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

Abgrenzung

Dieses Dokument befasst sich mit der Transportverschlüsselung von Nachrichten zwischen zwei E-Mail-Servern. Sie ist für eine Grundsicherung des Nachrichtenaustausches unabdingbar. Der Austausch von Nachrichten zwischen einem E-Mail-Client und einem Server oder die Ende-zu-Ende Verschlüsselung von Nachrichten sind nicht Gegenstand dieses Artikels. Wenn es darum gehen soll, ein sicheres Gesamtsystem zu erschaffen, sollten diese Aspekte zusätzlich zu den Ausführungen in diesem Artikel betrachtet werden.

Ausgangssituation

Als der erste Standard für das Simple Mail Transfer Protocol (kurz: SMTP) verabschiedet wurde, war Verschlüsselung des Transports nicht Teil davon. Alle Nachrichten wurden als Klartext zwischen den Servern ausgetauscht. Sie waren damit grundsätzlich lesbar für jeden, der sich in den Datenaustausch zwischen den beiden Servern einklinken konnte.

Dies änderte sich erst, als mit der Einführung der SMTP Service Extensions für Extend SMTP (kurz: ESMTP) eine Möglichkeit geschaffen wurde, Transportverschlüsselung als opportunistisches Merkmal eines Datenaustausches zu wählen. Opportunistisch, weil davon ausgegangen werden musste, dass nicht alle Server Transportverschlüsselung beherrschen würden. Sie sollten nur dann verschlüsseln, wenn es opportun wäre und nicht zwingend (mandatory).

Um einem sendenden Server die grundsätzliche Fähigkeit zur Verschlüsselung anzudeuten wurde vereinbart, dass der empfangende Server zu Beginn einer ESMTP-Transportsitzung das Schlüsselwort STARTTLS ausgeben solle.

STARTTLS

STARTTLS kann den Transport zwischen zwei E-Mail-Servern verschlüsseln. Der empfangende Server signalisiert dem senden wollenden Server dazu nach Aufbau einer Verbindung und in der ESMTP-Sitzung die Fähigkeit zur Verschlüsselung.

Ist der senden wollende Server grundsätzlich in der Lage verschlüsselten Transport durchzufuhren, kann er das Angebot annehmen und den empfangenden Server zum Start einer TLS-verschlüsselten Verbindung auffordern.

Daraufhin verhandeln die beiden Server unter welchen Bedingungen diese den Transport verschlüsseln wollen. Können beide Server sich auf die Kriterien einer verschlüsselten ESMTP-Sitzung einigen, erstellt der empfangenden Server einen Sitzungsschlüssel (Session-Key). Dieser wird nur zwischen diesen beiden Servern und auch nur für eine gewisse Zeit verwendet, um die Kommunikation zwischen den beiden Parteien zu verschlüsseln.

STARTTLS gestattet sicheren, verschlüsselten Transport, wenn eine verschlüsselte Verbindung etabliert wurde, aber es weist kritische Mangel beim Sitzungsaufbau und bei der Erstellung des Sitzungsschlüssels auf.

Die Sicherheitsforscher Diffie und Hellman demonstrierten schon früh wie einfach es war, einen verschlüsselten Transport nachträglich zu entschlüsseln, sodass der Angreifer nur in Besitz des Sitzungsschlüssels und einer Aufzeichung der verschlüsselten Kommunikation beider E-Mail-Server wäre. Sie zeigten auch wie dieser Session Replay genannte Angriff durch den Einsatz weiterer Schlüssel verhindert und dadurch Perfect Forward Secrecy erreicht werden konnte.

Für andere Angriffsvektoren wurden lange Zeit keine Gegenmaßnahmen etabliert. So erfährt ein senden wollender Server zum Beispiel erst in der Sitzung mit dem anderen E-Mail-Server, dass dieser den verschlüsselten Transport beherrscht. Ein Angreifer, der den Datenstrom der beiden Server kontrollieren kann, kann die Fähigkeit zum ESMTP oder das Schlüsselwort STARTTLS unterdrücken und den sendenden Server auf diese Weise zu einem "Session Downgrade" zwingen. Die Kommunikation findet dann unverschlüsselt statt und der Angreifer kann alle ausgetauschten Nachrichten im Klartext mitschneiden.

Einen weiteren Angriffsvektor stellt die Man-in-the-Middle Attacke dar. Bei dieser Form des Angriffs platziert der Angreifer ein eigenes System zwischen den beiden E-Mail-Servern und gibt sich als Zielsystem aus, das auch verschlüsselten Transport anbieten kann.

Ein sendender Server, welcher "nur" STARTTLS beherrscht, ist ohne weitere Schutzmaßnahmen nicht in der Lage, den Man-in-the-Middle zu erkennen,
denn SMTP bietet Prinzip-bedingt keine Methoden an, mit denen Server sich vor Verbindungsaufbau Identitätsmerkmale der Gegenseite beschaffen und diese nach Verbindungsaufbau vergleichen können.

Entsprechend durch den Angreifer getäuscht, kann ein Server also im guten Glauben mit dem richtigen Server zu kommunizieren, dem Falschen die schützenswerten Daten übermitteln. Die Kommunikation kann dann sogar verschlüsselt erfolgen.

Diese beiden Schwachstellen behebt DANE.

DANE

Die Methode "DNS-Based Authentication of Named Entities" (kurz: DANE) behebt die genannten Schwachstellen von STARTTLS. DANE beschreibt ein abstraktes Verfahren. Es kann grundsätzlich in vielen Protokollen und nicht nur in SMTP eingesetzt werden. Dieses Dokument beschränkt sich auf die Implementierung von DANE für SMTP.

DANE sieht vor, im DNS der Zieldomain Informationen zu hinterlegen, welche noch vor Verbindungsaufbau mit dem Zielserver erkennen lassen, dass der Server STARTTLS unterstützt und anhand welches Merkmals der Zielserver identifiziert werden kann. Weis der sendende Server vorab, dass das Zielsystem STARTTLS unterstützt, kann es nicht Opfer einer Session Downgrade Attacke werden. Und weiß es, anhand welcher Merkmale es sein Gegenüber identifizieren kann, kann es nicht Opfer einer Man-in-the-Middle Attacke werden, denn nur der richtige Server verfügt über die passenden Merkmale.

Antworten traditioneller DNS-Server sind für DANE nicht geeignet, denn sie können gefälscht werden. Ein Angreifer konnte einen senden wollenden Server auf diese Weise auf den falschen Weg schicken. Deshalb fordert die DANE-Methode, dass DNS-Server, welche DANE-relevante Antworten ausgeben wollen, die DNS-Security Extensions (DNSSEC) einsetzen. Mit Hilfe von DNSSEC werden die Antworten des DNS-Servers kryptographisch signiert. Der senden wollende Server kann prüfen ob "der richtige DNS-Server" geantwortet hat und ob die DNS-Antwort unverfälscht angekommen ist.

DANE verändert das Vertrauensmodell, welches der Verschlüsselung mit Zertifikaten zu Grunde liegt. Es verlasst sich nicht mehr auf die Vertrauenskette einer Certification Authority (kurz: CA), sondern es verankert den Trust in der DNS-Zone des Zielsystems.

Der DANE-Methode folgend ist es unerheblich, ob es sich bei dem vorliegenden Zertifikat um ein selbst-signiertes oder abgelaufenes Zertifikat handelt.

Solange die DNSSEC-signierte Zone das Zertifikat als gültig ausweist, ist es einsetzbar. DANE setzt DNSSEC voraus und das hindert seine Verbreitung auf Seiten der Empfänger, denn der Anteil an DNSSEC-signierten DNS-Zonen ist global betrachtet gering.

Versender hindert die geringe Verbreitung von DNSSEC nicht daran, DANE zu nutzen. Deren E-Mail-Server müssen beim Versenden nur prüfen, ob das Zielsystem DNSSEC und DANE anbietet. Ist beides gegeben, kann es DANE-Sicherheit zum Schutz von Transportverschlüsselung in vollem Umfang nutzen.

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." – Don Owens

Kritiker von DANE, welche sich daran stören, dass es DNSSEC voraussetzt, haben deshalb MTA-STS spezifiziert.

MTA-STS

SMTP MTA Strict Transport Security (kurz: MTA-STS) verbessert STARTTLS ohne DNSSEC zwingend voraus zu setzen. Es belässt den Trust bei der CA und etabliert ein "Trust on first use" (TOFU) Modell. Richtlinien für den "richtigen Versand" werden beim ersten Verbindungsaufbau aus der Domain des Zielsystems bezogen und fortan befolgt.

Auf diese Weise kann MTA-STS einem Sender signalisieren, dass dieser STARTTLS zu erwarten hat und ihn so vor einer Session Downgrade Attacke beschützen.

Dies gelingt nur dann, wenn ein Angreifer das DNS des Senders nicht vorab mit falschen Informationen "vergiftet" (Cache Poisoning) hat.

Bei Einsatz von DNSSEC ist diese Art des Angriffs Prinzip-bedingt ausgeschlossen.

Weiterhin setzt es voraus, dass ein Angreifer nicht in Besitz eines für die Zieldomain geeigneten Zertifikates ist. MTA-STS verlässt sich dabei darauf, dass CAs Kontrollmechanismen einsetzen, die das mehrfache Ausstellen eines Zertifikates für ein Zielsystem verhindern. Nicht schützen kann MTA-STS vor einer Man-in-the-Middle Attacke, denn es übermittelt dem Sender keine Kriterien, mit denen es das Zielsystem eindeutig identifizieren kann. Auch hier verlasst sich MTA-STS auf das Vertrauensmodell des CA-Systems.

Zusammenfassung und Fazit

Traditionelles SMTP schützt Nachrichten während des Transports nicht.

STARTTLS verschlüsselt den Transport, aber es bietet Angriffspunkte, die es ermöglichen Transportverschlüsselung zu unterlassen oder mit dem falschen System verschlüsselt zu kommunizieren.

DANE verschlüsselt den Transport und es ist Prinzip-bedingt immun gegen die genannten Angriffe. Dafür setzt es eine DNSSEC-signierte Zone auf Seite des Empfängers voraus. Weil DNSSEC als komplex und kompliziert wahrgenommen wird, steht es der Verbreitung von DANE im Weg. Diese Hürde umgeht MTA-STS.

MTA-STS verschlüsselt den Transport und es erschwert die Ausnutzung der genannten Schwachstellen. Es stellt diese aber nicht ab, denn dazu ist es Prinzip-bedingt nicht in der Lage.

Wer die Übermittlung von E-Mail absichern möchte, sollte beim Versenden DANE nutzen, denn dort muss die eigenen DNS-Zone nicht mit DNSSEC abgesichert werden.

Wann immer das eigene System beim Versenden auf eine DANE-aktiviertes Zielsystem trifft, können die Vorteile von DANE zum Tragen kommen.

Für die eigene Domain ergibt es, auch wenn es bisher kaum MTA-STS fähige E-Mail-Server gibt, in einem ersten Anlauf Sinn, MTA-STS für Sender anzubieten. Verglichen mit dem traditionellen STARTTLS kann es die Sicherheit erhöhen.

Mittel- bis langfristig sollte die eigene Domain mit DNSSEC abgesichert werden. Der dann folgende Schritt zur DANE-gesicherten Domain ist leicht. Dann können Sender den unerreichten Sicherheitsgewinn von DANE nutzen und der verschlüsselte Transport von E-Mails wird effektiv und umfassend geschützt.

Autor: Patrick Koetter,
Leiter Kompetenzgruppe E-Mail,
Vorstand sys4 AG