Hoe u gesimuleerde phishing-perscampagnes via de Cisco e-mail security applicatie toestaat

Inhoud

Inleiding

In dit document worden de configuratiestappen in de Cisco Email Security Appliance (ESA) beschreven om gesimuleerde phishing-platforms met succes toe te staan.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Berichtings- en contentfilters maken op de ESA.
- Configuratie van de Host Access Tabel (HAT).
- Begrijpen met de inkomende e-mailleiding van Cisco ESA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Simulatie van phishing-platforms stelt beheerders in staat om phishing-campagnes te voeren als onderdeel van een cyclus om één van de grootste bedreigingen te beheersen die de e-mailsystemen gebruikt als een vector van sociale technische aanvallen.

Probleem

Wanneer de ESA niet voor dergelijke simulaties is voorbereid, is het niet ongebruikelijk dat zijn scanmotoren de phishing campagne-berichten stopzetten, wat resulteert in een storing of afname van de effectiviteit van de simulaties.

Oplossing

> **Voorzichtig:** In dit configuratievoorbeeld wordt *TRUSTED* mail flow-beleid geselecteerd om de ESA in staat te stellen door grotere gesimuleerde phishing campagnes zonder trotling. Doorlopende phishing-campagnes van grote omvang kunnen invloed hebben op de e-mailverwerkingsprestaties.

Om ervoor te zorgen dat de phishing campagne-boodschappen niet worden tegengehouden door een veiligheidscomponent van de ESR-configuratie, dient te worden geïnstalleerd.

1. Een nieuwe gebruikersgroep maken **GUI > Mail Policies > HAT Overzicht** en verbind het met *TRUSTED* mail flow beleid (anders kan een nieuw beleid met soortgelijke opties worden gecreëerd onder **GUI > Mail Policy > Mail Flow Policy**).
2. Voeg de verzendende host(s) of IP(s) van het gesimuleerde phishing platform toe aan deze Sender Group. Als het gesimuleerde phishing platform een groot bereik van IPs heeft, kunt u gedeeltelijke hostnamen in plaats daarvan of IP bereiken indien van toepassing toevoegen.
3. Beveel de Sender Group boven je *BLOCKLIST* Sender Group om er zeker van te zijn dat er eerder statistisch dan SBRS op wordt afgestemd.
4. Schakel alle beveiligingsfuncties voor het *TRUSTED* mail flow-beleid uit onder **GUI > Mail-beleid > Mail Flow-beleid > TRUSTED** (of uw nieuw gemaakte mail flow-beleid):

Security Features	
Spam Detection:	○ Use Default (On) ○ On ◉ Off
AMP Detection	○ Use Default (On) ○ On ◉ Off
Virus Protection:	○ Use Default (On) ○ On ◉ Off
Sender Domain Reputation Verification:	○ Use Default (On) ○ On ◉ Off
Virus Outbreak Filters:	○ Use Default (On) ○ On ◉ Off
Advanced Phishing Protection:	○ Use Default (On) ○ On ◉ Off
Graymail Detection:	○ Use Default (On) ○ On ◉ Off
Content Filters:	○ Use Default (On) ○ On ◉ Off
Message Filters:	○ Use Default (On) ○ On ◉ Off

5. **Breng deze wijzigingen aan en geef jezelf aan.**

Voorafgaande AsyncOS v.14

> **Voorzichtig:** In dit configuratievoorbeeld wordt *TRUSTED* mail flow-beleid geselecteerd om de ESA in staat te stellen door grotere gesimuleerde phishing campagnes zonder trotling. Doorlopende phishing-campagnes van grote omvang kunnen invloed hebben op de e-

mailverwerkingsprestaties.

Om ervoor te zorgen dat de phishing campagne-boodschappen niet worden tegengehouden door een veiligheidscomponent van de ESR-configuratie, dient te worden geïnstalleerd.

1. Een nieuwe gebruikersgroep maken **GUI > Mail Policies > HAT Overzicht** en binden het aan *TRUSTED* mail flow beleid.
2. Voeg de verzendende host(s) of IP(s) van het gesimuleerde phishing platform toe aan deze Sender Group. Als het gesimuleerde phishing platform een groot bereik van IPs heeft, kunt u gedeeltelijke hostnamen in plaats daarvan of IP bereiken indien van toepassing toevoegen.
3. Beveel de Sender Group boven je *BLOCKLIST* Sender Group om er zeker van te zijn dat er eerder statistisch dan SBRS op wordt afgestemd.
4. **Breng deze veranderingen in en begaan.**
5. Navigeer naar de CLI en voeg het nieuwe berichtfilter, **CLI > filters toe,** kopieer en wijzig de syntaxis en voegt het filter toe.
6.
```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```
7. Beveel het berichtfilter in de lijst om er zeker van te zijn dat het niet wordt overgeslagen door een ander berichtfilter erboven, dat ook de skip-filters actie omvat.
8. Druk op ENTER-toets om terug te navigeren naar de hoofdcommandoprompt van AsyncOS en geef de opdracht "**toegewijd**" uit om de wijzigingen vast te leggen. (klik niet op CTRL+C - alle wijzigingen worden gewist).
9. Navigeren in naar het **beleid GUI> Mail > Inkomend contentfilters**
10. Maak een nieuw Inkomend contentfilter met toestand ***"Overige header"*** ingesteld om naar de aangepaste kop **"x-sp"** te zoeken en naar de *unieke waarde* die is ingesteld in het berichtenfilter en stel de actie ***Niet resterende contentfilters in (Eindactie)***.
11. Bestellen het filter van de inhoud aan "1" om ervoor te zorgen dat andere filters geen actie tegen het gesimuleerde phishing bericht zullen ondernemen.
12. Navigeren in op **GUI > Mail-beleid > inkomend postbeleid** en het contentfilter toewijzen aan het gewenste beleid.
13. **Breng veranderingen in en begaan.**
14. Start de gesimuleerde phishing platform campagne en controleer de mail_logs/Message Tracking om stroom en beleidsregels bij elkaar te brengen.