

Securing Security – DNSSEC und DANE

Patrick Koetter und Carsten Strotmann, sys4 AG

DNSSEC als neue Internet PKI

- die traditionelle Internet PKI über Zertifizierungsstellen (CA) ist problematisch:
 - allen CAs muss ultimativ vertraut werden
 - es gibt zu viele CAs (2.000 +)
 - Sicherheit des Modells nur so gut wie Sicherheit des schwächsten Glied
- Ziel: Kontrolle über Trust und Policies zurückerhalten

DNSSEC als neue Internet PKI

- DANE - DNS(SEC) Authenticated Named Entities ersetzt die Funktion der CAs durch DNSSEC
 - Besitzer einer Domain hat die Autorität, im Namen der Domain Inhalte zu publizieren
 - DNSSEC authentisiert die Inhalte
 - Sicherheit-Level ist gleichwertig mit Domain-Validated (DV) x509-Zertifikaten
 - ↪The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

DNSSEC als neue Internet PKI

- der Besitzer einer DNSSEC-signierten Domain erstellt oder erhält ein x509-Zertifikat
- der Besitzer der Domain publiziert den Hash des Zertifikats im DNS (TLSA-Record, DNSSEC gesichert) und konfiguriert das Zertifikat auf dem Dienst (Server)

DNSSEC als neue Internet PKI

- Beispiel eines TLSA-Records (für einen der GMX.DE Mail-Server):

```
% dig _25._tcp.mx01.emig.gmx.net tlsa +multi

; <<>> DiG 9.10.4-P4-RedHat-9.10.4-2.P4.fc25 <<>> _25._tcp.mx01.emig.gmx.net tlsa +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29351
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_25._tcp.mx01.emig.gmx.net. IN TLSA

;; ANSWER SECTION:
_25._tcp.mx01.emig.gmx.net. 293 IN TLSA 3 1 1 (
                                9BDE51EA74128A327A6A4F3A4F21CBA855475DCF88BC
                                1532A2B45B35E16E6D61 )

;; WHEN: Mon Dec 19 07:41:58 CET 2016
;; MSG SIZE rcvd: 102
```

DNSSEC als neue Internet PKI

- DANE-fähiger Client prüft ob das vom Server präsentierte x509-Zertifikat mit den Informationen (Hash) im TLSA-Record übereinstimmt
- Dienst-Domain-Name wird über den Namen des TLSA-Records abgeglichen. Der Common-Name (CN) oder die Domain-Namen im Zertifikat müssen *nicht* mit dem Server-Namen des Dienstes übereinstimmen
- Zertifikat ist solange gültig, wie ein passenden TLSA-Record im DNS existiert. Das Ablauf-Datum (Expire-Time) des x509-Zertifikats wird *nicht* ausgewertet
- Zertifikats-Kette des x509-Zertifikats muss *nicht* ausgewertet werden. Vertrauensstellung zum Zertifikat wird über DNSSEC und den TLSA-Record etabliert

DANE-TLSA

- DANE-TLSA ist spezifiziert für
 - SMTP (E-Mail)
 - HTTPS (Web) (Client-Browser Support fehlt)
 - IRC
 - XMPP/Jabber
 - generische Dienste mit SRV-Records (RFC 7673)
 - ...

DANE-SMTP

- Technische Richtlinie BSI TR-03108, "Sicherer E-Mail-Transport"
 - Anforderungen an E-Mail-Diensteanbieter für einen sicheren Transport von E-Mail
 - "Zertifikate ... mittelfristig automatisiert durch ... DANE/TLSA ... über DNSSEC ... gesicherte Verbindung vom ... EMDA" abrufen
 - DANE wird "Verpflichtend bei Re-Zertifizierung"
 - posteo.de als erster Mail-Provider im Dezember 2016 zertifiziert
 - mail.de als erster Mail-Provider in 2022 mit IT-Sicherheitskennzeichen

DANE-SMTP

- weitere DANE-SMTP Anbieter:
 - Mailbox.org
 - Web.de/Gmx.de
 - mail.de
 - bund.de
 - Microsoft
 - GMail (Inbound - für spezielle Kunden)
 - viele Universitäten (z.B. Bayrisches Hochschulnetz)

DANE-SMTP

• DANE-SMTP Nutzer

gmx.at	lrz.de	ouderportaal.nl
travelbirdbelgie.be	mail.de	overheid.nl
travelbirdbelgique.be	posteo.de	pathe.nl
nic.br	ruhr-uni-bochum.de	uvt.nl
registro.br	tum.de	xs4all.nl
gmx.ch	uni-erlangen.de	domeneshop.no
open.ch	one.com	handelsbanken.no
switch.ch		webcruitermail.no
anubisnetworks.com	web.de	aegee.org
gmx.com	egmontpublishing.dk	debian.org
isavedialogue.com	netic.dk	freebsd.org
mail.com	tilburguniversity.edu	gentoo.org
solvinity.com	octopuce.fr	ietf.org
t-2.com	comcast.net	isc.org
trashmail.com	dd24.net	netbsd.org
xfinity.com	dns-oarc.net	openssl.org
xfinityhomesecurity.com	gmx.net	samba.org
xfinitymobile.com	hr-manager.net	torproject.org
nic.cz	mpssec.net	asf.com.pt
bayern.de	t-2.net	handelsbanken.se
bund.de	xs4all.net	t-2.si
fau.de	bhosted.nl	mail.co.uk
freenet.de	boozishop.nl	govtrack.us
gmx.de	hierinloggen.nl	

DANE-SMTP

- DANE-SMTP Domains nach Ländern (09/2023)

Land	DANE Domains
Deutschland	3553
USA	1894
Niederlande	1886
Frankreich	822
Tschechische Republik	443
Grossbritannien	369

- DANE schützt AnwenderInnen! Anzahl der Domains ist nicht aussagekräftig.

Einige dieser Domains schützen Millionen von E-Mail AnwenderInnen.

DANE-SMTP

- DANE-SMTP Implementierungen:
 - postfix ([↪https://postfix.org](https://postfix.org))
 - exim ([↪Exim DANE Wiki](#))
 - opensmtpd ([↪https://www.opensmtpd.org/](https://www.opensmtpd.org/))
 - Port25
 - Halon ([↪https://halon.io/](https://halon.io/))
 - MS Exchange via Add-On Filter ([↪CryptoFilter](#))
 - MS Office 365 sendet seit Anfang 2022 und wird Ende 2023 empfangen. Siehe [↪outbound DANE](#).

Fragen?
