Wie kann ich eingebettete Hyperlinks mit ausführbaren Dateien erfassen und blockieren?

Inhalt

Frage

Wie kann ich eingebettete Hyperlinks mit ausführbaren Dateien erfassen und blockieren?

Antwort

Sie können den Text und alle HTML-Anhänge mit einem Nachrichtenfilter durchsuchen. Diese E-Mails werden in der Regel per HTML-E-Mail versendet. Damit das Scan-Modul es erkennen kann, müssen Sie den Zustand "Textkörper" verwenden. Wenn Sie nur ausgehende E-Mails verarbeiten, können Sie die Bedingung 'only-body-contains' verwenden.

Der folgende Nachrichtenfilter sucht nach einem Hyperlink mit beliebiger Länge, der mit einer ausführbaren Datei endet. Sobald die Bedingung erfüllt ist, werden zwei Aktionen aktiviert. Die erste Aktion besteht darin, den lokalen Administrator per E-Mail an admin@example.com zu benachrichtigen.

Die zweite Aktion ist das Ablegen der E-Mail. Die E-Mail muss nicht verworfen werden, sondern kann in Quarantäne gestellt werden. Das Entfernen der Aktion unten von '`drop();`' kann durch '`quarantine('Policy');`' ersetzt werden.

Die Quarantäne muss definiert werden, da die Filter-Engine den Filter nicht zulässt. Sie können entweder die Standard-Policy-Quarantäne verwenden oder eine eigene Quarantäne erstellen (Informationen zum Erstellen oder Löschen von Quarantänen finden Sie im Handbuch unter Quarantäne).

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
notify ("admin@example.com");
drop();
}
```

Sie können auch diese Version verwenden, mit der die schädlichen URLs aus dem Text entfernt und durch die URL ENTFERNT wurden.

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

Detaillierte Anweisungen zum Eingeben eines Nachrichtenfilters finden Sie unter Wie füge ich meiner Cisco IronPort Appliance einen neuen Nachrichtenfilter hinzu?

Lesen Sie den Abschnitt Cisco ESA AsyncOS ADVANCED USER GUIDE for Email Security Appliances mit dem Namen "Policy Enforcement" (Richtliniendurchsetzung), um Nachrichtenfilter zu überprüfen.