E-Mail Transportverschlüsselung STARTTLS vs. DANE vs. MTA-STS

Umfang des Dokuments

Der Umfang dieses Dokuments beschränkt sich auf den verschlüsselten Transport zwischen zwei E-Mail-Servern. Die Verbindung zwischen E-Mail-Client und Server oder Ende-zu-Ende Verschlüsselung ist kein Bestandteil, sollte für ein sicheres Gesamtsystem aber ebenfalls betrachtet werden.
Transportverschlüsselung zwischen E-Mail-Servern ist für eine Erhöhung der Sicherheit in der E-Mail-Kommunikation unabdingbar.

STARTTLS

Mittels STARTTLS kann die Verbindung zwischen Mailservern abgesichert werden. Das Verfahren hat allerdings eklatante Schwächen. Zunächst wird im Allgemeinen das Zertifikat des E-Mailservers beim Verbindungsaufbau nicht geprüft. In vielen Fällen könnte man es noch nicht mal prüfen, da selbstsignierte Zertifikate genutzt werden. Hinzu kommt, dass bei STARTTLS der initiale Verbindungsaufbau unverschlüsselt stattfindet und die E-Mail-Server die Verschlüsselung aushandeln. Man spricht hier von einer opportunistischen Verschlüsselung, da lediglich dann verschlüsselt kommuniziert wird, wenn beide E-Mail-Server STARTTLS unterstützen. Ein Angreifer könnte mit einem Man-in-the-Middle-Angriff den STARTTLS-Befehl herausfiltern. Die E-Mails würden dann im Klartext übermittelt und der Angreifer kann den Inhalt mitlesen.

DANE

Mit DNS-Based Authentication of Named Entities (DANE) werden die Schwächen von STARTTLS addressiert. DANE kann für verschiedene Anwendungen eingesetzt werden, wir interessieren uns aber hier für den verschlüsselten E-Mail-Transport. DANE ermöglicht es einem Domaininhaber Zertifikate auszustellen und mit entsprechenden Einträgen im Domain Name System (DNS) zu verknüpfen. Ein Kommunikationspartner kann auf diese Weise das Zertifikat verifizieren ohne dass auf eine Certificate Authority (CA) zurückgegriffen werden muss. In diesem Konstrukt ist es allerdings erforderlich, dass die DNS Einträge vor Manipulation durch Dritte geschützt sind. DANE setzt darum DNS-Security Extensions (DNSSEC) voraus.
Leider ist DNSSEC global gesehen aktuell nur gering verbreitet, und damit auch DANE. Aus Sicht eines Versenders benötigt DANE allerdings kein DNSSEC, da lediglich der Versender das Zertifikat des empfangenden E-Mail-Servers verifiziert.

Don Owens von Cisco Talos Intelligence Group über DANE:
"DANE ist eine ausgezeichnete Möglichkeit, den Datenverkehr zu verschlüsseln und gleichzeitig MITM-Angriffe (Man-in-the-Middle) zu vermeiden. Wenn DANE vom Empfänger nicht unterstützt wird, ist es möglich, MITM-Angriffe mit MTA-STS zu erschweren. Eine weitere Möglichkeit besteht darin, opportunistisches TLS zu verwenden, um eine Sicherheitsebene zu schaffen, auch wenn es anfälliger für MITM-Angriffe ist. Aber wirklich, Empfänger sollten DANE einrichten, wo immer es möglich ist, um die bestmögliche Sicherheit für den E-Mail-Verkehr zu gewährleisten."

MTA-STS

Eine Alternative zu DANE welche ebenfalls eine deutliche Verbesserung zu STARTTLS darstellt, allerdings kein DNSSEC voraussetzt ist SMTP MTA Strict Transport Security (MTA-STS). MTA-STS basiert auf einem sogenannten "Trust on first use" (TOFU) Modell. Einfach gesagt wird bei einer ersten Verbindung zu einem neuen Server der Fingerprint des Zertifikats in einer lokalen Datenbank als zukünftige Referenz gespeichert. Bei jedem weiteren Verbindungsaufbau zu diesem Server wird das Zertifikat gegen diesen lokalen Fingerprint geprüft. Das TOFU Modell findet ebenfalls typischerweise bei ssh Verbindungen und bei HTTP Strict Transport Security (HSTS) eine Rolle. MTA-STS bedeutet zwar keinen 100%igen Schutz gegen einen Man-in-the-Middle-Angriff, allerdings könnte ein solcher lediglich dann erfolgreich sein, wenn der erste Verbindungsaufbau zu einem neuen Server angegriffen würde.

Zusammenfassung und Fazit

STARTTLS schützt zwar vor einem passiven mitlesen einer Verbindung zwischen zwei E-Mail-Servern, kann allerdings bereits mit relativ geringem Aufwand durch eine downgrade Attacke auf eine unverschlüsselte Verbindung zurückgestuft werden.
DANE löst das Problem und erhöht die Sicherheit beträchtlich, setzt allerdings DNSSEC voraus. MTA-STS ist auf den ersten Blick eine gute Alternative zu DANE. Allerdings ist hierbei zu beachten, dass es in den meisten Fällen sinnvoller wäre die Zeit und Ressourcen, welche für die Implementierung von MTA-STS eingesetzt werden müssten, in die Implementierung von DNSSEC und darauffolgend DANE zu investieren.
Denn MTA-STS bietet eine (zugegeben kleine) Angriffsfläche die DANE nicht aufweist, und zudem verlassen sich einige weitere Protokolle wie SPF und DKIM auf DNS Einträge. Somit ist eine höhere Verbreitung von DNSSEC für alle von Vorteil.

Autor: Alexander Zeh,
Engineering Manager Certified Senders Alliance