Häufige Konfigurationsfehler auf der ESA

Inhalt

Einführung

Dieses Dokument beschreibt häufige Konfigurationsfehler auf E-Mail Security Appliance (ESA).

Welche häufigen Konfigurationsfehler gibt es auf der ESA?

Unabhängig davon, ob Sie eine neue Evaluierung einrichten oder eine vorhandene Konfiguration überblicken, können Sie auf diese Checkliste mit häufigen Konfigurationsfehlern zurückgreifen.

HAT

- Legen Sie keine positiven SBRS-Bewertungen wie +5 oder +7 in die ALLOWLIST. Ein Bereich von 9.0-10.0 wäre in Ordnung, aber wenn Sie niedrigere Bewertungen haben, wird es nur wahrscheinlicher, dass Spam durchkommt.
- Deaktivieren Sie die DNS-Verifizierung für UNKNOWNLIST, Umschlagabsender, und stellen Sie eine Verbindung her, sofern Sie diese nicht wirklich benötigen und verstehen.
- Anstatt die Nachrichtengröße und andere Richtlinieneinstellungen in jeder Mail Flow Policy zu ändern, gehen Sie zum Menü Mail Flow Policies (Mail-Flow-Richtlinien), und wählen Sie die letzte Option, "Default Policy Parameters" (Standardrichtlinienparameter) aus.
- Die maximale Anzahl an Verbindungen für die meisten Absender auf drei zu beschränken und dies als Standard für neue Mail Flow-Richtlinien festzulegen.
- Stellen Sie sicher, dass SenderBase-Werte zwischen -10,0 und -2,0 in der BLOCKLIST enthalten sind. Die Dokumentations- und Einrichtungsassistenten sind zu konservativ. in diesem Bereich gibt es derzeit keine Fehlalarme.

Richtlinie

- Benennen Sie Richtlinien, nachdem Sie sie erhalten, und nicht, was Sie tun. Benennen Sie alle Content-Filter nach dem, was sie tun, und verwenden Sie Abkürzungen wie Q_basic_Attachments, D_spoofers, Strip_Multi-Media, wobei Q für Quarantäne und D für Drop

steht.
- Nicht standardmäßige Richtlinien sollten "Use Default Settings" (Standardeinstellungen verwenden) für Anti-Spam, Anti-Virus, Content-Filter und Outbreak-Filter verwenden, außer wenn Sie wirklich spezielle Einstellungen benötigen. Stellen Sie diese Einstellungen nicht in den einzelnen Richtlinien wieder her, wenn dies nicht erforderlich ist.
- Deaktivieren Sie "Infizierte Anhänge löschen", oder geben Sie viele leere E-Mails weiter, in denen der Virus entfernt wurde.
- Anti-Virus-Einstellungen für ausgehenden Datenverkehr müssen den Absender benachrichtigen, nicht den Empfänger.
- Outbreak-Filter und Anti-Spam sollten beim ausgehenden Datenverkehr deaktiviert werden.

Eingehende Relays

Wenn "Monitor > Overview" (Überwachung > Übersicht) Verbindungen von Ihren eigenen Servern und Domänen anzeigt, müssen Sie diese der Einrichtung für eingehende Relays hinzufügen. Ein sehr häufiger Fehler bei der Verwendung der GUI besteht darin, zu glauben, dass Sie die Funktion "Eingehendes Relay" aktiviert haben, wenn Sie nur die Einträge zur Tabelle hinzufügen. Darüber hinaus:

- Fügen Sie für diese eine spezielle HAT-Absendergruppe hinzu, oben ZULÄSSIG, für Berichtszwecke. Wählen Sie keine Ratenbeschränkung oder DHAP, aber Spam und Virenerkennung sind in Ordnung.
- Fügen Sie einen Nachrichtenfilter hinzu, der der BLOCKLIST-Richtlinienaktion entspricht. Beispiel:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

In seltenen Fällen, in denen Sie E-Mails erneut injizieren (z. B. die Weiterverarbeitung von E-Mails zwischen Abonnenten über die Richtlinie für eingehende E-Mails), muss Ihr Filter auch die Schnittstelle für die Zurückweisung ausnehmen. Normalerweise ist dies nicht notwendig.

DNS

Viele Kunden zwingen die ESA, ihre internen DNS-Server aus Gewohnheit abzufragen. In den meisten Installationen befinden sich 100 % der DNS-Datensätze, die wir benötigen, im Internet und nicht im internen DNS. Es ist sinnvoller, die Internet-Root-Server abzufragen und so die Weiterleitungslast auf dem internen DNS zu reduzieren.

Filter für Nachrichten und Inhalte

Der häufigste Fehler besteht darin, Zuordnungsbedingungen in Content-Filtern einzufügen, wenn diese nicht erforderlich sind. Die meisten Filter sollten einige Aktionen auflisten, aber die Bedingung sollte leer bleiben. Der Filter ist immer *wahr* und wird immer ausgeführt. Sie steuern, welche Benutzer/Richtlinien diese Aktionen empfangen, indem Sie nach Bedarf neue Richtlinien für eingehende oder ausgehende E-Mails erstellen und diesen Filter auf die Richtlinie anwenden. Die folgenden Beispiele sind falsch und korrekt:

- Es ist fast immer ein Fehler, den Zustand rcpt-to in einem Nachrichtenfilter zu verwenden. Das richtige Verfahren besteht darin, einen Filter für eingehende Inhalte zu schreiben und diesen für einen bestimmten Benutzer durch Hinzufügen einer empfängerbasierten Richtlinie für eingehende E-Mails zu spezifizieren.
- Es ist fast immer ein Fehler, einen Content-Filter-Test auf das Vorhandensein einer Anlage zu führen und dann die Anlage zu verwerfen. Die richtige Methode besteht darin, diese Anlage immer zu löschen, ohne ihre Anwesenheit zu testen.
- Es ist fast immer ein Fehler bei der Verwendung von deliver(). Bereitstellung bedeutet, alle verbleibenden Filter zu überspringen und dann zu liefern. Wenn Sie nur liefern möchten, ohne die übrigen Filter zu überspringen, ist keine explizite Aktion erforderlich (implizite Bereitstellung).

Open Relay Prevention

Einige Dienste prüfen, ob Ihr Message Transfer Agent (MTA) Adressen akzeptiert, die möglicherweise zu offenen Relay-Bedingungen führen können. Da das Verlassen der MTA als funktionierendes offenes Relay schlecht ist, können diese Sites Sie zu einer BLOCKLIST hinzufügen, es sei denn, Sie lehnen diese gefährlichen Adressen in der SMTP-Konversation ab.

Fügen Sie für diese eine spezielle HAT-Absendergruppe hinzu, oben ZULÄSSIG, für Berichtszwecke. Wählen Sie keine Ratenbeschränkung oder DHAP, sondern lassen Sie Spam und Viren erkennen.

- Ändern Sie die Einstellung in Strict Address Parsing (Lose ist die Standardeinstellung). Dies ist notwendig, um doppelte @-Zeichen in Adressen zu verhindern.
- Ungültige Zeichen ablehnen (nicht entfernen). Dies ist auch notwendig, um doppelte @-Zeichen in Adressen zu verhindern.
- Literale ablehnen und folgende Zeichen eingeben: *%!\/?

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems