Simulierte Phishing-Plattformkampagnen über die Cisco Email Security Appliance

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfigurationsschritte auf der Cisco E-Mail Security Appliance (ESA), um simulierte Phishing-Plattformen-Kampagnen erfolgreich zu ermöglichen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Erstellung von Message- und Content-Filtern auf der ESA.
- Konfiguration der Host Access Table (HAT).
- Verständnis der eingehenden E-Mail-Pipeline der Cisco ESA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Simulierte Phishing-Plattformen ermöglichen es Administratoren, Phishing-Kampagnen als Teil eines Zyklus durchzuführen, um eine der größten Bedrohungen zu bewältigen, die die E-Mail-Systeme als Vektor für Social Engineering-Angriffe nutzt.

Problem

Wenn die ESA nicht für solche Simulationen vorbereitet ist, ist es nicht ungewöhnlich, dass ihre Scan-Engines die Phishing-Kampagnennachrichten stoppen, was zu einem Ausfall oder einer Abnahme der Wirksamkeit der Simulationen führt.

Lösung

> **Vorsicht:** In diesem Konfigurationsbeispiel wird eine *TRUSTED* Mail Flow-Richtlinie ausgewählt, die es der ESA ermöglicht, größere simulierte Phishing-Kampagnen ohne Einschränkung zu durchlaufen. Die Durchführung fortlaufender Phishing-Kampagnen mit hohem Volumen kann sich negativ auf die Leistung der E-Mail-Verarbeitung auswirken.

Um sicherzustellen, dass die Phishing-Kampagnenmeldungen nicht von einer Sicherheitskomponente der ESA-Konfiguration gestoppt werden, muss eine Sicherheitskomponente eingerichtet werden.

1. Neue Absendergruppe erstellen: **GUI > Mail Policies > HAT Overview** und binden sie an *TRUSTED* Mail Flow Policy (alternativ kann eine neue Richtlinie mit ähnlichen Optionen unter **GUI > Mail Policies > Mail Flow Policies** erstellt werden).
2. Fügen Sie den bzw. die sendenden Host(s) oder IP(s) der simulierten Phishing-Plattform dieser Absendergruppe hinzu. Wenn die simulierte Phishing-Plattform über eine große Anzahl von IP-Adressen verfügt, können Sie stattdessen partielle Hostnamen oder ggf. IP-Bereiche hinzufügen.
3. Bestellen Sie die Absendergruppe über Ihrer *BLOCKLIST*-Absendergruppe, um sicherzustellen, dass sie statisch statt SBRS zugeordnet wird.
4. Deaktivieren Sie alle Sicherheitsfunktionen für die *TRUSTED* Mail Flow-Richtlinie unter **GUI > Mail Policies > Mail Flow Policies > TRUSTED** (oder Ihre neu erstellte Mail Flow-Richtlinie):

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. **Senden Sie diese Änderungen und bestätigen Sie sie.**

Vorherige AsyncOS v.14

> **Vorsicht:** In diesem Konfigurationsbeispiel wird eine *TRUSTED* Mail Flow-Richtlinie

ausgewählt, die es der ESA ermöglicht, größere simulierte Phishing-Kampagnen ohne Einschränkung zu durchlaufen. Die Durchführung fortlaufender Phishing-Kampagnen mit hohem Volumen kann sich negativ auf die Leistung der E-Mail-Verarbeitung auswirken.

Um sicherzustellen, dass die Phishing-Kampagnenmeldungen nicht von einer Sicherheitskomponente der ESA-Konfiguration gestoppt werden, muss eine Sicherheitskomponente eingerichtet werden.

1. Neue Absendergruppe erstellen: **GUI > Mail Policies > HAT Overview** und binden sie an *TRUSTED* Mail Flow Policy.
2. Fügen Sie den bzw. die sendenden Host(s) oder IP(s) der simulierten Phishing-Plattform dieser Absendergruppe hinzu. Wenn die simulierte Phishing-Plattform über eine große Anzahl von IP-Adressen verfügt, können Sie stattdessen partielle Hostnamen oder ggf. IP-Bereiche hinzufügen.
3. Bestellen Sie die Absendergruppe über Ihrer *BLOCKLIST*-Absendergruppe, um sicherzustellen, dass sie statisch statt SBRS zugeordnet wird.
4. **Senden Sie diese Änderungen und bestätigen Sie sie.**
5. Navigieren Sie zur CLI, und fügen Sie einen neuen Nachrichtenfilter, **CLI > Filter,** kopieren und ändern Sie die Syntax, und fügen Sie den Filter hinzu.
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. Bestellen Sie den Nachrichtenfilter in der Liste nach oben, um sicherzustellen, dass er nicht von einem anderen Nachrichtenfilter übersprungen wird, der die Aktion "Überspringen" beinhaltet.
8. Drücken Sie die Eingabetaste, um zurück zur Hauptbefehlsaufforderung von AsyncOS zu navigieren, und geben Sie den Befehl "**commit**" (**Bestätigung**) aus, um die Änderungen zu bestätigen. (Klicken Sie nicht auf STRG+C - es werden alle Änderungen gelöscht).
9. Navigieren Sie zu **GUI > Mail Policies > Incoming Content Filters.**
10. Erstellen Sie einen neuen Filter für eingehende Inhalte mit der Bedingung ***"Other Header"***, dass Sie nach dem benutzerdefinierten Header **"x-sp"** und seinem *einzigartigen Wert* im Nachrichtenfilter suchen und die Aktion ***Überspringen verbleibender Inhaltsfilter (abschließende Aktion)*** konfigurieren.
11. Bestellen Sie den Content-Filter auf "1", um sicherzustellen, dass andere Filter keine Maßnahmen gegen die simulierte Phishing-Nachricht ergreifen.
12. Navigieren Sie zu **GUI > Mail Policies > Incoming Mail Policies (Benutzeroberflächen > Mail-Policys > Richtlinien für eingehende E-Mails)**, und weisen Sie den Content-Filter der erforderlichen Richtlinie zu.
13. **Änderungen senden und bestätigen.**

14. Führen Sie die simulierte Phishing-Plattformkampagne aus, und überwachen Sie die Mail_logs/Message Tracking, um die Übereinstimmung von Fluss- und Richtlinienregeln zu überprüfen.