Wie kann ich eine Mail-Schleifensituation auf der ESA identifizieren und behandeln?

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Mailschleife auf der E-Mail Security Appliance (ESA) identifiziert wird.

Hintergrundinformationen

Mailschleifen können durch Nachrichten mit derselben Message-ID angezeigt werden, die mehr als dreimal eingespeist wurden. Mail-Loops können Symptome von hoher CPU, langsamer Lieferung und allgemeinen Leistungsproblemen verursachen. In der Regel bedeuten Nachrichten-IDs, die mehr als einmal injiziert wurden, Looping, aber manchmal werden sie aufgrund von Problemen mehrmals injiziert, oder es könnte sich um einen schlampigen Spammer handeln, der die gleiche Spam-Nachricht mit derselben Message-ID weiter injiziert.

In der Regel wird eine E-Mail-Schleife durch ein E-Mail-Infrastruktur-Problem verursacht, das dieselbe Nachricht oder dieselbe Gruppe von Nachrichten sendet, die in Ihrem Netzwerk unbegrenzt vom Mailserver zum Mailserver gesendet werden. Diese Botschaften können sich zwar sehr lange auf diese Weise unterhalten, aber es ist weder für Ihre Netzwerkbandbreite noch für die ESA-Verarbeitungskosten von Vorteil.

Lösung

Eine Mail-Schleife zu identifizieren, wenn Sie vermuten, dass dies das Problem sein könnte, ist normalerweise ziemlich einfach, wenn Sie es mit einem Augenbecher versehen müssen.
Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) des Systems an, und geben Sie einen der folgenden Befehle ein, oder beide Befehle, wenn Sie die besten Vorteile erzielen:

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

Besonders bei der Suche nach Message-ID, wenn Sie immer wieder Instanzen von genau derselben ID sehen, dann wissen Sie, dass Sie eine Mail-Schleife haben. Manchmal reicht dies

jedoch nicht aus, da einer der Mail-Server, der dieselbe Nachricht zurückruft, hilfreich sein kann, den Message-ID-Header zu ändern oder zu entfernen. Wenn Sie also nichts mit der Message-ID-Prüfung identifizierbar machen, versuchen Sie es mit der Betreff-Prüfung.

Wenn Sie die Schleifenmeldung anhand der Message-ID gefunden haben, sollten Sie auch weitere Informationen über die Nachricht und die übergeordnete Verbindung (ICID) erhalten. Mithilfe der Message-ID und einer MID in derselben Protokollzeile können Sie Folgendes ausführen:

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

Anhand der Ergebnisse finden Sie die entsprechende ICID und DCID und führen folgende Schritte durch:

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

Jetzt sollten Sie die komplette Verbindung haben - Message-Transaktion und sehen, woher sie gekommen ist und wo sie geliefert wurde (wenn dies bereits geschehen ist). Sobald Sie die Schleifenmeldung identifiziert haben, sehen Sie sich die Nachricht an, um das Problem zu beheben. Ohne die Ursache der Schleife zu beheben, ist es wahrscheinlich, dass diese Nachricht und andere weiterhin schleifen oder dass das Problem bald wieder auftreten wird.

Erstellen Sie einen Nachrichtenfilter, ähnlich dem folgenden:

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
}
```

Bestätigen Sie diese Änderung und geben Sie den folgenden Befehl aus, um die Nachricht auszuchecken:

```
tail looper
```

Mithilfe der Informationen, die Sie über das Remote-System erhalten können, indem Sie sich die E-Mail-Protokolle anschauen, und anderer Informationen, die Sie durch das Betrachten der Nachricht selbst erhalten können, sollten Sie feststellen können, wo Ihr Problem liegt.

Wie kann verhindert werden, dass E-Mail-Schleifen auftreten?

In komplexen Umgebungen kann dies schwierig sein. Sie können verstehen, wie E-Mails in Ihrer Umgebung fließen und wie sich eine neue Netzwerkänderung, entweder auf der ESA oder auf einem anderen Gerät, auf diesen Datenverkehr auswirkt. Eine häufige Ursache für Laufzeitschleifen ist das Entfernen des Empfangs-Headers. Die ESA erkennt und stoppt automatisch eine Mailschleife, wenn sie 100 empfangene Header in einer Nachricht sieht, aber die ESA ermöglicht das Entfernen dieses Headers, der oft zu einer schlechten Mail-Schleife führt. Wenn es keinen *wirklich* guten Grund dafür gibt, schalten Sie den Received-Header nicht aus oder veranlassen Sie ihn zu entfernen.

Nachfolgend finden Sie ein Filterbeispiel, das Ihnen helfen kann, eine Mail-Schleife zu verhindern oder zu beheben:

```
External_Loop_Count:
if (header("X-ExtLoop1")) {
 if (header("X-ExtLoopCount2")) {
   if (header("X-ExtLoopCount3")) {
     if (header("X-ExtLoopCount4")) {
       if (header("X-ExtLoopCount5")) {
         if (header("X-ExtLoopCount6")) {
           if (header("X-ExtLoopCount7")) {
             if (header("X-ExtLoopCount8")) {
               if (header("X-ExtLoopCount9")) {
                  notify ('joe@example.com');
                  drop();
               }
             else {insert-header("X-ExtLoopCount9", "from
                  $RemoteIP");}}
           else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
         else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
       else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
     else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
   else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
 else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1"); }
```