E-Mails auf dem Transportweg schützen

Umverpackung

Sven Krohlas

Seit vielen Jahren versuchen E-Mail-Anbieter, die ihnen anvertraute Kommunikation vor Lauschangriffen und Manipulation zu schützen. Aber bis heute hat sich kein Standard dafür durchgesetzt. MTA-STS soll nun den Durchbruch bringen.

Den Datentransfer von E-Mails zu verschlüsseln und sie nicht einfach im Klartext per Simple Mail Transfer Protocol (SMTP) zu versenden, ist eine Vision, an deren Verwirklichung die Beteiligten bereits seit über 20 Jahren arbeiten – weitgehend erfolglos. Schon 1997 war Port 465 für SMTPS reserviert. Er sollte dazu dienen, SMTP-Nachrichten über SSL zu versenden. Die Reservierung entfiel bald darauf für das in SMTP integrierte Kommando STARTTLS, das einen TLS-Handshake in der SMTP-Session einleitet.

STARTTLS ist sehr flexibel und ermöglicht die Nutzung desselben Ports sowohl für verschlüsselte als auch für Klartextverbindungen. Doch schon bald stellte sich heraus, dass es sich zu einfach unterbinden lässt. Im unverschlüsselten Teil der Verbindung können Überwacher das Kommando erkennen, manipulieren oder ausfiltern. Die Chinese Firewall und andere Netzwerkfilter unterbinden also gesicherte Verbindungen. Zudem kann der Nutzer der Namensauflösung und dem Routing nicht trauen und ein „Man in the Middle“ die Kommunikation abhören oder gar manipulieren. Gegen mächtige Angreifer wie Geheimdienste oder Banden mit hoher krimineller Energie besteht kein ausreichender Schutz.

Nach Edward Snowdens Enthüllungen im Jahr 2013 wuchs der Druck, eine Lösung herbeizuführen. 2014 erkannte die IETF derartige Angreifer als realistisch an (RFC 7258, zu diesen und anderen Quellen siehe ix.de/ix1812110). Nach Versuchen mit proprietären Verfahren wie „E-Mail Made in Germany“ wurde 2015 DANE für SMTP als offenes Verfahren standardisiert, mit dem Einlieferer herausfinden können, ob ein Mailserver verschlüsselte Verbindungen aufbauen und authentifizieren kann. Basis hierfür ist eine ebenso manipulationssichere und authentifizierte Namensauflösung per DNSSEC. Einige große Mailboxprovider wie 1&1 oder Comcast haben DANE schnell implementiert, wenn auch nicht auf all ihren Domains. Für viele Administratoren ist DANE jedoch nicht umsetzbar, da eben nicht jede Domain per DNSSEC auflösbar ist. Daher konnte es sich bis heute nicht flächendeckend durchsetzen.

Behelfsbrücke zur Sicherheit

Der neue Standard „SMTP MTA Strict Transport Security“ (MTA-STS) soll eine Brücke schlagen zwischen dem als nicht sicher genug eingestuften STARTTLS und dem oft noch nicht realisierbaren DANE. MTA-STS setzt ähnlich wie der Namensvetter HTTP Strict Transport Security (HSTS) oder Autocrypt auf Trust on First Use (TOFU) als Vertrauensanker. Vereinfacht gesagt handelt es sich um eine Art DANE ohne DNSSEC. Die Ergebnisse der DNS-Abfragen speichert jedoch ein Cache, sodass Manipulationen bei späteren Verbindungsversuchen während der Vorhaltezeit auffallen können. Das erreicht zwar nicht das Sicherheitsniveau von DANE, erschwert aber Angriffe wie bei STARTTLS erheblich.

Um die Präsenz einer MTA-STA-Policy bekannt zu geben, erhält die Empfänger-Domain im DNS einen Text-Record unter dem Label _mta.sts, beispielsweise:

```
_mta-sts.example.com. IN TXT "v=STSv1;
id=20181027085700Z;"
```

Man kann auch per CNAME auf den Eintrag des Mailproviders verweisen, wenn man dessen Infrastruktur und keinen eigenen Mailserver nutzt:

```
_mta-sts.example.com. IN CNAME
_mta-sts.example.net.
```

Der Schlüssel *v* bezeichnet die Version des Standards, *id* einen eindeutigen Identifier, der sich mit jeder Änderung der Domain-Policy ändern muss. Es handelt sich dabei jedoch ausdrücklich nicht um eine hochzuzählende Versionsnummer.

Ein Einlieferer entnimmt dem DNS-Record, dass eine MTA-STS-Policy existiert, und erhält diese via HTTPS unter dem Label *mta-sts* im Verzeichnis */.well-known/mta-sts.txt*. Im Beispiel wäre das:

```
https://mta-sts.example.com/.well- ↵
                              known/mta-sts.txt
```

Im Falle einer Delegation kann dieses Label zu einem Server des Mailproviders auflösen oder per CNAME darauf verweisen. Eine Alternative besteht in einem unter dieser URL erreichbaren Reverse Proxy, der die Policy beim eigentlichen Mailboxprovider abruft.

Das Zertifikat dieses Abrufs muss in jedem Fall gültig sein. Sein Name muss zum Hostnamen der Ziel-Domain passen (und im Delegationsfall nicht nur zu der des Mailboxproviders) und es muss von einer CA ausgestellt sein, der der Einlieferer vertraut. Zudem darf es nicht zu HTTP-Umleitungen (Statuscodes 3xx) oder zu einem Abruf aus HTTP-Caches kommen. Die abgerufene Textdatei enthält wieder Informationen zur Version des Standards, mx-Muster der Domain (eventuell mit einer Wildcard für das am weitesten links stehende Label) sowie die gewünschte Caching-Zeit *max_age* in Sekunden:

```
version: STSv1
mode: enforce
mx: mail.example.com
mx: *.example.net
mx: backupmx.example.com
max_age: 604800
```

Je länger ein Eintrag im Cache bleiben darf, desto geringere Angriffsflächen bietet die Domain. Dies bezahlt man mit verringerter Flexibilität beim Ändern von Policies. Es empfiehlt sich zudem, den Cache nicht ablaufen zu lassen, sondern ihn rechtzeitig aufzufrischen. Das erschwert es einem Angreifer, für Manipulationen geeignete Zeitpunkte vorherzusehen.

Der Modus ähnelt der entsprechenden Policy in DMARC: Domains können Einträge zum Testen *(mode: testing)* veröffentlichen, womit die Domain signalisiert, dass sie Berichte über Verbindungs-

Stand der Umsetzung bei Mailboxprovidern

Land	Anbieter	Domain	MTA-STS	Reports	DANE
in Deutschland	Arcor	arcor.de	–	–	–
	freenet	freenet.de	–	–	✓
	T-Online	t-online.de	–	–	–
	Posteo	posteo.de	–	–	✓
	Heinlein	mailbox.org	✓, testing	mailto	✓
	mail.de	mail.de	✓, testing	mailto	✓
	United Internet	web.de	✓, testing	mailto	✓
		email.de	–	–	–
		gmx.de	–	–	✓
		gmx.net	✓, testing	mailto	✓
weltweit		mail.com	✓, testing	mailto	✓
	Google	gmail.com	✓, testing	mailto	–
	Oath	yahoo.com	✓, testing	mailto	–
		yahoo.de	–	–	–
		aol.com	–	–	–
	Microsoft	outlook.com	✓, fehlt	–	–
		hotmail.com	–	–	–
		hotmail.de	–	–	–
	Apple	icloud.com	–	–	–
in den USA	Comcast	comcast.net	✓, testing	mailto	✓
in Australien	Fastmail	fastmail.fm	✓, fehlt	–	–

✓: umgesetzt; –: nicht umgesetzt; Angaben aus dem DNS laut DANE Validator von sys4

versuche wünscht, der standardkonforme Verbindungsaufbau jedoch scheitern könnte und daher noch nicht zwingend einzuhalten ist. *mode: enforce* bezeichnet den voraussichtlich fehlerfreien Livebetrieb.

In diesem Modus dürfen E-Mails nur an einen MX gesendet werden, dessen Name zu einem der angegebenen Muster passt. Er muss STARTTLS beherrschen und sein Zertifikat muss gültig sein und von einer vertrauenswürdigen CA für diesen Host als Subject Alternative Name (SAN) stammen. Es sollte auch nicht auf Zertifikatsperrlisten (Certificate Revocation List, CRL) auftauchen. *mode: none* schließlich bedeutet, die Domain so zu behandeln, als besäße sie gar keine MTA-STS-Policy.

Policies zum langsamen Herantasten

Dank der Policy-Abstufungen können Domain-Administratoren MTA-STS schrittweise einführen. Zunächst können sie mit einer *testing*-Policy Erfahrungen sammeln. Falls dabei keine Schwierigkeiten auftreten, stellen sie auf *enforce* um. Hierzu sollten sie erst die Policy auf dem HTTPS-Endpunkt anpassen und dann die *id* der aktuellen Policy auf einen bisher nicht genutzten Wert ändern. Spätestens nach Ablauf von *max_age* sollten alle Einlieferer die neue Policy nutzen.

Wer umgekehrt aus MTA-STS aussteigen will, muss ebenso zuerst die Policy ändern, in diesem Fall auf *none*, und dann die *id* im TXT Record auf einen neuen Wert setzen. Nach Ablauf von *max_age* lassen sich der DNS-Eintrag und die per HTTPS veröffentlichte Policy entfernen. Das kann allerdings auch ein hinreichend mächtiger Angreifer umsetzen.

Schutz vor diesem Szenario bietet DANE, aber nicht MTA-STS allein. Der Einsatz der STARTTLS Policy List der Electronic Frontier Foundation (EFF) bietet Unterstützung: Die Liste enthält Mailserver, die den STARTTLS-Mindestvorgaben der EFF genügen.

Doch wie erfährt der Administrator des empfangenden Mailservers, ob MTA-STS gut oder schlecht funktioniert? Dabei helfen die bereits erwähnten Berichte.

Ein guter Mechanismus zum Melden von Zustellfehlern kann die Akzeptanz neuer Standards erhöhen. Wenn die Seite der Kommunikation, die einen Fehler entdeckt, der auslösenden Seite die Ursache mitteilt, lässt sich die Ursache schnell beheben. Ein prominentes Beispiel ist DMARC: Informiert der vorgesehene Empfänger einer Nachricht den Absender darüber, dass die Überprüfung fehlschlägt, kann Letzterer seine Konfiguration korrigieren oder gegen den vorgeblichen Absender vorgehen.

Reporting: Zeige mir meine Fehler

DMARC sieht für das Reporting zweierlei Rückmeldungen vor: forensische Berichte über einzelne Fehler *(ruf)* und Zusammenfassungen über einen längeren Zeitraum *(rua)*. Die forensischen Berichte galten bereits vor der DSGVO als datenschutzrechtlich heikel und sind daher kaum im Einsatz.

Aus der Entwicklung von MTA-STS heraus ist SMTP TLS Reporting entstanden (RFC 8460), ein Standard für Fehlerberichte, der nicht nur MTA-STS berücksichtigt, sondern sich auch für DANE eignet. Auf die umstrittenen forensischen Berichte verzichtet er wohlweislich. Eine Domain fordert Berichte über einen TXT-Record unter dem Label *_smtp._tls* an:

```
smtp._tls.example.com. IN TXT ⤸
    "v=TLSRPTv1;rua=mailto:reports@example.com"
```

Der Schlüssel *v* bezeichnet wieder die Version des Standards, *rua* gibt den Endpunkt zum Versenden der Berichte in Form einer URL an. Berichte lassen sich per E-Mail und per POST-Request an eine HTTPS-URL versenden. E-Mails sind vollständig mittels DKIM zu signieren – die Signatur darf sich also nicht nur auf einen Teil der Nachricht beziehen – und der Selektor muss vom Servicetyp *tlsrpt* sein:

```
dkim_selector._domainkey.example.com. TXT ⤸
   "v=DKIM1;k=rsa;s=tlsrpt;p=Mlf4qwSZfase4fa=="
```

Vielversprechende Mitstreiter

Die Berichte sind JSON-formatiert, das zugehörige Schema spezifiziert der RFC. Ein Bericht sollte den Zeitraum von einem Tag umfassen und zwecks Lastverteilung nicht immer zum gleichen Zeitpunkt versendet werden. Berichte enthalten neben der Anzahl erfolgreicher und fehlgeschlagener Zustellungen auch die Fehlergründe. Je nach Fehlertyp sind verschiedene Kennungen registriert, etwa bezüglich TLS, DANE oder MTA-STS, die die Diagnose erleichtern sollen.

Wie die Chancen für die breite Umsetzung eines neuen Standards stehen, zeigt ein Blick auf dessen Autoren und Unterstützer. Im RFC für MTA-STS finden sich Mitarbeiter von Google, Oath, Comcast, Microsoft und 1&1, was für ein großes Interesse in der Branche spricht. Ende Oktober 2018, wenige Wochen nach Verabschiedung der Standards, befanden sich bereits einige MTA-STS-Policies und Reporting-Endpunkte im Test. Bisher kommt offenbar ausschließlich E-Mail als Berichtsweg zum Einsatz.

Viele große Mailboxprovider testen den Standard direkt auf ihren häufig genutzten Haupt-Domains. Manchmal ist die Umsetzung jedoch noch unvollständig. Großes Interesse herrscht derzeit offenbar insbesondere in Deutschland – anders als in den Nachbarländern.

Um die Relevanz für die eigenen Ziel-Domains abzuschätzen, reicht ein kurzes Skript, in das man die häufigsten Zustell-Domains des eigenen Mailservers einfügt:

```
#!/bin/bash
for domain in example.com example.net; do
  echo $domain:
  host -t txt _mta-sts.$domain
  curl -s "https://mta-sts.$domain/ ⤸
                        .well-known/mta-sts.txt"
  host -t txt _smtp._tls.$domain
done
```

Fazit

Möchten Administratoren den Mailtransport zu ihrer Domain absichern, scheint MTA-STS eine gute Option zu sein. Es lässt sich relativ einfach umsetzen und verbreitet sich derzeit rasch. Um den Cache zu füllen, ist jedoch eine gewisse Menge an ausgehendem Mailverkehr nötig und das Verfahren mit der STARTTLS Policy List der EFF zu kombinieren.

Noch mehr Sorgfalt sollten Administratoren daher auch bei der Auswahl ihres Hosters walten lassen und ihn nach dessen Umsetzung für DNSSEC aussuchen, um DANE implementieren zu können. DANE ist im deutschsprachigen Raum bereits relativ weit verbreitet und bietet von Anfang an ohne Rücksicht auf Cache-Belange ein höheres Schutzniveau. (un@ix.de)

Sven Krohlas

ist E-Mail-Spezialist und IT Security Consultant bei der BFK edv-consulting GmbH in Karlsruhe.

Alle Links: ix.de/ix1812110