Spam-Nachrichten der Cisco E-Mail Security Appliance (ESA) in Ihrem Unternehmen

Inhalt

Einführung

Dieses Dokument beschreibt fünf Methoden, mit denen Spam-E-Mails in Ihr Unternehmen gelangen können.

Methoden

1. Legitimative Nachricht/Marketing-Mail

Die legitime Nachricht wurde vom Benutzer ausgewählt, oder ihr Name wurde an eine andere Organisation verkauft. Im ersten Fall muss der Benutzer Schritte unternehmen, um sich von der Liste abzumelden. Falls dies der Fall ist, senden Sie die Nachricht erneut an spam@access.ironport.com, damit die Antispam-Definitionen global aktualisiert werden können, was die Spam-Abfangrate Ihrer ESA insgesamt verbessert. Durch Aktivieren von Marketing-E-Mails in der Richtlinie für eingehende E-Mails kann die Wahrnehmung geändert werden, dass diese Nachricht "Marketing" über "Spam" lautet.

2. Der Anti-Spam wird nicht korrekt aktualisiert

Anti-Spam ist deaktiviert oder der Feature-Schlüssel ist abgelaufen. Um zu überprüfen, ob Anti-Spam aktualisiert wird, gehen Sie zu **GUI > Security Services > IronPort Anti-Spam**. In diesem Fenster sollten Sie innerhalb der letzten 6 Stunden Updates der Regelsätze oder Engine sehen. Auf dieser Registerkarte oben können Sie auch sicherstellen, dass der Anti-Spam-Dienst aktiviert ist. Sie können den Status des Feature-Schlüssels auf der Registerkarte Systemverwaltung > Feature-Schlüssel überprüfen, um den Status des Anti-Spam-Schlüssels zu überprüfen.

3. Mail-Policy oder Nachrichtenfilter

Spam kann in Ihr Unternehmen gelangen, wenn die Anti-Spam-Sicherheitslösung für einen bestimmten Absender oder Empfänger pro Mail-Policy eines Kunden deaktiviert ist. Eine weitere Möglichkeit, die Spam-Filterung zu überspringen, sind Nachrichtenfilter (CLI: Befehl **filter**).

4. Mail Flow-Richtlinie

Eine Nachricht wird mithilfe der ICID der Nachricht klassifiziert. In dieser Situation ist es wahrscheinlich, dass die Anti-Spam-Sicherheitsfunktion deaktiviert ist, was die Mail-Policy überschreibt. Sie können dies bestimmen, indem Sie sich die E-Mail-Protokolle ansehen. In den Protokollen müssen Sie zunächst die ICID überprüfen, um zu ermitteln, in welche SenderGroup die Nachricht klassifiziert wurde. Von dort aus wird die zugehörige Mail Flow Policy überprüft. Wenn Sie eine große Anzahl von Einträgen in der Zulassungsliste haben, müssen Sie möglicherweise einige der eingesendeten Nachrichten überprüfen, um festzustellen, ob sie von der AntiSpam-Engine gescannt wurden. Öffnen Sie die Kopfzeilen einer Nachricht, und suchen Sie nach dem Header X-IronPort-Spam. Das Vorhandensein dieses Headers bedeutet, dass die Nachricht die Engine durchlaufen hat.

5. Nachricht ist Spam

Die Nachricht ist tatsächlich Spam. Sie haben bestätigt, dass die Nachricht von der Antispam-Engine mithilfe der Nachrichtenverfolgungsfunktion gescannt wurde (suchen Sie in der Nachrichtenverfolgung nach "CASE"). Wenn das Urteil negativ ist und Sie die Nachricht als Spam betrachten, senden Sie die ursprüngliche Nachricht an spam@access.ironport.com. Dies könnte ein Fall sein, bei dem eine neue Spam-Bedrohung gerade veröffentlicht wird oder eine ältere Bedrohung, die überarbeitet wurde.

Die Bearbeitung der Spam-Einsendungen erfolgt automatisch und manuell und es gibt kein Feedback für Ihre spezifische Einsendung. Sie können sich jederzeit an das Cisco TAC wenden und eine Evaluierung und Antwort anfordern.