Wie kann sich eine Firewall oder ein SMTP-Proxy auf ESMTP-Services auswirken?

Inhalt

Frage

Wie kann sich eine Firewall oder ein SMTP-Proxy auf ESMTP-Services auswirken?

Antwort

In Verbindung mit der E-Mail-Verarbeitung über eine Cisco E-Mail Security Appliance (ESA) sind eine Reihe von Firewalls und SMTP-Proxy-Services verfügbar, die Funktionen zum Schutz von Mail-Servern vor Exploits bereitstellen.

Einige dieser Schutzmethoden können ESMTP-Dienste wie TLS und SMTP-Authentifizierung beeinträchtigen.

Dienste wie TLS und SMTP-Authentifizierung verwenden ESMTP-Befehle (Extended SMTP). Um auf den ESMTP-Befehlssatz zuzugreifen, muss der EHLO-Befehl den empfangenden Server erreichen. Einige Firewall- und Proxy-Sicherheitsfunktionen blockieren oder ändern den EHLO-Befehl während der Übertragung. Wenn das Sicherheitsgerät EHLO nicht zulässt, sind keine ESMTP-Dienste verfügbar. In diesem Fall sind nur die in RFC 821 Abschnitt 4.5.1 angegebenen SMTP-Befehle auf einem Mailserver zulässig. Diese sind: HELO, MAIL, RCPT, DATA, RSET, NOOP und QUIT. Es sind keine ESMTP-Befehle verfügbar.

Eine weitere Sicherheitsfunktion dieser Geräte ist die Änderung von SMTP-Bannern. Um den Typ und die Version des geschützten Mail-Servers auszublenden, verdecken einige Geräte bis auf die 220 Teile des Banners, die für die Kommunikation erforderlich sind.

Das Banner sieht oft ähnlich aus wie:

```
220**************
```

Ein Teil der Informationen, die ausgeblendet werden, ist die ESMTP-Werbung im Banner. Wenn diese Anzeige entfernt wird, wird einem sendenden Server nicht bekannt sein, dass ESMTP-Befehle akzeptiert werden.

Zusammenfassend können Firewalls und SMTP-Proxyserver EHLO-Befehle blockieren und ESMTP-Bannerwerbung ausblenden. Wenn diese Sicherheitsmaßnahmen implementiert sind, ist

möglicherweise kein Zugriff auf ESMTP-Befehle möglich. Um sicherzustellen, dass andere Hosts mit der ESA über ESMTP kommunizieren können, müssen Sie diese Sicherheitsfunktionen auf Ihrem Sicherheitsgerät deaktivieren.

Zugehörige Informationen

- Testen der PIX Firewall Mailguard-Funktion
- Cisco PIX: Erweiterte Funktionen und Angriffsschutz
- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems