ESA-Spoofed Mail-Filterung

Inhalt

[Einführung](#)
[Problem](#)
[Lösung](#)
[Filter anwenden](#)
[Zusätzliche Maßnahmen](#)

Einführung

Dieses Dokument beschreibt ein Problem, das auf der Cisco E-Mail Security Appliance (ESA) auftritt, wenn Spam und betrügerische E-Mails in das Netzwerk eindringen.

Problem

Betrüger versuchen, E-Mails zu imitieren. Wenn die E-Mail einen Mitarbeiter Ihres Unternehmens imitiert (angeblich von ihm stammt), kann dies besonders trügerisch sein und zu Verwirrung führen. Um dieses Problem zu beheben, könnten E-Mail-Administratoren versuchen, eingehende E-Mails zu blockieren, die scheinbar aus dem Unternehmen stammen (*gefälschte* E-Mails).

Es mag logisch erscheinen, dass wenn Sie die eingehende E-Mail aus dem Internet blockieren, die die Rücksendeadresse des Unternehmens im Domänennamen enthält, es das Problem löst. Wenn Sie E-Mails auf diese Weise blockieren, können Sie jedoch gleichzeitig legitime E-Mails blockieren. Hier einige Beispiele:

- Ein Mitarbeiter reist und verwendet einen Internet Service Provider (ISP) im Hotel, der den gesamten SMTP-Verkehr (Simple Mail Transfer Protocol) transparent an die ISP-Mail-Server umleitet. Wenn E-Mails gesendet werden, scheint es, als ob sie direkt über den SMTP-Server des Unternehmens fließen, aber tatsächlich über einen SMTP-Server eines Drittanbieters gesendet werden, bevor sie an das Unternehmen geliefert werden.

- Ein Mitarbeiter abonniert eine E-Mail-Diskussionsliste. Wenn Nachrichten an die E-Mail-Liste gesendet werden, werden sie an alle Abonnenten zurückgegeben, anscheinend vom Urheber.

- Ein externes System wird verwendet, um die Leistung oder Erreichbarkeit von extern sichtbaren Geräten zu überwachen. Wenn eine Warnung auftritt, enthält die E-Mail den Firmendomänennamen in der Rücksendeadresse. Drittanbieter wie WebEx tun dies recht häufig.

- Aufgrund eines temporären Netzwerkkonfigurationsfehlers wird die E-Mail von innerhalb des Unternehmens über den eingehenden Listener und nicht über den ausgehenden Listener gesendet.

- Jemand außerhalb des Unternehmens erhält eine Nachricht, dass er mit einem Mail User Agent (MUA), der neue Header-Zeilen anstatt des ursprünglichen Headers verwendet, zurück in das Unternehmen leitet.

- Eine internetbasierte Anwendung, z. B. die Federal Express-**Versandseiten** oder die Yahoo-**E-Mail-**Seite, erstellt legitime E-Mails mit einer Rücksendeadresse, die auf das Unternehmen zurückweist. Die E-Mail ist legitim und hat eine Quelladresse aus dem Unternehmen, aber sie stammt nicht von innen.

Diese Beispiele zeigen, dass eingehende E-Mails, die auf Domäneninformationen basieren, blockiert werden können, um falsche Positivmeldungen zu erzeugen.

Lösung

In diesem Abschnitt werden die empfohlenen Aktionen beschrieben, die Sie ausführen sollten, um dieses Problem zu beheben.

Filter anwenden

Um den Verlust legitimer E-Mail-Nachrichten zu vermeiden, sollten Sie die eingehenden E-Mails nicht anhand der Domäneninformationen blockieren. Stattdessen können Sie die Betreffzeile dieser Arten von Nachrichten beim Betreten des Netzwerks kennzeichnen, was dem Empfänger anzeigt, dass die Nachrichten möglicherweise gefälscht sind. Dies kann mithilfe von Nachrichtenfiltern oder Content-Filtern erreicht werden.

Die grundlegende Strategie für diese Filter besteht darin, die rückwärts gerichteten Body-Header-Zeilen (die **Von-**Daten sind die wichtigsten) sowie den RFC 821-Umschlagabsender zu überprüfen. Diese Überschriften werden am häufigsten in MUAs angezeigt und werden am wahrscheinlichsten von betrügerischen Personen gefälscht.

Der Nachrichtenfilter im nächsten Beispiel zeigt, wie Sie Meldungen kennzeichnen können, die möglicherweise imitiert werden. Dieser Filter führt mehrere Aktionen aus:

- Wenn die Betreffzeile bereits **"{Möglicherweise gefälscht}"** enthält, wird vom Filter keine weitere Kopie hinzugefügt. Dies ist wichtig, wenn Antworten im Nachrichtenfluss enthalten sind und eine Betreffzeile möglicherweise mehrmals das E-Mail-Gateway durchläuft, bevor ein Nachrichtenthread abgeschlossen ist.

- Dieser Filter sucht nach dem Umschlagabsender oder dem **Von-**Header mit einer Adresse, die im Domänennamen **@yourdomain.com** endet. Beachten Sie, dass bei der Suche nach E-Mail-Nachrichten automatisch die Groß- und Kleinschreibung nicht beachtet wird, bei der Suche nach *dem* from-Header jedoch nicht. Wenn der Domänenname an beiden Standorten gefunden wird, fügt der Filter **"{Möglichst gefälscht}"** am Ende der Betreffzeile ein.

Hier ein Beispiel für den Filter:

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
```

```
    if (mail-from == "@yourdomain\\.com$") OR
       (header("From") == "(?i)@yourdomain\\.com")
    {
        strip-header("Subject");
        insert-header("Subject", "$Subject {Possibly Forged}");
    }
}
```

Zusätzliche Maßnahmen

Da es keine einfache Möglichkeit gibt, gefälschte E-Mails von legitimen E-Mails zu identifizieren, gibt es keine Möglichkeit, das Problem vollständig zu beheben. Cisco empfiehlt daher, IronPort Anti-Spam Scanning (IPAS) zu aktivieren, das betrügerische E-Mails (Phishing) oder Spam effektiv erkennt und diese positiv blockiert. Die Verwendung dieses Anti-Spam-Scanners bietet in Verbindung mit den im vorherigen Abschnitt beschriebenen Filtern die besten Ergebnisse ohne den Verlust legitimer E-Mails.

Wenn Sie betrügerische E-Mails identifizieren müssen, die in Ihr Netzwerk gelangen, sollten Sie die Domain Keys Identified Mail (DKIM)-Technologie in Betracht ziehen. Sie erfordert mehr Einrichtung, ist aber eine gute Maßnahme gegen Phishing und betrügerische E-Mails.

> **Hinweis**: Weitere Informationen zu Nachrichtenfiltern finden Sie im **AsyncOS-Benutzerhandbuch** auf der Support-Seite der Cisco Email Security Appliance.