Wie speichere ich Kopien von Nachrichten, die von meinem Nachrichtenfilter abgeglichen wurden?

Inhalt

Frage:

Wie speichere ich Kopien von Nachrichten, die von meinem Nachrichtenfilter abgeglichen wurden?

Antwort:

Es gibt mehrere Möglichkeiten, Kopien von Nachrichten beizubehalten, die einem Nachrichtenfilter zugeordnet sind.

Die Filter-Aktion Archive-Nachricht archiviert eine Kopie der Nachricht in einer Protokolldatei auf der ESA im UNIX-mbox-Dateiformat (ein sehr einfaches Textformat). Nach der Erstellung kann die Protokolldatei mit dem `filters->logconfig` CLI-Befehl. Protokolldateien können an regulären Grenzen abgeschnitten und regelmäßig auf einen Archivdateiserver verschoben werden. Im Folgenden finden Sie ein Beispiel für einen Nachrichtenfilter, mit dem alle eingehenden E-Mails an den Empfänger alan@exchange.example.com protokolliert werden:

```
Log-Alan-All-Mail:
if (recv-listener == "InboundMail")
and (rcpt-to == "alan@exchange\\.example\\.com") {
 archive("alan-all-mail");
}
```

In der archivierten Nachricht werden weitere X-IronPort-RCPT-TO-Module hinzugefügt: Header werden für jeden Umschlagempfänger hinzugefügt (die sich möglicherweise von dem Inhalt unterscheiden können An: Header Line). Bitte beachten Sie, dass diese Liste der Umschlagempfänger nicht unbedingt alle Empfänger enthält, die der Absender benannt hat. Wenn ein Absender beispielsweise eine bcc-Adresse angibt, kann die sendende MTA entscheiden, diese als separate Nachricht komplett zu senden. Im Archivprotokoll sind die Umschlagempfänger der SMTP-Transaktion enthalten, die die Nachricht erstellt hat.

Hinweis: Die Filter-Aktion für die Archivnachricht ersetzt die Protokollaktion. Nachrichtenfilter, die die vorherigen Namen verwenden, werden automatisch aktualisiert, wenn das System aktualisiert

wird.

Eine andere Möglichkeit, Kopien einer Nachricht zu behalten, besteht darin, eine Kopie mit der Aktion "bcc filter" zu generieren. Die bcc-Aktion erstellt eine exakte Kopie der Nachricht und sendet sie an den angegebenen Empfänger. Dies kann eine Sammelmailbox auf einem Archivserver sein. Dabei handelt es sich um eine genaue Kopie des Nachrichteninhalts, jedoch nicht um Envelope-Empfänger (die sich vom Inhalt unterscheiden können An: Header Line).

```
Copy-Alan-All-Mail:
if (recv-listener == "InboundMail")
and (rcpt-to == "alan@exchange\\.example\\.com") {
 bcc("sam@exchange.example.com");
}
```

In beiden oben genannten Fällen wird die Nachrichtenkopie durch die Filteraktion erstellt und ohne weitere Verarbeitung geliefert, die zusätzliche Nachrichtenfilter, Antispam-, Antivirus- oder Content-Filter enthält. Eine Nachrichtenkopie könnte also einen Virus enthalten.

Es gibt eine neue Filteraktion namens bcc-scan. Diese kann in bcc eingefügt werden, damit die neue Kopie über die normale E-Mail-Pipeline gescannt wird. Auf diese Weise können Viren oder Spam-Nachrichten nicht in Ihr Netzwerk gelangen. Hier ein Beispiel:

```
Copy-Alan-All-Mail:
if (recv-listener == "InboundMail")
and (rcpt-to == "alan@exchange\\.example\\.com") {
 bcc-scan("sam@exchange.example.com");
}
```

Beachten Sie, dass in den oben genannten Nachrichtenfiltern das Argument für die Regel rcpt-to ein regulärer Ausdruck ist, bei dem ein Escapen von Regex-Operatoren wie "." erforderlich ist. In den Archiv- oder bcc-Aktionen ist das Argument einfach eine Zeichenfolge.

Eine sehr kurzfristige Möglichkeit zum Überprüfen von Nachrichten, die einem Filter zugeordnet sind, besteht in der Verwendung von Systemquarantäne.

Weitere Informationen finden Sie unter

Antwort-ID 87: Wie kann ich einen Nachrichtenfilter oder Content-Filter testen und debuggen, bevor ich ihn in die Produktionsumgebung stelle?

Weitere Informationen zu Nachrichtenfilteraktionen finden Sie im AsyncOS for Email Advanced Configuration Guide:

Cisco Email Security Appliance - Benutzerhandbücher