MTA-STS i TLS-RPT: szyfrowanie poczty między serwerami, a BIMI informacyjnie

◫◫ Poziom: średnio

◫◫ Dotyczy: MTA-STS (RFC 8461), TLS-RPT (RFC 8460), MailCow 2025-09 lub nowszy (zakładka MTA-STS, kontener postfix-tlspol-mailcow), Exchange Online, Gmail, Traefik na docker01, nginx 1.30.6, BIMI, stan na 26 października 2026

▯ Czas: ~40 min

Poczta między serwerami jest szyfrowana tylko wtedy, gdy obie strony się na to zgodzą, a napastnik w środku może tę zgodę po cichu zablokować. MTA-STS ogłasza światu, że nasze serwery pocztowe zawsze mają szyfrowanie z ważnym certyfikatem, a TLS-RPT każe nadawcom raportować, gdy coś się nie udało. Na końcu krótko o BIMI, czyli logo firmy w skrzynce odbiorcy.

◫◫ ZAŁOŻENIA SCENARIUSZA

w tym ćwiczeniu poczta działa w podejściu A, MailCow w wersji 2026-07a stoi na `docker01` za Traefikiem (certyfikaty Let's Encrypt przez Traefika, `acme-mailcow` wyłączony), a zapasowy MX `poczta2.zielona.example` to Postfix na `edge-az01` z wariantu b na stronie Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate. W podejściach B i C plik polityki wystawiamy na `docker01` w osobnym kontenerze nginx, co opisujemy niżej.

◫◫ Skróty użyte na tej stronie (22)

Skrót	Co znaczy
BIMI	Brand Indicators for Message Identification: rekord DNS wskazujący logo firmy, które skrzynka odbiorcy może pokazać obok nadawcy, gdy wiadomość przeszła DMARC
CMC	Common Mark Certificate: certyfikat logo dla BIMI bez zarejestrowanego znaku towarowego; Gmail pokazuje przy nim logo, ale bez znaczka weryfikacji

Skrót	Co znaczy
CNAME	Canonical Name: rekord DNS będący aliasem, drugą nazwą wskazującą na już istniejący rekord A
DANE	DNS-based Authentication of Named Entities: odcisk certyfikatu serwera opublikowany w rekordzie TLSA podpisanej strefy, po którym nadawca sprawdza, że rozmawia z właściwym serwerem
DMARC	Domain-based Message Authentication, Reporting and Conformance: reguła domeny mówiąca, co robić z mailem, który nie przeszedł SPF i DKIM
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DNSSEC	DNS Security Extensions: podpisy cyfrowe w DNS, dzięki którym można sprawdzić, że odpowiedź nie została po drodze podmieniona
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
JSON	JavaScript Object Notation: tekstowy format danych z klamrami i cudzysłowami
MTA-STS	Mail Transfer Agent Strict Transport Security: zasada opublikowana przez domenę, że poczta do niej ma być wysyłana wyłącznie szyfrowanym połączeniem z serwerem o ustalonej nazwie
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny
PS	PowerShell: powłoka i język skryptowy Windowsa (w Linuksie ps to polecenie process status)
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty
STARTTLS	włączenie szyfrowania w trakcie już nawiązanej, nieszyfrowanej sesji pocztowej
SVG	Scalable Vector Graphics: format grafiki wektorowej, którą można skalować bez utraty ostrości
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
TLS-RPT	SMTP TLS Reporting: rekord _smtp._tls z adresem, na który serwery nadawców wysyłają raz na dobę raport o udanych i nieudanych szyfrowanych połączeniach z naszymi serwerami poczty (RFC 8460)
TLSA	rekord DNS, w którym domena publikuje odcisk certyfikatu swojego serwera, żeby inni mogli sprawdzić, że łączą się z właściwą maszyną (mechanizm DANE)
TXT	typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC
UTC	Coordinated Universal Time: uniwersalny czas bez strefy, punkt odniesienia dla wszystkich stref czasowych na świecie
VMC	Verified Mark Certificate: certyfikat logo dla BIMI, wydawany przez urząd certyfikacji na podstawie zarejestrowanego znaku towarowego; daje znaczek weryfikacji w Gmailu

Fiszka

Odczyty robimy z dowolnego Linuksa spoza sieci Zielonej. Zmiany w MailCow robimy w panelu administratora, a pliki na `docker01` jako użytkownik z uprawnieniami sudo.

□□ TYLKO ODCZYT

Odczyt sygnału MTA-STS: dig TXT _mta-sts

```
dig +short TXT _mta-sts.NazwaDomeny
```

Rekord mówi nadawcom, że domena ma politykę, a pole `id` zmienia się przy każdej zmianie polityki, żeby nadawcy pobrali ją od nowa.

Przykład (poglądowy):

```
"v=STSv1; id=20261027170000"
```

□□ **MTA-STS** = Mail Transfer Agent Strict Transport Security: zasada opublikowana przez domenę, że poczta do niej ma być wysyłana wyłącznie szyfrowanym połączeniem z serwerem o ustalonej nazwie · **TXT** = typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC · **dig** = domain information groper: odpytywanie DNS

□□ TYLKO ODCZYT

Pobranie pliku polityki: curl

```
curl -s https://mta-sts.NazwaDomeny/.well-known/mta-sts.txt
```

Dokładnie to samo robi serwer nadawcy. Odpowiedź musi przyjść od razu, bez przekierowania, z kodem 200 i przez HTTPS z ważnym certyfikatem dla nazwy `mta-sts`.

Przykład:

```
version: STSv1
mode: testing
mx: poczta.zielona.example
mx: poczta2.zielona.example
max_age: 86400
```

□□ **HTTPS** = HTTP zabezpieczony szyfrowaniem TLS · **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

□□ ZMIENIA SYSTEM

Sprawdzenie certyfikatu hosta polityki: openssl s_client

```
openssl s_client -connect mta-sts.NazwaDomeny:443 -servername mta-sts.NazwaDomeny
</dev/null 2>/dev/null | openssl x509 -noout -subject -enddate
```

Pokazuje, na jaką nazwę wystawiono certyfikat i kiedy wygasa. Wygasły certyfikat na `mta-sts` nie psuje dostarczania od razu, ale nadawcy przestają odświeżać politykę.

Przykład:

```
subject=CN=mta-sts.zielona.example
notAfter=Jan 24 17:02:11 2027 GMT
```

openssl = zestaw narzędzi do certyfikatów i szyfrowania

ZMIENIA SYSTEM

Sprawdzenie szyfrowania i certyfikatu serwera MX: openssl s_client -starttls smtp

```
openssl s_client -starttls smtp -connect NazwaSerweraMX:25 -servername NazwaSerweraMX
</dev/null 2>/dev/null | openssl x509 -noout -subject -enddate
```

(gdzie `NazwaSerweraMX` to każda nazwa z rekordów MX, w Zielonej `poczta.zielona.example` i `poczta2.zielona.example`)

W trybie `enforce` nadawca dostarczy pocztę tylko do serwera, który ma STARTTLS i certyfikat ważny dla nazwy z polityki. Sprawdzamy więc każdy MX, także zapasowy.

MX = Mail Exchanger: rekord DNS wskazujący serwer poczty domeny · **STARTTLS** = włączenie szyfrowania w trakcie już nawiązanej, nieszyfrowanej sesji pocztowej · **openssl** = zestaw narzędzi do certyfikatów i szyfrowania

TYLKO ODCZYT

Odczyt adresu raportów TLS: dig TXT _smtp._tls

```
dig +short TXT _smtp._tls.NazwaDomeny
```

Przykład:

```
"v=TLSRPTv1; rua=mailto:raporty-tls@zielona.example"
```

TLS = Transport Layer Security: szyfrowanie połączeń, np. w HTTPS · **TXT** = typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC · **dig** = domain information groper: odpytywanie DNS

KLIKAMY W INTERFEJSIE

Ustawienie polityki w MailCow: zakładka MTA-STS domeny

```
E-Mail → Configuration → Domains → (zielona.example) → Edit → MTA-STS → Version STSv1, Mode, Maximum Age, MX → Active → Save changes
```

MailCow od wersji 2025-09 generuje politykę dynamicznie z tych pól i nadaje nowe `id` przy każdym zapisie. Aktualną wartość rekordu `_mta-sts` pokazuje przycisk DNS przy domenie.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: zakładka MTA-STS w oknie edycji domeny `zielona.example` w MailCow, tryb `testing`, Maximum Age 86400, pole MX z wpisami `poczta.zielona.example,poczta2.zielona.example`, zaznaczone Active.

MTA-STS = Mail Transfer Agent Strict Transport Security: zasada opublikowana przez domenę, że poczta do niej ma być wysyłana wyłącznie szyfrowanym połączeniem z serwerem o ustalonej nazwie · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **MX** = Mail Exchanger: rekord DNS wskazujący serwer poczty domeny

PLIK KONFIGURACYJNY

Dopisanie nazwy mta-sts do routera Traefika: docker-compose.override.yml

```
services:
  nginx-mailcow:
    labels:
      - "traefik.http.routers.poczta.rule=Host(`poczta.zielona.example`) || Host(`mta-sts.zielona.example`)"
```

Plik konfiguracyjny: zmieniona linia reguły w `/docker/apps/mailcow/docker-compose.override.yml` z Instalacja MailCow na docker01 od zera; pozostałe etykiety zostają

bez zmian. Traefik dołącza wtedy nazwę `mta-sts` do certyfikatu i kieruje ją do panelu MailCow, który odpowiada plikiem polityki. Po zmianie wykonujemy `sudo docker compose up -d` w `/docker/apps/mailcow`.

□□ TYLKO ODCZYT

Plik polityki dla Microsoft 365 albo Google Workspace: mta-sts.txt

```
version: STSv1
mode: testing
mx: *.mail.protection.outlook.com
max_age: 604800
```

Plik konfiguracyjny `/docker/apps/mta-sts/html/.well-known/mta-sts.txt` dla podejścia B. W podejściu C linia `mx` ma wartość `smtp.google.com`, a przy starszych wartościach `aspmx` wpisujemy każdą nazwę z rekordów MX. Microsoft zaznacza, że wieloznaczny wpis `*.mail.protection.outlook.com` jest wyjątkiem dla Exchange Online, a dla domeny z rekordem MX w nowej strefie `mx.microsoft` właściwy wpis sprawdzamy w dokumentacji.

□□ **MX** = Mail Exchanger: rekord DNS wskazujący serwer poczty domeny

□□ PLIK KONFIGURACYJNY

Wystawienie pliku polityki na docker01: compose.yaml

```
services:
  mta-sts:
    image: nginx:1.30.6-alpine
    container_name: mta-sts
    restart: unless-stopped
    volumes:
      - /docker/apps/mta-sts/html:/usr/share/nginx/html:ro
    networks:
      - proxy
    labels:
      - "traefik.enable=true"
      - "traefik.docker.network=proxy"
      - "traefik.http.routers.mta-sts.rule=Host(`mta-sts.zielona.example`)"
      - "traefik.http.routers.mta-sts.entrypoints=websecure"
```

```
      - "traefik.http.routers.mta-sts.tls=true"
      - "traefik.http.routers.mta-sts.tls.certresolver=letsencrypt"
      - "traefik.http.services.mta-sts.loadbalancer.server.port=80"

networks:
  proxy:
    external: true
```

Plik konfiguracyjny `/docker/compose/mta-sts/compose.yaml` dla podejść B i C. Rekord `mta-sts` wskazuje wtedy publiczny adres `docker01` (203.0.113.10), a nie serwer poczty, bo pocztę obsługuje Microsoft albo Google.

> W naszym środowisku dane aplikacji trzymamy w `/docker/apps/<nazwa>`, a plik Compose w `/docker/compose/<nazwa>/compose.yaml`. To konwencja, nie wymóg Dockera: można ją zmienić, byle w całej firmie była jedna. Katalog `/docker` to osobny wolumen `vgDocker/lvDocker`, żeby pełny dysk aplikacji nie zatrzymał systemu.

Z życia wzięte

Z ŻYCIA WZIĘTE

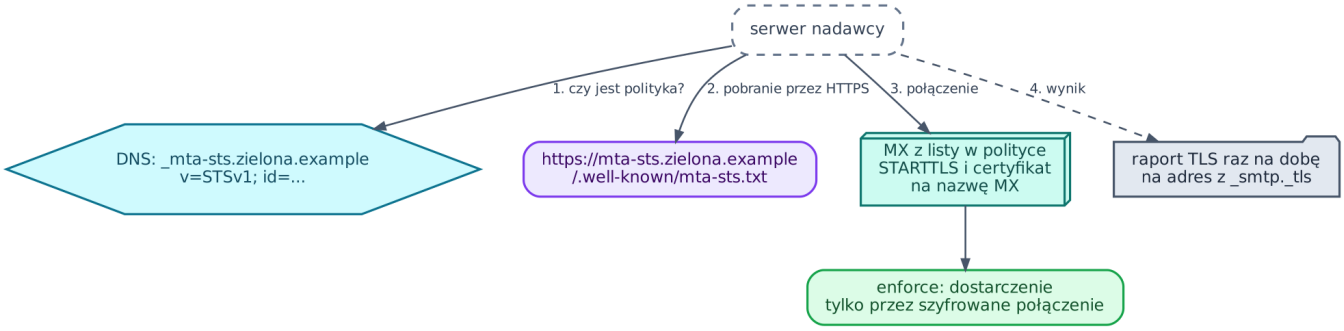
Poniedziałek, 6:50. Po weekendowej awarii światłowodu poczta od dużego odbiorcy hurtowego nie dochodzi, choć `edge-az01` działa i MX 20 przyjmuje połączenia. Tomek znajduje w raporcie TLS od tego nadawcy błędy `certificate-host-mismatch` dla `poczta2.zielona.example`: Postfix na `edge-az01` przedstawiał się certyfikatem z nazwą maszyny, a polityka MTA-STS była w trybie `enforce`. Nadawca zrobił dokładnie to, o co prosiliśmy, czyli nie oddał poczty serwerowi z niepasującym certyfikatem, i trzymał ją w kolejce. Od tej pory certyfikat `poczta2` jest w inwentarzu, a test `openssl s_client` dla obu MX stoi w procedurze próby przełączenia łącza.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: STARTTLS. Polecenie, którym serwer nadawcy prosi serwer odbiorcy o przejście na szyfrowanie w trakcie zwykłego połączenia SMTP. Gdy odbiorca nie ogłosi tej możliwości, nadawca zwykle wysyła bez szyfrowania. Napastnik między serwerami może usunąć to ogłoszenie z odpowiedzi i poczta pójdzie otwartym tekstem, a nikt się nie dowie.

Pojęcie: MTA-STS (Mail Transfer Agent Strict Transport Security). Zasada ogłaszana przez właściciela domeny: „moja poczta przychodzi tylko na te serwery MX, zawsze z TLS i z certyfikatem od publicznego urzędu". Nadawca pobiera politykę przez HTTPS z `https://mta-sts.domena/.well-known/mta-sts.txt`, zapamiętuje ją na `max_age` sekund i w trybie `enforce` nie dostarczy poczty, gdy warunki nie są spełnione.



Rysunek 1. Jak nadawca używa MTA-STS: pyta DNS o rekord _mta-sts, pobiera politykę przez HTTPS z mta-sts.zielona.example, łączy się z MX z listy, wymaga STARTTLS i certyfikatu pasującego do nazwy, a wynik raportuje raz na dobę na adres z rekordu _smtp._tls (kliknięcie otwiera pełny rozmiar)

Polityka ma cztery pola. `version` to zawsze `STSv1`. `mode` przyjmuje wartości `testing` (sprawdzaj i raportuj, ale dostarczaj), `enforce` (nie dostarczaj, gdy coś nie pasuje) albo `none` (wycofanie polityki). `mx` wymienia dozwolone serwery, każdy w osobnej linii, z jednym poziomem gwiazdki na początku. `max_age` to czas pamiętania polityki w sekundach, najwyżej 31 557 600, czyli rok.

Etap	`mode`	`max_age`	Ile trwa
Start	`testing`	86400 (MailCow zaleca dobę) albo 604800	dwa tygodnie, Google zaleca 1 do 2 tygodni dla testów
Wymuszenie	`enforce`	604800	po dwóch tygodniach czystych raportów TLS

Etap	`mode`	`max_age`	Ile trwa
Wycofanie	`none`	krótki, na przykład 86400	gdy zmieniamy dostawcę poczty; nadawcy zapominają politykę po starym `max_age`

Najważniejsza pułapka: polityka obejmuje każdy MX. Zapasowy `poczta2.zielona.example` na `edge-az01` musi mieć STARTTLS i certyfikat od publicznego urzędu wystawiony na tę nazwę, inaczej przy awarii światłowodu nadawcy w trybie `enforce` przytrzymają pocztę w kolejkach. To samo dotyczy zmiany podejścia: przed przejściem z MailCow do Microsoft 365 albo Google publikujemy nową politykę w trybie `testing` z nowymi MX i nowym `id`, a dopiero po upływie starego `max_age` przełączamy rekordy MX.

Gdzie leży plik polityki

Podejście	Gdzie leży polityka	Rekord `mta-sts`	Certyfikat
A: MailCow	MailCow generuje ją dynamicznie (od 2025-09)	CNAME do `poczta.zielona.example`	Traefik na `docker01`, nazwa dopisana do reguły routera
B: Microsoft 365	Exchange Online nie wystawia polityki za klienta; plik na `docker01` w kontenerze nginx albo statyczna strona w Azure (Microsoft zaleca Azure Static Web Apps)	A 203.0.113.10 albo CNAME do hostingu	Traefik albo hosting; urząd hostingu dopisujemy do CAA
C: Google Workspace	Google nie wystawia polityki; plik na `docker01` jak w B	A 203.0.113.10	Traefik

Wyjście w drugą stronę, czyli przestrzeganie cudzych polityk przy wysyłce, mają wszystkie trzy podejścia. MailCow od wersji 2025-09 robi to kontenerem `postfix-tlspol-mailcow`, Exchange Online sprawdza polityki odbiorców zawsze i bez ustawień, a Gmail stosuje się do polityk w trybie `enforce`.

TLS-RPT: raporty o szyfrowaniu

> **Pojęcie: TLS-RPT (SMTP TLS Reporting).** Rekord TXT `_smtp._tls` z adresem, na który serwery nadawców wysyłają raz na dobę (od 00:00 do 24:00 UTC) raport w JSON: ile połączeń z naszymi MX się udało, a ile nie i dlaczego. Raporty przychodzą jako załączniki

> skompresowane gzipem z tematem zaczynającym się od „Report Domain:”.

W Zielonej raporty TLS trafiają na alias `raporty-tls@`, czyli do tej samej skrzynki co raporty DMARC, a parsedmarc z opcją `save_smtp_tls` przetwarza je razem z nimi, jak opisuje Droga DMARC od p=none do p=reject z raportami parsedmarc na docker01. Najczęstsze typy błędów w raportach i ich znaczenie:

Typ błędu w raporcie	Co znaczy	Gdzie szukamy
`starttls-not-supported`	serwer MX nie zaproponował szyfrowania	konfiguracja Postfiksa na danym MX
`certificate-host-mismatch`	certyfikat nie ma nazwy MX	certyfikat MX, zwłaszcza zapasowego
`certificate-expired`	certyfikat MX wygasł	odnowienie przez Traefika albo na `edge-az01`
`certificate-not-trusted`	certyfikat od urzędu, którego nadawca nie zna (na przykład z `CA-Zielona`)	MX musi mieć certyfikat publiczny
`sts-policy-fetch-error`	nadawca nie pobrał polityki	Traefik, rekord `mta-sts`, certyfikat hosta polityki
`sts-policy-invalid`	błąd składni polityki	plik polityki, końce linii, nazwy w `mx`
`validation-failure`	inny błąd sprawdzania	szczegóły w polu z opisem błędu w raporcie

DANE: druga droga do tego samego celu

DANE osiąga ten sam efekt bez HTTPS: w podpisanej strefie publikujemy rekord TLSA z odciskiem certyfikatu serwera pocztowego, a nadawca sprawdza go przez DNSSEC. Wymaga więc podpisanej strefy, co opisuje Rekordy publiczne Zielonej, DNSSEC i CAA, i pilnowania rekordu TLSA przy każdej wymianie klucza certyfikatu. Exchange Online obsługuje DANE dla poczty przychodzącej od października 2024 roku. W Zielonej zaczynamy od MTA-STS, bo działa u większości dużych nadawców bez dodatkowych kluczy, a DANE rozważymy po roku z DNSSEC.

BIMI informacyjnie

>

> **Pojęcie: BIMI (Brand Indicators for Message Identification).** Rekord TXT `default._bimi` ze wskazaniem logo firmy w formacie SVG Tiny PS i, opcjonalnie, certyfikatu logo. Skrzynki, które go obsługują, pokazują logo obok nadawcy, ale tylko dla wiadomości, które przeszły DMARC.

Warunek	Szczegóły
DMARC w trybie wymuszenia	`quarantine` albo `reject` dla domeny i poddomen; `p=none` i wartości `pct` poniżej 100 nie wystarczą
Logo	plik SVG w profilu Tiny PS, publicznie pod adresem HTTPS
Certyfikat logo	VMC (Verified Mark Certificate) oparty na zarejestrowanym znaku towarowym albo CMC (Common Mark Certificate) bez znaku towarowego; Gmail obsługuje CMC od września 2024 roku, ale znaczek weryfikacji pokazuje tylko przy VMC
Rekord	`default._bimi.zielona.example TXT "v=BIMI1; l=https://...; a=https://..."`

Dla Zielonej BIMI to pomysł na później: warunkiem jest `p=reject` z poprzedniej strony, a certyfikat logo kosztuje i wymaga dokumentów firmy. Wracamy do tematu, gdy dział handlowy zacznie wysyłać newsletter do tysięcy odbiorców i zapyta, jak wyróżnić się w skrzynce. Którzy dostawcy poczty pokazują logo, sprawdzamy w aktualnym zestawieniu BIMI Group.

Częste błędy

Objaw	Przyczyna	Co robimy
Raporty TLS pokazują `sts-policy-fetch-error`	brak nazwy `mta-sts` w regule Traefika albo w certyfikacie	reguła routera z Fiszki, `openssl s_client` na `mta-sts`
Polityka pobrana w przeglądarce, a nadawcy jej nie widzą	odpowiedź przychodzi przez przekierowanie (na przykład z `http` albo na inny adres)	RFC 8461 zakazuje podążania za przekierowaniami; plik wystawiamy pod dokładnym adresem
Zmiana polityki nie działa	`id` w rekordzie `_mta-sts` bez zmiany	w MailCow zapisujemy zmianę w zakładce (nowe `id`), w B i C zmieniamy `id` ręcznie
Po przejściu na `enforce` poczta czeka w kolejkach nadawców	jeden z MX nie ma STARTTLS albo certyfikat nie pasuje	test `openssl s_client -starttls smtp` dla każdego MX, powrót do `testing`
Po migracji do Microsoft 365 część poczty nie dochodzi przez kilka dni	stara polityka z MX MailCow zapamiętana przez nadawców	nowa polityka w `testing` przed zmianą MX, odczekanie starego `max_age`

Objaw	Przyczyna	Co robimy
Brak raportów TLS	brak rekordu `_smtp._tls` albo raporty lądują w Junk	`dig` rekordu, lista dozwolonych w skrzynce raportów
Certyfikat dla `mta-sts` nie powstaje w zewnętrznym hostingu	rekord CAA nie dopuszcza urzędu hostingu	dopisujemy urząd do CAA

□□ Ćwiczenia

1. Dlaczego sam STARTTLS bez MTA-STS nie chroni poczty przed podsłuchem?

Odpowiedź

Bo nadawca, który nie dostanie ogłoszenia STARTTLS, wyśle wiadomość bez szyfrowania i nie potraktuje tego jako błędu. Napastnik między serwerami może usunąć ogłoszenie z odpowiedzi. MTA-STS mówi nadawcy z góry, że szyfrowanie z ważnym certyfikatem jest obowiązkowe, więc w trybie `enforce` nadawca nie wyśle poczty otwartym tekstem.

1. Zielona planuje przejście z MailCow do Google Workspace. Co robimy z polityką MTA-STS i w jakiej kolejności?

Odpowiedź

Najpierw stawiamy kontener nginx z nową polityką (MX `smtp.google.com`, tryb `testing`), zmieniamy rekord `mta-sts` na adres `docker01` i nadajemy nowe `id`. Czekamy, aż minie `max_age` starej polityki, przełączamy MX na Google, sprawdzamy raporty TLS i dopiero wtedy wracamy do `enforce`.

1. Raport TLS pokazuje `certificate-not-trusted` dla `poczta.zielona.example`. Co się mogło stać?

Odpowiedź

Serwer poczty przedstawia certyfikat, któremu nadawca nie ufa, na przykład wystawiony przez wewnętrzny urząd `CA-Zielona` zamiast Let's Encrypt, albo bez pełnego łańcucha. Serwery MX widoczne z internetu muszą mieć certyfikat od publicznego urzędu.

1. Pan Zbigniew widział logo banku przy wiadomości w Gmailu i chce takie samo dla Zielonej „od jutra”. Co odpowiadamy?

Odpowiedź

Że BIMI wymaga najpierw DMARC w trybie `quarantine` albo `reject` dla całej domeny (w Zielonej planowo od lutego 2027 roku), logo w formacie SVG Tiny PS i zwykle certyfikatu logo. Certyfikat VMC wymaga zarejestrowanego znaku towarowego, a CMC go nie wymaga, ale Gmail pokazuje przy nim logo bez znaczka weryfikacji. Od jutra się nie da, za kilka miesięcy tak.

Powiązane: Rekordy publiczne Zielonej, DNSSEC i CAA · SPF, DKIM i DMARC: trzy podejścia do poczty i systemy wysyłające w imieniu domeny · Instalacja MailCow na docker01 od zera · MailCow: codzienna praca z domenami, skrzynkami i spamem · Reverse proxy w Dockerze: Traefik przed wszystkimi aplikacjami na docker01 · Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate

Źródła (odczyt 26 października 2026): rfc-editor.org: RFC 8461 (wrzesień 2018; `_mta-sts`, plik polityki, `testing`, `enforce`, `none`, `max_age` do 31 557 600, zakaz przekierowań, certyfikat dla nazwy `mta-sts`), RFC 8460 (wrzesień 2018; `_smtp._tls`, `v=TLSRPTv1`, raport dobowy w JSON, gzip, temat „Report Domain:”) · docs.mailcow.email, „Setting up MTA-STS” (wersja 2025-09, zakładka w oknie domeny, polityka generowana dynamicznie, CNAME `mta-sts`, zalecane 86400 s) · emailexpert.com, aktualizacja MailCow z września 2025 (`postfix-tlspol-mailcow`) · learn.microsoft.com, „Enhancing mail flow with MTA-STS” (Exchange Online sprawdza polityki przy wysyłce, nie wystawia polityki za klienta, `*.mail.protection.outlook.com`, Azure Static Web Apps) · knowledge.workspace.google.com, „About MTA-STS and TLS reporting” i „Create an MTA-STS policy” (Gmail przestrzega polityk w trybie `enforce`, test 1 do 2 tygodni) · bleepingcomputer.com, Exchange Online inbound DANE (28 października 2024) · bimigroup.org, „Implementation Guide” · workspaceupdates.googleblog.com, „Gmail: additional BIMI protections” (CMC od 24 września 2024, znaczek tylko z VMC) · nginx.org, wersja stabilna 1.30.6.

Revision #2
Created 2026-10-26 14:06:18 UTC by Tomasz Konieczny
Updated 2026-10-26 14:28:38 UTC by Tomasz Konieczny