ESA DHAP-Funktion

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die DHAP-Funktion (Directory Harvest Attack Prevention) der Cisco E-Mail Security Appliance (ESA) aktivieren, um DHAs (Directory Harvest Attacks) zu verhindern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ESA
- AsyncOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Versionen von AsyncOS.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Ein DHA ist eine Technik, die von Spammern verwendet wird, um gültige E-Mail-Adressen zu finden. Es gibt zwei Haupttechniken, die verwendet werden, um die Adressen zu generieren, die DHA-Ziele:

- Der Spammer erstellt eine Liste aller möglichen Kombinationen von Buchstaben und Zahlen und hängt dann den Domänennamen an.

- Der Spammer verwendet einen Standard-Wörterbuchangriff mit der Erstellung einer Liste, die

gemeinsame Vor- und Nachnamen und Initialen kombiniert.

DHAP ist eine von den Cisco Content Security Appliances unterstützte Funktion, die bei der LDAP-Akzeptanzvalidierung aktiviert werden kann. Die DHAP-Funktion verfolgt die Anzahl der ungültigen Empfängeradressen eines bestimmten Absenders.

Sobald ein Absender einen vom Administrator definierten Grenzwert überschreitet, gilt er als nicht vertrauenswürdig, und E-Mails von diesem Absender werden ohne NDR (Network Design Requirement) oder Fehlercodegenerierung blockiert. Sie können den Schwellenwert anhand der Reputation des Absenders konfigurieren. Nicht vertrauenswürdige oder verdächtige Absender können beispielsweise einen niedrigen DHAP-Schwellenwert haben, vertrauenswürdige oder seriöse Absender einen hohen DHAP-Schwellenwert.

DHAP aktivieren

Um die DHAP-Funktion zu aktivieren, navigieren Sie in der Benutzeroberfläche der Content Security Appliance zu **Mail Policies > Host Access Table (HAT)** und wählen Sie **Mail Flow Policies (Mail-Fluss-Richtlinien)**. Wählen Sie in der Spalte **Policy** Name (**Richtlinienname)** die Richtlinie aus, die Sie bearbeiten möchten.

Die HAT verfügt über vier grundlegende Zugriffsregeln, die für Verbindungen von Remote-Hosts verwendet werden:

- **AKZEPTIEREN**: Die Verbindung wird akzeptiert, und die Annahme von E-Mails wird durch die Listener-Einstellungen weiter eingeschränkt. Dies schließt die Recipient Access Table (für öffentliche Listener) ein.
- **ABLEHNEN**: Die Verbindung wird zunächst akzeptiert, aber der Client, der versucht, eine Verbindung herzustellen, erhält eine 4XX- oder 5XX-Begrüßung. Es wird keine E-Mail akzeptiert.
- **TCPREFUSE**: Die Verbindung wird auf TCP-Ebene abgelehnt.
- **RELAIS**: Die Verbindung wird akzeptiert. Der Empfang für einen Empfänger ist zulässig und wird nicht durch die Recipient Access Table eingeschränkt. Die Domänenschlüsselsignierung ist nur für Relay-Mail-Flow-Richtlinien verfügbar.

Suchen Sie im Abschnitt **Mail Flow Limits (Mail Flow Limits**) der ausgewählten Richtlinie nach der **DHAP-Konfiguration (Directory Harvest Attack Prevention), und legen Sie diese fest, indem Sie die Max.** Ungültige Empfänger pro Stunde. Sie können auch die Max. Ungültiger Code für Empfänger pro Stunde und Maximum Text für ungültige Empfänger pro Stunde, falls gewünscht.

Sie müssen diesen Abschnitt wiederholen, um DHAP für zusätzliche Richtlinien zu konfigurieren.

Stellen Sie sicher, dass Sie alle Änderungen in der GUI senden und bestätigen.

> **Anmerkung:** Cisco empfiehlt, für die **maximale Anzahl ungültiger Empfänger pro Stunde aus einer Remote-Host-**Einstellung eine Höchstzahl zwischen fünf und zehn zu verwenden.

> **Anmerkung:** Weitere Informationen finden Sie im **AsyncOS-Benutzerhandbuch** im Cisco

Support Portal.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.