ESR-mailfiltering

Inhoud

[Inleiding](#)
[Probleem](#)
[Oplossing](#)
[Filters toepassen](#)
[Aanvullende maatregelen](#)

Inleiding

Dit document beschrijft een probleem dat op Cisco Email Security Appliance (ESA) wordt aangetroffen wanneer spam en frauduleuze e-mail het netwerk binnendringen.

Probleem

Fraudsters proberen e-mail te imiteren. Wanneer de e-mail een medewerker van het bedrijf imiteert (zogenaamd van), kan hij bijzonder bedrieglijk zijn en tot verwarring leiden. In een poging om dit probleem op te lossen, kunnen e-mailbeheerders proberen inkomende mail te blokkeren die vanuit het bedrijf (*gespoofde* mail) lijkt te ontstaan.

Het lijkt logisch dat als je de inkomende mail van het internet blokkeert dat het bedrijf het adres in de domeinnaam heeft, het het probleem oplost. Helaas, als je op deze manier e-mail blokkeert, kan het ook legale e-mail tegelijkertijd blokkeren. Bekijk deze voorbeelden:

- Een werknemer reist en gebruikt een Internet Service Provider (ISP) van het hotel dat alle Simple Mail Transfer Protocol (MTP)-verkeer op transparante wijze naar de ISP-mailservers doorstuurt. Wanneer e-mail wordt verzonden, kan het lijken dat het direct door de onderneming-MTP-server stroomt, maar het wordt eigenlijk verzonden door een derde-partij-MTP-server voordat het aan de onderneming wordt geleverd.

- Een medewerker tekent zich in op een e-maildiscussielijst. Wanneer berichten naar de e-maillijst worden verstuurd, worden ze naar alle abonnees teruggestuurd, blijkbaar van de originator.

- Een extern systeem wordt gebruikt om de prestaties of bereikbaarheid van extern zichtbare apparaten te bewaken. Wanneer er een melding wordt ontvangen, heeft de e-mail de domeinnaam van het bedrijf in het adres dat u wilt teruggeven. Serviceleveranciers van derden, zoals Webex, doen dit vrij vaak.

- Vanwege een tijdelijke fout in de netwerkconfiguratie, wordt de post van binnen het bedrijf verzonden via de inkomende luisteraar, in plaats van de uitgaande luisteraar.

- Iemand buiten het bedrijf ontvangt een bericht dat ze terugsturen naar het bedrijf met een Mail User Agent (MUA) dat nieuwe headers in plaats van de originele header gebruikt.

- Een op internet gebaseerde toepassing, zoals de **verzendpagina's** van de Federal Express of de Yahoo **e-mail** dit artikel pagina, maakt legitieme mail met een retouradres dat terugwijst naar het bedrijf. De post is legitiem en heeft een bronadres van binnenuit van het bedrijf, maar het komt niet van binnenuit.

Deze voorbeelden tonen aan dat als u inkomende mail op basis van de domeininformatie blokkeert, het in valse positieven kan resulteren.

Oplossing

In dit gedeelte worden de aanbevolen acties beschreven die u moet uitvoeren om dit probleem op te lossen.

Filters toepassen

Blokkeer de inkomende e-mail niet op basis van de domeininformatie om het verlies van legitieme e-mailberichten te voorkomen. In plaats daarvan, kunt u de onderwerpregel van deze types van berichten verbinden terwijl zij het netwerk binnengaan, wat aan de ontvanger aangeeft dat de berichten potentieel vervalst zijn. Dit kan met berichtfilters of met contentfilters worden verwezenlijkt.

De basisstrategie voor deze filters is om de achterwaarts gerichte lichaamskopregels (de **Van** gegevens is het belangrijkst) te controleren, evenals de RFC 821-geldzender. Deze headers worden meestal getoond in MUA's en zijn degene die waarschijnlijk het meest vervalst zullen worden door een frauduleus persoon.

Het berichtfilter in het volgende voorbeeld toont hoe u berichten kunt markeren die potentieel geïmpersoneerd zijn. Dit filter voert verschillende handelingen uit:

- Als de onderwerpregel reeds **" {Mogelijk Versmeerd}"** in het heeft**"**, dan wordt een andere kopie niet door het filter toegevoegd. Dit is belangrijk wanneer de antwoorden in de berichtstroom zijn opgenomen en een onderwerpregel kan meerdere malen via de mailgateway bewegen voordat een bericht-draad is voltooid.

- Dit filter zoekt naar de Envelope Sender of de **From** header die een adres heeft dat eindigt met de domeinnaam **@yourdomain.com**. Het is belangrijk om op te merken dat de mail-van-zoekopdracht automatisch hoofdlettergevoelig is, maar het zoeken van-header is niet voldoende. Als de domeinnaam in één van beide plaatsen wordt gevonden, voegt de filter toe **" {Mogelijk samengevoegd}"** aan het eind van de onderwerpregel.

Hier is een voorbeeld van het filter:

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
          (header("From") == "(?i)@yourdomain\\.com")
       {
           strip-header("Subject");
```

```
        insert-header("Subject", "$Subject {Possibly Forged}");
    }
}
```

Aanvullende maatregelen

Omdat er geen makkelijke manier is om gespoofde post van legitieme post te identificeren, is er geen manier om het probleem volledig op te lossen. Daarom raadt Cisco u aan IronPort Anti-Spam Scanning (IPAS) in te schakelen, die frauduleuze mail (phishing) of spam effectief identificeert en het positief blokkeert. Het gebruik van deze anti-spamscanner biedt, in combinatie met de filters die in de vorige sectie zijn beschreven, de beste resultaten zonder het verlies van legitieme e-mail.

Als u frauduleuze e-mails moet identificeren die in uw netwerk komen, dan moet u het gebruik van de Domain Keys Identified Mail (DKIM)-technologie overwegen; er zijn meer regels nodig , maar het is een goede maatregel tegen phishing en frauduleuze e - mails .

> Opmerking: Raadpleeg voor meer informatie over berichtfilters de **AsyncOS-gebruikershandleiding** op de pagina Cisco e-mail security applicatie.