Liste de contrôle de l'efficacité antispam de l'appliance de sécurité de la messagerie Cisco (ESA)

Contenu

Introduction

Les procédures et recommandations suivantes sont des « meilleures pratiques » pour réduire le nombre de spams transitant par l'ESA. Notez que chaque client est différent et que certaines de ces recommandations peuvent augmenter le nombre de courriels légitimes classés comme spam (faux positifs).

Configuration de base

1. Assurez-vous que l'antispam est activé :

   Vérifiez que tous vos enregistrements MX (y compris les enregistrements de priorité inférieure) relaient le courrier via les ESA.Assurez-vous que vos appliances disposent d'une clé de fonction antispam valide.Assurez-vous que l'antispam est activé pour toutes les stratégies de messagerie entrante appropriées.

2. Vérifiez que vous recevez des mises à jour de règles antispam. Vérifiez que les horodatages **les plus récents** pour les mises à jour sous Security Services > Anti-Spam proviennent des 2 dernières heures.

3. Assurez-vous que les messages sont analysés par Anti-Spam :

   Vérifiez un exemple de messages indésirables manqués pour l'en-tête suivant : X-IronPort-Anti-Spam-Result :Si cet en-tête est manquant :

   Vérifiez que vous n'avez pas d'entrées de liste d'autorisation ou de filtres qui empêchent le spam de contourner l'analyse du spam (voir ci-dessous).Vérifiez que les messages ne contournent pas l'analyse car ils dépassent la taille maximale d'analyse des messages (la valeur par défaut est 262 144 octets). La réduction de ce paramètre n'améliore pas considérablement les performances et peut entraîner une absence de SPAM. Lors d'une évaluation, il est également important de s'assurer que le paramètre IPAS est le même que tous les autres produits testés.Parcourez chaque entrée de TAH et confirmez que « spam_check=on » pour toutes les stratégies de flux de courrier entrant. Tant que la valeur

par défaut est « spam_check= on » et qu'aucune des stratégies de flux de courrier ne la désactive explicitement, ceci est configuré correctement. Faites particulièrement attention aux paramètres TRUSTED/allowLIST. Souvent, les clients ajoutent par inadvertance un expéditeur à leur liste d'autorisation qui transfère du spam - par exemple, en ajoutant le domaine d'un FAI ou d'un partenaire qui transfère du spam et des e-mails légitimes au groupe d'expéditeurs allowLIST.

Vérifiez rapidement les filtres de messages pour vous assurer qu'il n'y a pas de filtres qui « ignorent-spamcheck ». S'il y en a, assurez-vous qu'ils font ce qu'ils doivent faire (en gardant à l'esprit que la correspondance d'un seul accusé de réception peut correspondre sur les messages avec plus de 30 destinataires).

Recherchez un exemple récent de SPAM (heure, date, rcpt, etc.), et référencez les journaux de messagerie pour voir ce qui s'est passé. Confirmez que Anti-Spam a retourné un verdict négatif.

4. Assurez-vous que vous effectuez les actions souhaitées sur les messages indésirables positifs. Vérifiez les stratégies de messagerie entrante pour savoir comment les verdicts antispam sont gérés. Assurez-vous que les messages SPAM positifs et suspects sont supprimés ou mis en quarantaine dans la stratégie par défaut et que toutes les autres stratégies utilisent le comportement par défaut ou remplacent délibérément la stratégie par défaut.

5. Appliquez des seuils de spam plus agressifs si les faux positifs sont moins préoccupants que les spams manqués :

   Réduisez le seuil de spam positif à 80 (la valeur par défaut est 90) si les faux positifs ne sont pas un problème au niveau du seuil 'certain'.

   Réduisez le seuil de spam suspecté à 40 (la valeur par défaut est 50) si les faux-positifs ne sont pas un problème au niveau du seuil 'suspect'.

   Si la plupart de vos plaintes de spam proviennent d'un sous-ensemble de destinataires, vous pouvez créer une stratégie de messagerie distincte pour ces utilisateurs avec des seuils de spam inférieurs afin de filtrer plus agressivement pour ces destinataires uniquement.

   Les modifications apportées à ces valeurs ne doivent pas être prises à la légère et ne doivent pas non plus être adoptées sans données précises pour déterminer quels seront les effets répursifs.

   En outre, ne pas nécessairement ajuster les valeurs dans l'autre direction seulement pour éviter les faux positifs.Assurez-vous que les faux positifs et faux négatifs sont soumis au TAC.

6. Optimisez vos paramètres SBRS et vos stratégies HAT :

   La plupart des entreprises sont prêtes à ajouter SBRS -10 à -3.0 à leur liste de blocage et SBRS -3.0 à -1.0 à leur SUSPECTLIST. Les clients plus agressifs peuvent bloquer SBRS -

10 à -2.0 et ajouter -2.0 à -0.6 à SUSPECTLIST.

Dans certains cas, le fait qu'un expéditeur n'ait pas encore de Score de réputation SenderBase prouve que cet expéditeur peut être un spammeur. Vous pouvez ajouter SBRS « none » directement à un groupe d'expéditeurs qui obtient la stratégie « Throttled », par exemple à votre groupe d'expéditeurs SUSPECT.

Remplacez le nombre maximal de destinataires par heure par 5 pour la stratégie « Limitée ».

Envisagez de créer plus d'une stratégie limitée pour appliquer différentes limites de destinataires par heure - par exemple, la limitation du débit des expéditeurs avec un SBRS compris entre -2 et -1 à 5 destinataires par heure et des expéditeurs avec un SBRS compris entre -1 et 0 à 20 destinataires par heure.

7. Activez la vérification de l'expéditeur pour la stratégie de flux de messages « limité » :

   Les clients peuvent choisir d'ajouter des expéditeurs avec un DNS inexistant ou mal configuré au groupe d'expéditeurs SUSPECTLIST.

   L'enregistrement PTR de l'hôte de connexion n'existe pas dans DNS.Échec de la recherche d'enregistrement PTR de l'hôte en raison d'une défaillance DNS temporaire.

   La recherche DNS inverse de l'hôte de connexion (PTR) ne correspond pas à la recherche DNS directe (A).

   Il existe un certain risque de faux positifs chez les expéditeurs avec un DNS mal configuré. Les clients peuvent donc vouloir configurer une stratégie de flux de messages distincte qui renvoie une réponse 4xx personnalisée indiquant la raison pour laquelle les messages sont rejetés.

   Pour plus d'informations sur la vérification de l'expéditeur, consultez l'aide en ligne ou le guide de l'utilisateur AsyncOS.

8. Activez LDAP accept and Directory Harvest Attack Protection :

   De nombreux spammeurs envoient des e-mails à un nombre élevé d'adresses non valides, de sorte que le blocage des expéditeurs qui envoient des messages aux destinataires non valides peut également réduire le spam.

   Si l'acceptation LDAP est déjà activée, assurez-vous que Directory Harvest Protection (DHAP) est également configuré pour chaque écouteur entrant avec un maximum de tentatives non valides entre 5 et 10 par IP.

9. Activer les dictionnaires de contenu :

   Votre ESA comporte deux dictionnaires de contenu : profanity.txt et sex_content.txt. Bien que l'utilisation de ces dictionnaires puisse générer des faux positifs, certains clients ont constaté que le filtrage de leur flux de messages pour rechercher des mots inappropriés peut réduire

le risque que la « mauvaise personne » reçoive le « mauvais courrier ». Ces filtres ne peuvent être appliqués qu'aux « roulettes de courroux » en les autorisant pour un groupe d'utilisateurs dans une politique de courrier spécifique.

10. Signalez les messages mal classés au TAC Cisco.

11. Pour éviter un grand nombre de faux positifs, SBRS doit être désactivé pour l'analyse sortante. En effet, SBRS examine la réputation des adresses IP entrantes et, dans un réseau interne, la plupart de ces adresses IP sont dynamiques. Suivez les étapes de la section suivante.

Activer SBNP

1. Assurez-vous que les messages entrants et sortants se trouvent sur des écouteurs distincts.

2. Désactivez les recherches SenderBase pour les e-mails sortants par défaut. Pour ce faire à partir de l'interface graphique utilisateur, accédez à Réseau > Écouteurs, sélectionnez les écouteurs sortants, choisissez Avancé et décochez la case en regard de « Utiliser le profilage IP SenderBase ».

   La participation au réseau SenderBase (SBNP) peut augmenter de manière significative l'efficacité des filtres de réputation, des filtres antispam et des filtres contre les attaques de virus. SBNP n'a pas non plus d'impact notable sur les performances si elle est activée lors de l'utilisation de l'antispam et est hautement sécurisée.

   Note: Le volume de spam reçu par votre entreprise va changer au fil du temps. Il est possible que davantage de spams passent par les ESA simplement parce que vous recevez plus de spams que par le passé. Vous pouvez suivre ce comportement au fil du temps en consultant la page Présentation des messages entrants et en ajoutant les éléments de ligne « interceptés par le filtrage de réputation » et « messages indésirables détectés ».

Justification SBRS

La grande préoccupation avec False Positives est que les e-mails importants pourraient se perdre. Dans ce contexte, la mise en quarantaine ou la suppression des e-mails SPAM Positive pose problème. Si un e-mail légitime est envoyé à une quarantaine ou à un dossier de spam, une recherche proactive est nécessaire pour y accéder et « signaler » que le spam a été mal classé comme spam.

En revanche, les e-mails bloqués et à débit limité sont bloqués de manière à ce que l'expéditeur soit immédiatement averti. Si cet expéditeur n'est PAS un spammeur, il est probable qu'il trouvera un autre moyen de vous contacter. En fait, en tant que stratégie globale, bloquer par défaut puis accepter des partenaires de confiance sur demande, est une meilleure position pour certaines entreprises.

La limitation, si elle est correctement définie, devrait rarement, voire jamais, affecter les partenaires, mais fournira une protection contre les domaines infectés par des virus. La limitation sera également un peu décevante pour les spammeurs. Nous sommes au courant d'une

technique de spammeur pour acheter un grand nombre d'IP, générer suffisamment de « bons » e-mails pour obtenir un score SBRS décent et ensuite commencer à spammer. Une plus grande plage de noms suspects devrait les détecter, limiter les dégâts qu'ils causent et éventuellement les empêcher d'envoyer du spam à votre domaine.