Lista de verificación de la eficacia del Anti-Spam del dispositivo de seguridad del correo electrónico de Cisco (ESA)

Contenido

Los siguientes procedimientos y las recomendaciones son “mejores prácticas” para reducir la cantidad de Spam que consigue con el ESA. Observe que cada cliente es diferente y que algunas de estas recomendaciones pueden aumentar el número de correos electrónicos legítimos clasificados como Spam (falsos positivos).

Configuración básica

1. Aseegurese el Anti-Spam se gira:

   Marque para aseegurarse que todos sus expedientes de los expedientes MX (prioridad baja incluyendo) MX están retransmitiendo el correo con los ESA.Aseegurese sus dispositivos tener las teclas de función válidas del Anti-Spam.Asegúrese que el Anti-Spam esté habilitado para todas las directivas apropiadas del correo entrante.

2. Verifique que usted esté recibiendo las actualizaciones de la regla del anti-Spam. Marque para confirmar que los sellos de fecha/hora **más recientes** para las actualizaciones bajo los Servicios de seguridad > el Anti-Spam son dentro del último 2 horas.

3. Aseegurese que los mensajes están siendo analizados por el Anti-Spam:

   Marque una muestra de mensajes spam faltados para la encabezado siguiente: X-IronPort-Anti-Spam-resultado:Si esa encabezado falta:

   Marque para aseegurarse le no tienen ningunas entradas o filtros de la lista blanca que hacen el Spam desviar la exploración del Spam (véase abajo).Marque para aseegurarse que los mensajes no están desviando la exploración porque exceden los mensajes del máximo analizan el tamaño (el valor por defecto es 262144 bytes). La reducción de esta configuración no mejora grandemente el funcionamiento y puede dar lugar al SPAM faltado. Durante una evaluación, es también importante aseegurarse los IPA que la determinación es lo mismo que cualquier otros Productos que son probados.Pasa a través de cada entrada del SOMBRERO y confirma que el “spam_check=on” para todas las directivas entrantes del flujo de correo. Mientras el valor por defecto tenga “spam_check= en”, y ningunas de las

directivas del flujo de correo lo apagan explícitamente, esto se configura correctamente. Especial atención de la paga a las configuraciones TRUSTED/WHITELIST. Mide el tiempo a menudo de los clientes agregan inadvertidamente un remitente a su lista blanca que esté remitiendo el Spam - por ejemplo, agregando el dominio de un ISP o el partner que adelante mande spam y legitime el correo electrónico al grupo del remitente WHITELIST.

Haga una verificación rápida a través de los filtros del mensaje para aseegurarse allí no son cualquier filtro que “salto-spamcheck”. Si hay, aseegurese lo están haciendo lo que él debe (teniendo presente que corresponde con un solo RCPT-a la coincidencia de la poder en los mensajes con los beneficiarios 30+).

Encuentre un ejemplo reciente del SPAM (hora, fecha, rcpt, etc.), y refiérase a los mail_logs para ver qué sucedió. Confirme que el Anti-Spam volvió un veredicto negativo.

4. Aseegurese le están tomando las acciones deseadas en los mensajes del positivo del Spam. Marque las directivas entrantes del correo para cómo se manejan los veredictos del Anti-Spam. Aseegurese el SPAM positivo y los mensajes sospechados se caen o quarantined en la política predeterminada, y ése el resto de las directivas utiliza el comportamiento predeterminado o reemplaza deliberadamente el valor por defecto.

5. Aplique umbrales más agresivos del Spam si los falsos positivos son menos de una preocupación que el Spam faltado:

   Reduzca el umbral positivo del Spam a 80 (el valor por defecto es 90) si los falsos positivos no son una preocupación en el “cierto” umbral.

   Reduzca el umbral sospechoso del Spam a 40 (el valor por defecto es 50) si los falsos positivos no son una preocupación en el umbral “sospechado”.

   Si la mayor parte de sus denuncias del Spam están viniendo de un subconjunto de beneficiarios, usted puede crear una directiva separada del correo para estos usuarios con umbrales más bajos del Spam para filtrar más agresivamente para apenas estos beneficiarios.

   Los cambios a estos valores no se deben tomar ligeramente, ni se deben ellos decretar sin ningunos datos duros para comprobar cuáles serán los efectos repurcussive.

   También, no ajuste necesariamente los valores en la otra dirección para evitar solamente los falsos positivos.Aseegurese por favor que los falsos positivos y las negativas falsas están sometidos a TAC.

6. Optimice sus configuraciones SBR y directivas del SOMBRERO:

   La mayoría de las organizaciones son SBR que agregan cómodos -10 a -3.0 a su lista negra y SBR -3.0 a 1.0 a su SUSPECTLIST. Clientes más agresivos pueden poner los SBR -10 a -2.0 y agregar -2.0 a -0.6 al SUSPECTLIST.

   En algunos casos, el hecho de que un remitente todavía no tenga una calificación de la

reputación de SenderBase es pruebas que este remitente puede ser un spammer. Usted puede agregar los SBR “ningunos” directamente a un grupo del remitente que consiga la directiva “estrangulamienta”, por ejemplo a su grupo SOSPECHADO del remitente.

Cambie al Número máximo de beneficiarios por la hora a 5 para la directiva “estrangulamienta”.

Consider que creaba más de una “estranguló” la directiva para aplicar a diverso beneficiario por los límites de la hora - por ejemplo valore la limitación de los remitentes con los SBR entre -2 y -1 a 5 beneficiarios por la hora y los remitentes con los SBR entre -1 y 0 a 20 beneficiarios por la hora.

7. Habilite la verificación del remitente para la directiva “estrangulamienta” de Mailflow:

   Los clientes pueden elegir agregar los remitentes con el DNS inexistente o incorrectamente configurado al grupo del remitente SUSPECTLIST.

   La conexión del expediente PTR del host no existe en el DNS.La conexión del host que la PTR registra las operaciones de búsqueda falla debido al error de DNS temporal.

   La conexión de la búsqueda de DNS reversible del host (PTR) no hace juego la búsqueda de DNS delantera (a).

   Hay un cierto riesgo de falsos positivos de los remitentes con el DNS mis configurado, así que los clientes pueden querer poner una directiva separada de Mailflow que vuelva una respuesta de la aduana 4xx que indica que los mensajes de la razón están rechazados.

   Marque la Ayuda en Línea o el guía del usuario de AsyncOS para más información sobre la verificación del remitente

8. El permiso LDAP protección valida y del ataque de recopilación de direcciones:

   Muchos spammeres envían los correos electrónicos a un número alto de direcciones no válidas, bloqueando tan a los remitentes que envían a los beneficiarios inválidos pueden también disminuir el Spam.

   Si el LDAP valida está ya encendido, se aseegura la protección de la cosecha del directorio (DHAP) también se configura para cada módulo de escucha entrante con los intentos inválidos máximos entre 5 y 10 por el IP.

9. Diccionarios contentos del permiso:

   Su ESA viene con dos diccionarios contentos: profanity.txt y sexual_content.txt. Mientras que usar estos diccionarios puede generar los falsos positivos, algunos clientes han encontrado que la filtración de su secuencia del correo para las palabras inadecuadas puede reducir el riesgo de la “persona incorrecta” que consigue el “correo electrónico incorrecto”. Estos filtros se pueden aplicar solamente a las “ruedas chillonas” habilitandolas para un grupo de usuarios en una directiva específica del correo.

10. Señale los mensajes clasificados equivocadamente al TAC de Cisco.

11. Para prevenir un gran número de falsos positivos, los SBR se deben inhabilitar para la exploración saliente. Esto es porque los SBR miran la reputación de los IP entrantes, y en una red interna, la mayor parte de estos IP son dinámicos. Siga los pasos en la siguiente sección.

Habilite SBNP

1. Aseegurese entrante y el correo saliente está en los módulos de escucha separados.

2. Inhabilite las operaciones de búsqueda de SenderBase para el correo electrónico saliente por abajo. Para hacer esto del GUI, ir a la red > a los módulos de escucha, seleccionar a cualquier módulo de escucha saliente, elegir “avanzó” y desmarca el cuadro al lado “del IP de SenderBase del uso que perfilaba”.

   La participación de la red de SenderBase (SBNP) puede aumentar perceptiblemente la eficacia de los filtros de la reputación, del Anti-Spam y de los filtros del brote de virus. SBNP también no tiene ningún notable impacto del rendimiento si es habilitado al usar el Anti-Spam y es altamente seguro.

Observe que el volumen de Spam que su organización recibe cambiará en un cierto plazo. Es posible que más Spam está consiguiendo con los ESA simplemente debido al hecho de que usted esté recibiendo más Spam que en el pasado. Usted puede seguir este comportamiento en un cierto plazo mirando la página de la descripción del correo entrante y agregando “parado por la filtración de la reputación” y los elemntos de línea detectados los “mensajes spam”.

Fundamento SBR

La preocupación grande con los falsos positivos es que el correo electrónico importante podría conseguir perdido. En este contexto, la práctica del correo electrónico positivo Quarantining o de caída del SPAM es problemática. Si un correo electrónico legítimo se envía a una cuarentena o a una carpeta de correo no deseado, requiere una búsqueda dinámica entrar y “note” que el ham fue clasificado equivocadamente como Spam.

En cambio, se bloquean los correos electrónicos de la lista negra y de la tarifa limitada de una manera tal que el remitente se notifique inmediatamente. Si este remitente no es un spammer, encontrarán probablemente otra manera de hacer el contacto con usted. De hecho, como política general, bloqueando por abandono y después validar a los Partners de confianza a petición, es una mejor posición para algunos negocios.

El estrangular, si está fijado correctamente, debe raramente si nunca los Partners de la influencia, pero proporcionan la protección contra los dominios que consiguen infectados con los virus. El estrangular también será desalentador a los spammeres. Somos conscientes de una técnica del spammer comprar un gran número de IP, generamos bastante “buen” correo electrónico para conseguir una calificación decente SBR y después para comenzar a mandar spam. Un rango sospechado más grande de la lista debe coger éstos, limita el daño que hacen y puede hacerlos eventual parar el enviar del Spam a su dominio.