In che modo un firewall o un proxy SMTP può influire sui servizi ESMTP?

Sommario

Domanda

In che modo un firewall o un proxy SMTP può influire sui servizi ESMTP?

Risposta

In combinazione con l'elaborazione della posta tramite Cisco Email Security Appliance (ESA), sono disponibili una serie di firewall e servizi proxy SMTP che offrono funzionalità destinate a proteggere i server di posta dagli attacchi.

Alcuni di questi metodi di protezione possono ostacolare i servizi ESMTP come TLS e l'autenticazione SMTP.

I servizi, ad esempio l'autenticazione TLS e SMTP, utilizzano i comandi ESMTP (Extended SMTP). Per accedere al set di comandi ESMTP, il comando EHLO deve raggiungere il server ricevente. Alcune funzionalità di sicurezza del firewall e del proxy bloccheranno o modificheranno il comando EHLO in transito. Quando il dispositivo di sicurezza non consente EHLO, non saranno disponibili servizi ESMTP. In questo caso, solo i comandi SMTP specificati nella RFC 821 sezione 4.5.1 sono consentiti su un server di posta. ossia SmartNIC): HELO, MAIL, RCPT, DATA, RESET, NOOP E QUIT. Nessun comando ESMTP disponibile.

Un'altra funzionalità di protezione utilizzata da questi dispositivi è la modifica del banner SMTP. Per nascondere il tipo e la versione del server di posta protetto, alcuni dispositivi oscureranno tutte le parti del banner necessarie per la comunicazione, ad eccezione delle 220.

Il banner apparirà spesso simile a:

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

Parte delle informazioni nascoste è l'annuncio ESMTP nel banner. Quando l'annuncio viene rimosso, il server di invio non sarà consapevole dell'accettazione dei comandi ESMTP.

In sintesi, i firewall e i server proxy SMTP possono bloccare i comandi EHLO e nascondere gli annunci banner ESMTP. Quando queste misure di sicurezza sono in atto, i comandi ESMTP potrebbero non essere accessibili. Per assicurarsi che altri host possano comunicare con l'ESA

utilizzando ESMTP, potrebbe essere necessario disattivare queste funzioni di sicurezza sul dispositivo di sicurezza

Informazioni correlate

- Test della funzione Mailguard di PIX Firewall
- Cisco PIX: Funzioni avanzate e protezioni di attacco
- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems