Cisco e-mail security applicatie (ESR) - controlelijst voor demp-efficiëntie

Inhoud

Inleiding

De volgende procedures en aanbevelingen zijn "beste praktijken" voor het verminderen van de hoeveelheid spam die door de ESA wordt gepasseerd. Merk op dat elke klant anders is en dat sommige van deze aanbevelingen het aantal legitieme e-mails dat als spam (valse positieven) is geclassificeerd kunnen verhogen.

Basisinstelling

1. Controleer of de anti-spam ingeschakeld is:

   Controleer of al uw MX records (inclusief lagere prioriteit) MX-records via ESA's opnieuw e-mailen.Zorg ervoor dat uw apparatuur is voorzien van een geldige Anti-Spam optie-toets.Zorg ervoor dat Anti-Spam is ingeschakeld voor al uw juiste inkomende e-mailbeleid.

2. Controleer dat u anti-spam regelupdates ontvangt. Controleer of de **meest recente** tijdstempels voor updates onder Security Services > Anti-Spam in de afgelopen 2 uur zijn ontvangen.

3. Zorg ervoor dat de berichten door Anti-Spam worden gescand:

   Controleer een voorbeeld van gemiste spamberichten voor de volgende header: X-IronPort-anti-SPAM-resultaat:Als die header ontbreekt:

   Controleer of u geen toegestane items of filters hebt die spam veroorzaken om het scannen van spam te omzeilen (zie hieronder).Controleer of er geen berichten voorbij het scannen gaan omdat deze de maximale grootte van een bericht overtreffen (standaard 26214 bytes). Het verlagen van deze instelling verbetert de prestaties niet veel en kan resulteren in gemiste SPAM. Tijdens een evaluatie is het ook belangrijk om ervoor te zorgen dat de IPAS-instelling hetzelfde is als alle andere producten die worden getest.Ga door elke HAT ingang en bevestig dat "spam_check=on" voor al inkomende poststroombeleid. Zolang de standaardinstelling "spam_check= aan" heeft, en geen van de poststroombeleid het expliciet uitzet, wordt dit correct ingesteld. Let vooral op de instellingen TRUSTED/allowLIST. Vaak voegen klanten per ongeluk een zender toe aan hun allowlijst die spam door te sturen - bijvoorbeeld door het domein van een ISP of partner toe te voegen die zowel spam als

legitieme e-mail naar de allowLIST sender group doorstuurt.

Controleer de berichtfilters snel om te zien of er geen filters zijn die "spamcheck"overslaan. Als er iets is, zorg er dan voor dat ze doen wat ze zouden moeten (Houd er rekening mee dat het koppelen van één enkele CCPT-to berichten met meer dan 30 ontvangers kan vergelijken).

Vind een recent voorbeeld van SPAM (tijd, datum, recept, enz.), en verstuur de mail_logs om te zien wat er is gebeurd. Bevestig dat Anti-Spam een negatief vonnis heeft teruggegeven.

4. Zorg ervoor dat u de gewenste acties onderneemt op spam positieve boodschappen. Controleer het inkomende Mail-beleid hoe tegen Spam-oordelen worden behandeld. Zorg ervoor dat SPAM positieve en verdachte berichten in het standaardbeleid worden gedropt of in quarantaine geplaatst, en dat al het andere beleid of het standaardgedrag gebruikt of opzettelijk de standaard omzeilt.

5. Pas agressievere spamdrempels toe als valse positieven minder een zorg zijn dan gemiste spam:

   Verlaag de drempelwaarde voor positieve spam tot 80 (standaard 90) als valse positieven geen zorg zijn voor de "bepaalde" drempel.

   Verdachte spam Drempel terugbrengen naar 40 (standaard 50) als fout-positieven geen zorg zijn op de 'verdachte' drempel.

   Als de meeste van uw spamklachten afkomstig zijn van een deel van de ontvangers, kunt u een afzonderlijk postbeleid creëren voor deze gebruikers met lagere spamdrempels om agressiever te filteren voor slechts deze ontvangers.

   Wijzigingen in deze waarden mogen niet licht worden doorgevoerd en mogen ook niet zonder harde gegevens worden doorgevoerd om na te gaan wat de herzuiverende effecten zullen zijn.

   Pas niet per se alleen waarden in de andere richting aan om valse positieve kanten te voorkomen.Zorg ervoor dat valse positieve en verkeerde negatieve kanten aan TAC worden voorgelegd.

6. Optimaliseer uw SBRS-instellingen en HAT-beleid:

   De meeste organisaties vinden het leuk om SBRS -10 tot -3.0 aan hun Blocklist en SBRS -3.0 tot -1.0 aan hun SUSPECTLIST toe te voegen. agressievere klanten kunnen SBRS -10 tot -2.0 blokkeren en -2.0 tot -0.6 aan het USPECTLIST toevoegen.

   In sommige gevallen is het feit dat een afzender nog geen SenderBase Reputation Score heeft bewijs dat deze zender een spammer kan zijn. U kunt SBRS "niets" direct toevoegen aan een sendergroep die het "Geloven" beleid krijgt, bijvoorbeeld aan uw SUSPECT sendergroep.

Verander het maximum aantal ontvangers per uur naar 5 voor het "Geloven" beleid.

Overweeg het creëren van meer dan één ‘gedraaid' beleid om verschillende ontvangers per uur limieten af te dwingen - bijvoorbeeld het beperken van tarieven bij verzenden met een SBRS tussen -2 en -1 tot 5 ontvangers per uur en zenders met een SBRS tussen -1 en 0 tot 20 ontvangers per uur.

7. Sender Verificatie inschakelen voor het "Gedrukte" poststroombeleid:

   Klanten kunnen ervoor kiezen om zenders met niet-bestaande of niet correct geconfigureerde DNS aan de SUSPECTLIST-verzendgroep toe te voegen.

   Het aansluiten van PTR-host-record bestaat niet in DNS.Het aansluiten van het PTR-opnameverzicht op host verloopt niet vanwege tijdelijke DNS-storing.

   Connected host reverse DNS-lookup (PTR) komt niet overeen met de voorwaartse DNS-raadpleging (A).

   Er is een risico van valse-positieven van zenders met verkeerd-gevormde DNS, zodat kunnen de klanten een afzonderlijk beleid van de Brievenflow willen opstellen dat een aangepaste 4xx reactie terugkeert die de reden aangeeft dat de berichten worden verworpen.

   Controleer de online Help of AsyncOS-gebruikershandleiding voor meer informatie over verificatie van verzenders

8. Attack Protection voor LDAP accepteren en Directory Harvest inschakelen:

   Veel spammers verzenden e-mails naar een groot aantal ongeldige adressen, dus het blokkeren van zenders die naar ongeldige ontvangers sturen kan ook spam verminderen.

   Als LDAP Accepteer al is ingeschakeld, zorg er dan voor dat DHAP (Directory Harvest Protection) ook wordt ingesteld voor elke inkomende luisteraar met maximale ongeldige pogingen tussen 5 en 10 per IP.

9. Woordenboeken voor inhoud inschakelen:

   Uw ESA bestaat uit twee inhoudswoordenboeken: profanity.txt en sexueel_content.txt. Hoewel het gebruik van deze woordenboeken valse positieven kan opleveren, hebben sommige klanten ontdekt dat het filteren van hun mailstream voor onjuiste woorden het risico kan verkleinen dat de "verkeerde persoon" de "verkeerde e-mail" krijgt. Deze filters mogen alleen worden toegepast op de "krakkemikkige wielen" door ze voor een groep gebruikers in een specifiek postbeleid toe te staan.

10. Rapport niet-geclassificeerde berichten naar Cisco TAC.

11. Om een groot aantal valse positieven te voorkomen, moet SBRS worden uitgeschakeld voor het uitgaande scannen. Dit komt doordat SBRS de reputatie van inkomende IP's

bekijkt, en in een intern netwerk zijn de meeste van deze IP's dynamisch. Volg de stappen in het volgende gedeelte.

SBNP inschakelen

1. Zorg ervoor dat de inkomende en uitgaande post op afzonderlijke luisteraars zijn.

2. Uitschakelen van SenderBase raadpleging voor uitgaande e-mail per hieronder. Om dit vanuit de GUI te doen, ga naar Netwerk > Lijsten, selecteer om het even welke uitgaande luisteraars, kies "Geavanceerd" en uncheck het vakje naast "Gebruik het Profileren van SenderBase IP".

   SenderBase Network Participation (SBNP) kan de effectiviteit van Reputation Filters, Anti-Spam en Filters voor Uitsplitsing naar virus aanzienlijk verhogen. SBNP heeft ook geen merkbare impact op de prestaties als het wordt ingeschakeld bij gebruik van Anti-Spam en is zeer veilig.

   Opmerking: Het volume van spam dat uw organisatie ontvangt zal in de loop der tijd veranderen. Het is mogelijk dat de ESA's meer spam vertonen, eenvoudigweg omdat u meer spam ontvangt dan in het verleden. U kunt dit gedrag in de loop der tijd volgen door de pagina Inkomend Mail Overzicht te bekijken en de opties "geblokkeerd door reputatie filteren" en "spam berichten gedetecteerd" toe te voegen.

SBRS-rationeel

De grote zorg met False Positives is dat belangrijke e-mail verloren kan gaan. In deze context is het moeilijk om een positief e-mailadres van het SPAM in te vullen of af te geven. Als een legale e-mail wordt verstuurd naar een Quarantine of een spammap, dan moet er een pro-actieve zoekopdracht naar binnen gaan en "opmerken" dat ham verkeerd is geclassificeerd als spam.

In tegenstelling tot blocklist en snelheidsbeperkte e-mails worden zo geblokkeerd dat de afzender onmiddellijk op de hoogte wordt gebracht. Als deze afzender GEEN spammer is, zullen zij waarschijnlijk een andere manier vinden om contact met u te maken. In feite is het als algemeen beleid, door default te blokkeren en vervolgens op verzoek vertrouwde partners aan te nemen, een betere positie voor sommige bedrijven.

Als het goed wordt ingesteld, zal het roteren zelden de partners beïnvloeden, maar zal het bescherming bieden tegen domeinen die besmet raken met virussen. De rotting zal ook de spammers buiten schot houden. We zijn ons bewust van een spamertechniek om grote aantallen IP's te kopen, genoeg 'goede' e-mail te genereren om een fatsoenlijke SBRS-score te behalen en dan te beginnen met spammen. Een groter verdacht lijstbereik zou deze moeten vangen, de schade beperken die ze doen en het kan hen uiteindelijk veroorzaken om te stoppen met het verzenden van spam naar uw domein.