Le spam est détecté par l'appliance de sécurité de la messagerie Cisco (ESA) dans votre entreprise

Contenu

Introduction

Ce document décrit cinq méthodes que les courriers indésirables peuvent utiliser pour entrer dans votre entreprise.

Méthodes

1. Message légitime / Message marketing

Le message légitime a été choisi par l'utilisateur ou son nom a été vendu à une autre organisation. Dans le premier cas, l'utilisateur devra prendre des mesures pour se désinscrire de la liste. Si c'est le cas, envoyez le message à spam@access.ironport.com afin que les définitions antispam puissent être mises à jour globalement, améliorant ainsi le taux global de capture de spam de votre ESA. L'activation du message marketing dans la politique de courrier entrant peut aider à changer la perception de ce message comme étant « Marketing » par rapport au « Spam ».

2. L'antispam n'est pas mis à jour correctement

L'antispam est désactivé ou la clé de fonction a expiré. Pour vérifier et voir si l'antispam est en cours de mise à jour, accédez à **GUI > Security Services > IronPort Anti-spam**. Dans ce panneau, vous devriez voir les mises à jour des jeux de règles ou du moteur dans les 6 dernières heures. Dans cet onglet en haut, vous pouvez également vous assurer que le service antispam est activé. Pour consulter l'état de la clé de fonction, accédez à l'onglet Administration système > Clé de fonction pour vérifier l'état de la clé antispam.

3. Stratégie de messagerie ou filtre de message

Le courrier indésirable peut entrer dans votre entreprise si le moteur de sécurité antispam est désactivé pour un expéditeur ou un destinataire spécifique, conformément à la politique de messagerie d'un client. Une autre façon d'ignorer le filtrage du courrier indésirable consiste à utiliser des filtres de messages (CLI : **filter**).

4. Stratégie de flux de messages

Un message est classifié à l'aide de l'ICID du message. Dans ce cas, il est probable que la fonction de sécurité antispam est désactivée, ce qui remplace la stratégie de messagerie. Vous pouvez le déterminer en consultant les journaux de messagerie. Dans ces journaux, vous devez d'abord consulter l'ICID pour savoir dans quel SenderGroup le message a été classé. À partir de là, examinez la stratégie de flux de courrier associée. Si vous avez un grand nombre d'entrées dans AllowList, vous devrez peut-être revoir certains des messages qui arrivent pour voir s'ils ont été analysés par le moteur AntiSpam. Ouvrez les en-têtes d'un message et recherchez l'en-tête X-IronPort-Spam, la présence de cet en-tête signifie que le message est passé par le moteur.

5. Le message est un spam

Le message est un spam réel. Vous avez confirmé que le message a été analysé par le moteur antispam à l'aide de la fonctionnalité Suivi des messages (dans le suivi des messages, recherchez « CASE »). Si le verdict est négatif et que vous considérez le message comme du spam, envoyez le message d'origine à spam@access.ironport.com. Il peut s'agir d'une nouvelle menace de spam qui vient d'être lancée ou d'une menace plus ancienne qui a été restructurée.

Le traitement des envois de spam est à la fois automatique et manuel et il n'y a pas de retour pour votre envoi spécifique. À tout moment, vous pouvez contacter le centre d'assistance technique de Cisco et demander une évaluation et une réponse.