Liste de contrôle d'efficacité d'anti-Spam des appareils de sécurité du courrier électronique de Cisco (ESA)

Contenu

Les procédures suivantes et les recommandations sont des « pratiques recommandées » pour réduire la quantité de Spam obtenant par l'ESA. Notez que chaque client est différent et que certaines de ces recommandations peuvent augmenter le nombre d'emails légitimes classifiés comme Spam (faux positifs).

Installation de base

1. Assurez-vous que l'anti-Spam est activé :

   Vérifiez pour s'assurer que tous vos enregistrements MX d'enregistrements MX (priorité plus basse y compris) transmettent par relais la messagerie par ESAs.Veillez vos appliances pour avoir une touche de fonction valide d'anti-Spam.Assurez que l'anti-Spam est activé pour toutes les stratégies appropriées de messagerie entrante.

2. Vérifiez que vous recevez des mises à jour de règle d'anti-Spam. Vérifiez pour confirmer que les groupes date/heure **les plus récents** pour des mises à jour sous les Services de sécurité > l'anti-Spam ont lieu des 2 dernières heures.

3. Assurez-vous que des messages sont balayés par l'anti-Spam :

   Vérifiez un échantillon de messages spam manqués pour l'en-tête suivante : X-IronPort-Anti-Spam-résultat :Si cette en-tête manque :

   Vérifiez pour s'assurer que vous n'avez aucunes entrées ou filtre de Whitelist faisant sauter le Spam la lecture de Spam (voir ci-dessous).Vérifiez pour s'assurer que les messages ne sautent pas la lecture parce qu'ils dépassent la taille maximum de balayage de messages (le par défaut est de 262144 octets). La réduction de cette configuration n'améliore pas considérablement la représentation et peut avoir comme conséquence le Spam manqué. Pendant une évaluation, il est également important de s'assurer que la configuration IPAS est identique comme tous autres produits étant testés.Passez par chaque entrée de CHAPEAU et confirmez que « spam_check=on » pour toutes les stratégies d'arrivée de flux de courrier. Tant que le par défaut a le « spam_check= sur », et aucune des stratégies de

flux de courrier ne l'arrête explicitement, ceci est configuré correctement. Particulière attention de paiement aux configurations TRUSTED/WHITELIST. Chronomètre souvent des clients ajoutent par distraction un expéditeur à leur Whitelist qui expédie le Spam - par exemple, en ajoutant le domaine d'un ISP ou le partenaire qu'en avant spam et légitimez l'email au groupe d'expéditeur WHITELIST.

Faites un contrôle rapide par les filtres de message pour s'assurer qu'il n'y a pas aucun filtre qui « saut-spamcheck ». S'il y a, assurez-vous qu'ils font ce qu'ils devraient (maintenant dans l'esprit qui appariant un simple rcpt-à la correspondance de boîte sur des messages avec destinataires 30+).

Trouvez un exemple récent Spam (heure, date, rcpt, etc.), et mettez en référence les mail_logs pour voir ce qui s'est produit. Confirmez que l'anti-Spam a renvoyé un verdict négatif.

4. Assurez-vous que vous prenez les actions désirées sur des messages de positif de Spam. Vérifiez les stratégies d'arrivée de messagerie pour la façon dont des verdicts d'anti-Spam sont manipulés. Assurez-vous que les messages positifs et suspects Spam sont lâchés ou mis en quarantaine dans la stratégie par défaut, et que toutes autres stratégies utilisent le comportement par défaut ou délibérément ignorent le par défaut.

5. Appliquez des seuils plus agressifs de Spam si les faux positifs sont moins de souci que le Spam manqué :

   Ramenez le seuil positif de Spam à 80 (le par défaut est 90) si les faux positifs ne sont pas un souci au « certain » seuil.

   Réduisez a suspecté le seuil de Spam à 40 (le par défaut est 50) si les faux positifs ne sont pas un souci au seuil « suspect ».

   Si la plupart de vos plaintes de Spam proviennent un sous-ensemble de destinataires, vous pouvez créer une stratégie distincte de messagerie pour ces utilisateurs avec les seuils inférieurs de Spam afin de filtrer plus agressivement pour juste ces destinataires.

   Est-ce que modifications à ces valeurs ne devraient pas être prises légèrement, ni devraient elles n'être décrétées sans aucune données vérifiées pour s'assurer ce que seront les effets repurcussive.

   En outre, n'ajustez pas nécessairement les valeurs dans l'autre direction pour éviter seulement des faux positifs.Veuillez s'assurer que des faux positifs et les faux négatifs sont soumis au TAC.

6. Optimisez vos configurations SBRS et stratégies de CHAPEAU :

   La plupart des organismes sont SBRS ajoutants confortables -10 -3.0 à leur liste noire et SBRS -3.0 1.0 à leur SUSPECTLIST. Des clients plus agressifs peuvent mettre SBRS -10 -2.0 et additionner sur la liste noire -2.0 à -0.6 au SUSPECTLIST.

Dans certains cas, le fait qu'un expéditeur n'a pas encore un score de réputation de SenderBase est des preuves que cet expéditeur peut être un spammer. Vous pouvez ajouter SBRS « aucun » directement à un groupe d'expéditeur qui obtient la stratégie « étranglée », par exemple à votre groupe SUSPECT d'expéditeur.

Changez le nombre maximum de destinataires par heure à 5 pour la stratégie « étranglée ».

Consider créant plus d'un « a étranglé » la stratégie pour imposer le destinataire différent par limites d'heure - par exemple des expéditeurs de limitation de débit avec un SBRS entre -2 et -1 à 5 récepteurs par heure et expéditeurs avec un SBRS entre -1 et 0 à 20 destinataires par heure.

7. Activez la vérification d'expéditeur pour la stratégie « étranglée » de Mailflow :

   Les clients peuvent choisir d'ajouter des expéditeurs avec les DN inexistants ou incorrectement configurés au groupe d'expéditeur SUSPECTLIST.

   Inclure l'article PTR d'hôte n'existe pas dans des DN.Connecter l'hôte que le PTR enregistrent la consultation échoue en raison de la panne provisoire de DN.

   Connecter la consultation inverse de DN d'hôte (PTR) n'apparie pas la consultation en avant de DN (a).

   Il y a un certain risque de faux positifs des expéditeurs avec les DN SIG-configurés, ainsi les clients peuvent vouloir installer une stratégie distincte de Mailflow qui renvoie une réponse de la coutume 4xx indiquant que les messages de raison sont rejetés.

   Vérifiez l'aide en ligne ou le guide utilisateur d'AsyncOS pour plus d'informations sur la vérification d'expéditeur

8. Le LDAP d'enable protection d'attaque reçoivent et de récoltes de répertoire :

   Beaucoup de spammers envoient des emails à un nombre élevé d'adresses non valides, bloquant ainsi les expéditeurs qui envoient aux destinataires non valides peuvent également diminuer le Spam.

   Si le LDAP reçoivent est déjà en fonction, s'assurent que la protection de récolte de répertoire (DHAP) est également configuré pour chaque auditeur d'arrivée avec des tentatives non valides maximum entre 5 et 10 par IP.

9. Dictionnaires satisfaits d'enable :

   Votre ESA est livré avec deux dictionnaires satisfaits : profanity.txt et sexual_content.txt. Tandis que l'utilisation de ces dictionnaires peut générer des faux positifs, quelques clients ont trouvé cela filtrant leur flot de messagerie pour des mots inadéquats peuvent réduire le risque « de la personne fausse » obtenant « l'email faux ». Ces filtres peuvent seulement être appliqués « aux roues grinçantes » en les activant pour un groupe d'utilisateurs dans une stratégie spécifique de messagerie.

10. Messages mauvais par état à Cisco TAC.

11. Pour empêcher un grand nombre de faux positifs, SBRS devrait être désactivé pour la lecture sortante. C'est parce que SBRS regarde la réputation de l'IPS entrant, et dans un réseau interne, la majeure partie de ces IPS est dynamique. Suivez les étapes dans la section suivante.

Enable SBNP

1. Assurez-vous que la messagerie d'arrivée et sortante soyez sur les auditeurs distincts.

2. Désactivez les consultations de SenderBase pour l'email sortant par ci-dessous. Pour faire ceci du GUI, aller au réseau > aux auditeurs, sélectionner tous les auditeurs sortants, choisir « a avancé » et décoche la case à côté « de l'IP de SenderBase d'utilisation profilant ».

   La participation de réseau de SenderBase (SBNP) peut de manière significative augmenter l'efficacité des filtres de réputation, de l'anti-Spam et des filtres d'attaque de virus. SBNP également n'a aucune incidence des performances apparente si activé en utilisant l'anti-Spam et est fortement sécurisé.

Notez que le volume de Spam que votre organisation reçoit changera au fil du temps. Il est possible que plus de Spam obtienne par l'ESAs simplement étant donné que vous recevez plus de Spam que dans le passé. Vous pouvez dépister ce comportement au fil du temps en regardant la page d'aperçu de messagerie entrante et en ajoutant « arrêté par le filtrage de réputation » et les éléments de ligne détectés des « par messages spam ».

Raisonnement SBRS

Le grand souci avec des faux positifs est que l'important email pourrait obtenir perdu. Dans ce contexte, la pratique de mettre en quarantaine ou de relâcher l'email positif Spam est problématique. Si un email légitime est envoyé à une quarantaine ou à un répertoire de Spam, il exige d'une recherche proactive d'entrer et « notez » que du jambon a été mal classé comme Spam.

En revanche, la liste noire et les emails débit-limités sont bloqués de telle manière qu'on annonce immédiatement l'expéditeur. Si cet expéditeur n'est pas un spammer, ils trouveront vraisemblablement une autre manière d'établir le contact avec vous. En fait, comme stratégie globale, bloquant par défaut et puis recevoir les Partenaires de confiance sur demande, est une meilleure position pour quelques entreprises.

L'étranglement, si réglé correctement, devrait rarement si jamais les Partenaires d'affect, mais assureront la protection contre les domaines qui obtiennent infecté par des virus. L'étranglement sera également rebutant aux spammers. Nous nous rendons compte d'une technique de spammer pour acheter un grand nombre d'IP, générons assez de « bon » email pour obtenir un score convenable SBRS et puis pour commencer le Spamming. Une plage suspecte plus étendue de liste devrait attraper ces derniers, limitent les dommages qu'elles font et ils peuvent par la suite les faire cesser d'envoyer le Spam à votre domaine.