Lista de comprobación de eficacia antispam de Cisco Email Security Appliance (ESA)

Contenido

Introducción

Los siguientes procedimientos y recomendaciones son "prácticas recomendadas" para reducir la cantidad de spam que llega a través del ESA. Tenga en cuenta que cada cliente es diferente y que algunas de estas recomendaciones pueden aumentar el número de correos electrónicos legítimos clasificados como spam (falsos positivos).

Basic Setup (Configuración básica)

1. Asegúrese de que Anti-Spam esté activado:

   Asegúrese de que todos los registros MX (incluida la prioridad más baja) estén reenviando correo a través de los ESA.Asegúrese de que los dispositivos tienen una clave de característica Anti-Spam válida.Asegúrese de que Anti-Spam esté habilitado para todas las políticas de correo entrante apropiadas.

2. Compruebe que está recibiendo actualizaciones de reglas antispam. Verifique para confirmar que las marcas **más recientes** para las actualizaciones en Servicios de seguridad > Anti-Spam son de dentro de las últimas 2 horas.

3. Asegúrese de que Anti-Spam está analizando los mensajes:

   Verifique un ejemplo de mensajes de spam perdidos para el siguiente encabezado: Resultado de X-IronPort-Anti-Spam:Si falta ese encabezado:

   Asegúrese de que no dispone de entradas o filtros de lista permitida que hagan que el spam omita el análisis de spam (consulte a continuación).Verifique que los mensajes no se desvíen del escaneo porque exceden el tamaño máximo de escaneo de mensajes (el valor predeterminado es 262144 bytes). La reducción de esta configuración no mejora en gran medida el rendimiento y puede dar lugar a que se pierda SPAM. Durante una evaluación, también es importante asegurarse de que la configuración IPAS sea la misma que la de cualquier otro producto que se esté probando.Vaya a cada entrada de HAT y confirme que "spam_check=on" para todas las políticas de flujo de correo entrante. Siempre y cuando el valor predeterminado sea "spam_check= on" y ninguna de las políticas de flujo de correo lo desactive explícitamente, esto se configura correctamente. Preste especial atención a la

configuración TRUSTED/allowLIST. A menudo, los clientes añaden de forma involuntaria un remitente a su lista de permitidos que reenvía spam; por ejemplo, agregando el dominio de un ISP o partner que reenvía spam y correo electrónico legítimo al grupo de remitentes allowLIST.

Realice una revisión rápida a través de los filtros de mensajes para asegurarse de que no haya ningún filtro que "salte-spamcheck". Si la hay, asegúrese de que están haciendo lo que deberían (teniendo en cuenta que la coincidencia de un único destinatario puede coincidir en mensajes con más de 30 destinatarios).

Busque un ejemplo reciente de SPAM (hora, fecha, rcpt, etc.) y consulte los registros_de_correo para ver qué sucedió. Confirme que Anti-Spam devolvió un veredicto negativo.

4. Asegúrese de que está realizando las acciones deseadas en los mensajes spam positivos. Verifique las políticas de correo entrante para ver cómo se manejan los veredictos antispam. Asegúrese de que los mensajes SPAM positivos y sospechosos se eliminen o se pongan en cuarentena en la política predeterminada, y que todas las demás políticas utilicen el comportamiento predeterminado o invaliden deliberadamente el valor predeterminado.

5. Aplique umbrales de spam más agresivos si los falsos positivos son menos preocupantes que el spam perdido:

   Reduzca el umbral de spam positivo a 80 (el valor predeterminado es 90) si los falsos positivos no son una preocupación en el umbral "determinado".

   Reduzca el umbral de spam sospechoso a 40 (el valor predeterminado es 50) si los falsos positivos no constituyen una preocupación en el umbral de "sospechoso".

   Si la mayoría de las quejas de spam provienen de un subconjunto de destinatarios, puede crear una política de correo independiente para estos usuarios con umbrales de spam más bajos para filtrar más agresivamente sólo para estos destinatarios.

   Los cambios en estos valores no deben tomarse a la ligera, ni deben llevarse a cabo sin datos rigurosos para determinar cuáles serán los efectos repelentes.

   Además, no ajuste necesariamente los valores en la otra dirección sólo para evitar falsos positivos.Asegúrese de que los falsos positivos y los falsos negativos se envíen al TAC.

6. Optimice su configuración SBRS y sus políticas HAT:

   La mayoría de las organizaciones se sienten cómodas al agregar SBRS -10 a -3.0 a su lista de bloqueo y SBRS -3.0 a -1.0 a su lista de SOSPECHOSA. Los clientes más agresivos pueden bloquear SBRS -10 a -2.0 y agregar -2.0 a -0.6 a SUSPECTLIST.

   En algunos casos, el hecho de que un remitente aún no tenga una puntuación de reputación de SenderBase es evidencia de que este remitente puede ser un spammer. Puede agregar SBRS "none" directamente a un grupo de remitentes que obtenga la política "Throttled", por

ejemplo, a su grupo de remitentes SUSPECT.

Cambie el número máximo de destinatarios por hora a 5 para la política de aceleración.

Considere la posibilidad de crear más de una política de "aceleración" para aplicar diferentes límites de destinatarios por hora; por ejemplo, limitación de velocidad de remitentes con un SBRS entre -2 y -1 a 5 destinatarios por hora y remitentes con un SBRS entre -1 y 0 a 20 destinatarios por hora.

7. Habilitar verificación de remitente para la política de flujo de correo "acelerado":

   Los clientes pueden optar por agregar remitentes con DNS inexistente o mal configurado al grupo de remitentes SUSPECTLIST.

   El registro PTR del host de conexión no existe en DNS.La conexión de la búsqueda del registro PTR del host falla debido a una falla temporal de DNS.

   La búsqueda de DNS inverso (PTR) del host de conexión no coincide con la búsqueda de DNS de reenvío (A).

   Existe cierto riesgo de falsos positivos por parte de los remitentes con DNS mal configurado, por lo que es posible que los clientes deseen configurar una política de flujo de correo independiente que devuelva una respuesta 4xx personalizada que indique el motivo por el que se rechazan los mensajes.

   Consulte la ayuda en línea o la guía del usuario de AsyncOS para obtener más información sobre la verificación del remitente

8. Habilitar la aceptación LDAP y la protección contra ataques de recolección de directorios:

   Muchos spammers envían mensajes de correo electrónico a un gran número de direcciones no válidas, por lo que el bloqueo de remitentes que envían a destinatarios no válidos también puede reducir el spam.

   Si LDAP accept ya está activado, asegúrese de que Directory Harvest Protection (DHAP) también esté configurado para cada receptor entrante con un máximo de intentos no válidos entre 5 y 10 por IP.

9. Habilitar diccionarios de contenido:

   Su ESA incluye dos diccionarios de contenido: profanity.txt y sexual_content.txt. Aunque el uso de estos diccionarios puede generar falsos positivos, algunos clientes han descubierto que filtrar su flujo de correo por palabras inapropiadas puede reducir el riesgo de que la "persona equivocada" reciba el "correo electrónico equivocado". Estos filtros solo se pueden aplicar a las "ruedas chillonas" habilitándolas para un grupo de usuarios en una política de correo específica.

10. Informe mensajes mal clasificados al TAC de Cisco.

11. Para evitar un gran número de falsos positivos, el SBRS debe desactivarse para el escaneo saliente. Esto se debe a que SBRS observa la reputación de las IP entrantes y, en una red interna, la mayoría de estas IP son dinámicas. Siga los pasos de la siguiente sección.

Habilitar SBNP

1. Asegúrese de que el correo entrante y saliente se encuentren en receptores independientes.

2. Inhabilite las búsquedas de SenderBase para el correo saliente por debajo. Para hacerlo desde la GUI, vaya a Red > Listeners, seleccione cualquier receptor saliente, elija "Advanced" y desmarque la casilla junto a "Use SenderBase IP Profiles".

   La participación de red SenderBase (SBNP) puede aumentar significativamente la eficacia de los filtros de reputación, antispam y de brotes de virus. El SBNP tampoco tiene un impacto notable en el rendimiento si está habilitado al utilizar Anti-Spam y es muy seguro.

   Nota: El volumen de spam que recibe su organización cambiará con el tiempo. Es posible que más spam esté recibiendo a través de los ESA simplemente debido al hecho de que está recibiendo más spam que en el pasado. Puede realizar un seguimiento de este comportamiento a lo largo del tiempo en la página Descripción general del correo entrante y agregando los elementos de línea "Detención por filtrado de reputación" y "Mensajes de spam detectados".

Argumento de SBRS

La gran preocupación con los falsos positivos es que el correo electrónico importante podría perderse. En este contexto, la práctica de poner en cuarentena o rechazar el correo electrónico SPAM Positivo es problemática. Si se envía un correo electrónico legítimo a una cuarentena o a una carpeta de spam, se requiere una búsqueda proactiva para entrar y "notificar" que el correo no deseado se clasificó como spam.

Por el contrario, los correos electrónicos de lista de bloqueo y de velocidad limitada se bloquean de tal manera que se notifica inmediatamente al remitente. Si este remitente NO es un spammer, es probable que encuentre otra forma de ponerse en contacto con usted. De hecho, como política general, bloquear de forma predeterminada y después aceptar a partners de confianza cuando se les solicite es una mejor posición para algunas empresas.

La aceleración, si se establece correctamente, rara vez debe afectar a los partners, si es que alguna vez lo hace, pero proporcionará protección frente a los dominios que se infectan con virus. La aceleración también será desagradable para los spammers. Somos conscientes de una técnica de spammer para comprar grandes cantidades de IP, generar suficiente correo electrónico "bueno" para obtener una puntuación SBRS decente y luego empezar a enviar spam. Un rango de lista de sospechosos más grande debería detectarlos, limitar el daño que causan y eventualmente hacer que dejen de enviar spam a su dominio.