchette.

Politique

- Nommez les politiques après qui les obtient, pas ce qu'elles font. Nommez tous les filtres de contenu après ce qu'ils font, et utilisez des abréviations telles que Q_basic_pièces jointes,

D_spoofers, Strip_Multi-média, où Q signifie quarantaine et D signifie suppression.
- Les stratégies autres que les stratégies par défaut doivent utiliser les paramètres par défaut pour les filtres anti-spam, anti-virus, de contenu et contre les attaques, sauf si vous avez vraiment besoin de paramètres spéciaux. Ne recréez pas ces paramètres dans chaque stratégie si cela n'est pas nécessaire.
- Décochez la case « Supprimer les pièces jointes infectées », sinon vous transmettrez de nombreux e-mails vides où le virus a été supprimé.
- Les paramètres antivirus pour le trafic sortant doivent avertir l'expéditeur et non le destinataire
- Les filtres contre les attaques et l'antispam doivent être désactivés en sortie

Relais entrants

Si « Monitor > Overview » indique les connexions de vos propres serveurs et domaines, vous devez les ajouter à la configuration des relais entrants. Une erreur très courante, lors de l'utilisation de l'interface utilisateur graphique, est de penser que vous avez activé la fonction de relais entrant alors que tout ce que vous avez fait est d'ajouter les entrées à la table. En outre :

- Ajoutez un groupe d'expéditeurs HAT spécial pour eux, ci-dessus ALLOWLIST, à des fins de reporting. Choisissez pas de limitation de débit ou DHAP, mais la détection de spam et de virus est correcte.
- Ajoutez un filtre de message correspondant à votre action de stratégie BLOCKLIST. Exemple :

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

Dans les rares cas où vous réinjectez des courriels (par exemple, le retraitement des courriels interabonnés par le biais de la politique de courrier entrant), votre filtre devra également exempter l'interface de réinjection. Normalement, cela n'est pas nécessaire.

DNS

De nombreux clients forcent l'ESA à interroger leurs serveurs DNS internes par habitude. Dans la plupart des installations, 100 % des enregistrements DNS dont nous avons besoin se trouvent sur Internet et non dans le DNS interne. Il est plus logique d'interroger les serveurs racine Internet, réduisant ainsi la charge de transfert sur le DNS interne.

Filtres de messages et de contenu

L'erreur la plus courante consiste à placer les conditions correspondantes dans les filtres de contenu lorsqu'elles ne sont pas requises. La plupart des filtres doivent répertorier certaines actions, mais la condition doit rester vide. Le filtre sera *vrai* toujours et sera toujours exécuté. Vous contrôlez les utilisateurs/stratégies qui reçoivent ces actions en créant de nouvelles stratégies de courrier entrant ou sortant selon les besoins, et en appliquant ce filtre à la stratégie. Voici des exemples incorrects :

- Il est presque toujours erroné d'utiliser la condition rcpt-to dans un filtre de message. La

procédure correcte consiste à écrire un filtre de contenu entrant et à le rendre spécifique pour un utilisateur particulier en ajoutant une stratégie de messagerie entrante basée sur le destinataire.
- Il est presque toujours erroné d'avoir un test de filtre de contenu pour la présence d'une pièce jointe, puis de supprimer la pièce jointe. La méthode correcte consiste à toujours supprimer cette pièce jointe, sans tester sa présence.
- C'est presque toujours une erreur d'utiliser la fonction de livraison() . Livrer signifie ignorer les filtres restants, puis livrer. Si vous voulez simplement livrer sans ignorer le reste des filtres, aucune action explicite n'est requise (livraison implicite).

Prévention des relais ouverts

Certains services vérifieront si votre agent de transfert de messages (MTA) accepte des adresses qui pourraient entraîner des conditions de relais ouvert. Puisque le fait de laisser votre MTA comme un relais ouvert fonctionnel est mauvais, ces sites peuvent vous ajouter à une BLOCKLIST, sauf si vous rejetez ces adresses dangereuses dans la conversation SMTP.

Ajoutez un groupe d'expéditeurs HAT spécial pour eux, ci-dessus ALLOWLIST, à des fins de reporting. Choisissez no rate limit ou DHAP, mais autorisez la détection de spam et de virus.

- Passer à l'analyse stricte des adresses (Loose est la valeur par défaut). Ceci est nécessaire pour empêcher les doubles signes @ dans les adresses.
- Rejeter (non supprimer) les caractères non valides. Ceci est également nécessaire pour empêcher les doubles signes @ dans les adresses.
- Rejeter les littéraux (non accepter) et entrer les caractères suivants : *% !\/ ?

Informations connexes

- Support et documentation techniques - Cisco Systems