Cisco envia por correio eletrónico a lista de verificação da eficácia do Anti-Spam da ferramenta de segurança (ESA)

Índice

Os seguintes procedimentos e recomendações são “melhores prática” para reduzir a quantidade de Spam que obtém com o ESA. Note que cada cliente é diferente e que algumas destas recomendações podem aumentar o número de email legítimos classificados como o Spam (falsos positivos).

Instalação básica

1. Certifique-se que o Anti-Spam está girado sobre:

   Verifique para certificar-se de que todos seus registros dos registros MX (que incluem a baixa prioridade) MX estão retransmitindo o correio com os ESA.Certifique-se de seus dispositivos ter uma chave de recurso válida do Anti-Spam.Assegure-se de que o Anti-Spam esteja permitido para todas as políticas apropriadas do correio recebido.

2. Verifique que você está recebendo atualizações da regra do anti-Spam. Verifique para confirmar que os selos de tempo **os mais recentes** para atualizações sob Serviços de segurança > Anti-Spam se realizam de dentro das últimas 2 horas.

3. Certifique-se de que as mensagens estão sendo feitas a varredura pelo Anti-Spam:

   Verifique uma amostra de mensagens faltadas do Spam para ver se há o seguinte encabeçamento: X-IronPort-Anti-Spam-resultado:Se esse encabeçamento falta:

   Verifique para certificar-se você não tem nenhuns entradas ou filtros de Whitelist que fazem com que o Spam contorneie a exploração do Spam (veja abaixo).Verifique para certificar-se de que as mensagens não estão contorneando a exploração porque excedem o tamanho da varredura das mensagens do máximo (o padrão é 262144 bytes). Reduzir este ajuste não melhora extremamente o desempenho e pode conduzir ao Spam faltado. Durante uma avaliação, é igualmente importante certificar-se que o ajuste IPA é o mesmo como algum outro Produtos que está sendo testado.Atravessa cada entrada do CHAPÉU e confirma que o “spam_check=on” para todas as políticas de entrada do fluxo de correio. Enquanto o padrão tem o “spam_check= em”, e nenhumas das políticas do fluxo de correio o desligam

explicitamente, esta está configurada corretamente. Atenção especial do pagamento aos ajustes TRUSTED/WHITELIST. Cronometra frequentemente clientes adicionam inadvertidamente um remetente a seu Whitelist que está encaminhando o Spam - por exemplo, adicionando o domínio de um ISP ou de um sócio que encaminhem o Spam e o email legítimo ao grupo do remetente WHITELIST.

Faça uma verificação rápida através dos filtros da mensagem para certificar-se que não há nenhuns filtros que “faixa clara-spamcheck”. Se há, certifique-se que estão fazendo o que devem (se mantendo na mente que que combina um único RCPT-ao fósforo da lata em mensagens com os receptores 30+).

Encontre um exemplo recente Spam (hora, data, rcpt, etc.), e proveja os mail_logs para ver o que aconteceu. Confirme que o Anti-Spam retornou uma sentença negativa.

4. Certifique-se que você está tomando as ações desejadas em mensagens do positivo do Spam. Verifique as políticas de entrada do correio para ver se há como as sentenças do Anti-Spam são seguradas. Certifique-se que mensagens positivas e suspeitas Spam está deixado cair ou quarantined na política padrão, e que todas políticas restantes usam o comportamento padrão ou deliberadamente cancelam o padrão.

5. Aplique uns pontos iniciais mais agressivos do Spam se os falsos positivos são menos de um interesse do que o Spam faltado:

   Reduza o ponto inicial positivo do Spam a 80 (o padrão é 90) se os falsos positivos não são um interesse no “determinado” ponto inicial.

   Reduza suspeitou o ponto inicial do Spam a 40 (o padrão é 50 pés) se os falsos positivos não são um interesse no ponto inicial “suspeito”.

   Se a maioria de suas queixas do Spam estão vindo de um subconjunto dos receptores, você pode criar uma política separada do correio para estes usuários com os mais baixos pontos iniciais do Spam a fim filtrar mais agressivelmente para apenas estes receptores.

   As mudanças a estes valores não devem ser tomadas levemente, nem devem elas ser decretadas sem nenhuns dados duros para verificar o que os efeitos repurcussive serão.

   Também, não ajuste necessariamente valores no outro sentido para evitar somente falsos positivos.Certifique-se por favor de que os falsos positivos e os falsos negativos estão submetidos ao TAC.

6. Aperfeiçoe seus ajustes SBR e políticas do CHAPÉU:

   A maioria de organizações são SBR adicionando confortáveis -10 a -3.0 a sua lista negra e SBR -3.0 1.0 a seu SUSPECTLIST. Uns clientes mais agressivos podem põr SBR -10 a -2.0 e adicionar -2.0 a -0.6 ao SUSPECTLIST.

   Em alguns casos, o fato de que um remetente não tem ainda uma contagem da reputação de SenderBase é evidência que este remetente pode ser um spammer. Você pode adicionar

SBR “nenhuns” diretamente a um grupo do remetente que obtenha a política “estrangulada”, por exemplo a seu grupo SUSPEITO do remetente.

Mude o número máximo de receptores pela hora a 5 para a política “estrangulada”.

Consider que cria mais de uma “estrangulou” a política para reforçar o receptor diferente por limites da hora - por exemplo avalie a limitação de remetentes com SBR entre -2 e -1 aos receptores 5 pela hora e aos remetentes com SBR entre -1 e 0 a 20 receptores pela hora.

7. Permita a verificação do remetente para a política “estrangulada” de Mailflow:

   Os clientes podem escolher adicionar remetentes com o DNS inexistente ou impropriamente configurado ao grupo do remetente SUSPECTLIST.

   Conectar o registro PTR do host não existe no DNS.Conectar o host que o PTR grava a consulta falha devido à falha de DNS provisória.

   Conectar a pesquisa de DNS reversa do host (PTR) não combina a pesquisa de DNS dianteira (a).

   Há algum risco de falsos positivos dos remetentes com DNS desconfigurado, assim que os clientes podem querer setup uma política separada de Mailflow que retorne uma resposta do costume 4xx que indica que as mensagens da razão estão rejeitadas.

   Verifique a ajuda online ou o Guia do Usuário de AsyncOS para obter mais informações sobre da verificação do remetente

8. Permita o LDAP proteção do ataque aceitam e dos colheitas do diretório:

   Muitos spammer enviam email a um alto número de endereços inválidos, obstruindo assim os remetentes que enviam aos receptores inválidos podem igualmente diminuir o Spam.

   Se o LDAP aceita é já sobre, se certifica que a proteção da colheita do diretório (DHAP) está configurado igualmente para cada ouvinte de entrada com tentativas inválidas máximas entre 5 e 10 pelo IP.

9. Permita dicionários satisfeitos:

   Seu ESA vem com os dois dicionários satisfeitos: profanity.txt e sexual_content.txt. Quando usar estes dicionários puder gerar falsos positivos, alguns clientes encontraram que filtrar seu córrego do correio para palavras impróprias pode reduzir o risco “da pessoa errada” que recebe “o email errado”. Estes filtros podem somente ser aplicados “às rodas sibilantes” permitindo as para um grupo de usuários em uma política específica do correio.

10. Relate mensagens MIS-classificadas ao tac Cisco.

11. Para impedir um grande número falsos positivos, os SBR devem ser desabilitados para a exploração de partida. Isto é porque os SBR olham a reputação do IPs entrante, e em uma

rede interna, a maioria destes IPs são dinâmicos. Siga as etapas na próxima seção.

Permita SBNP

1. Certifique-se que do correio de entrada e de partida esteja em ouvintes separados.

2. Desabilite consultas de SenderBase para o email de partida por abaixo. Para fazer isto do GUI, para ir à rede > aos ouvintes, para selecionar todos os ouvintes de partida, para escolher “avançou” e desmarca a caixa ao lado do “do IP de SenderBase uso que perfila”.

   A participação da rede de SenderBase (SBNP) pode significativamente aumentar a eficácia de filtros da reputação, de Anti-Spam e de filtros da manifestação do vírus. SBNP igualmente não tem nenhum impacto no desempenho visível se permitido ao usar o Anti-Spam e é altamente seguro.

Note que o volume de Spam que sua organização recebe mudará ao longo do tempo. É possível que mais Spam está obtendo com os ESA simplesmente devido ao fato de que você está recebendo mais Spam do que no passado. Você pode seguir este comportamento ao longo do tempo olhando a página da vista geral do correio recebido e adicionando “parado pela filtração da reputação” e do “por itens de linha detectados mensagens Spam”.

Base racional SBR

Estar relacionado grande com falsos positivos é que o email importante poderia obter perdido. Neste contexto, a prática de Quarantining ou de deixar cair o email positivo Spam é problemática. Se um email legítimo é enviado a uma quarentena ou a um dobrador do Spam, exige uma busca dinâmica ir dentro e “observe” que o presunto misclassified como o Spam.

Ao contrário, a lista negra e os email do limite de taxa são obstruídos de tal maneira que o remetente é notificado imediatamente. Se este remetente não é um spammer, encontrarão provavelmente uma outra maneira de fazer o contato com você. De fato, como uma política total, obstruindo à revelia e então aceitar Parceiros confiados a pedido, é uma posição melhor para alguns negócios.

Estrangular, se ajustado corretamente, deve raramente se nunca os Parceiros da influência, mas fornecerão a proteção dos domínios que obtêm contaminados com vírus. Estrangular igualmente fora-estará pondo aos spammer. Nós estamos cientes de uma técnica do spammer comprar um grande número IP, geramos bastante “bom” email para obter uma contagem aceitável SBR e para começá-la então spamming. Uma escala suspeita maior da lista deve travar estes, limita o dano que fazem e pode eventualmente fazer com que parem de enviar o Spam a seu domínio.