heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

E-Mail Made in Germany: Broken by design, überflüssig dank DANE.

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

- **Heinlein Support**
  - IT-Consulting und 24/7 Linux-Support mit ~24 Mitarbeitern
  - Eigener Betrieb eines ISPs seit 1992
  - Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen
- Mailserver-Spezialisten seit 1992
- 24/7-Notfall-Hotline: 030 / 40 50 5 - 110
  - 25 Spezialisten mit LPIC-2 und LPIC-3
  - Für alles rund um Linux & Server & DMZ
  - Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
  - Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Kill den Mythos 1:

Was hat DE-Mail mit (IT-) Sicherheit zu tun?

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Wofür ist DE-Mail da?

- DE-Mail stellt die Identität der Beteiligten sicher
- DE-Mail bietet die Möglichkeit, den Zugang einer E-Mail zu beweisen.
- DE-Mail ist vor allem ein juristisches Konstrukt mit fragwürdigem Nutzen für den Bürger.
  - DE-Mail-Mails wirken Kraft Gesetzesdefinition wie eine Postzustellungsurkunde
  - Für den Bürger ist ein schlecht gepflegter DE-Mail-Account sehr problematisch!

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Bietet DE-Mail wenigstens eine sichere Verschlüsselung?

- DE-Mail bietet keine Ende-zu-Ende-Verschlüsselung auf Basis von nutzerindividuellen Schlüsseln.
- Stattdessen wird von Station zu Station verschlüsselt.
  - Auf dem jeweiligen Speicherserver liegt die E-Mail entschlüsselt im Klartext herum.
  - Von der Qualität so wie SSL/TLS.
  - „Lawful interception“ ist also Tür und Tor geöffnet.
- DE-Mail hat nichts mit (Daten-) Sicherheit zu tun.

heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Was hat DE-Mail mit Sicherheit zu tun?

Nichts.

(Ausführlicher DE-Mail-Vortrag auf unserer Webseite)

heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Kill den Mythos 2:

„E-Mail made in Germany“ macht E-Mails jetzt sicher

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Der lange Weg zu „E-Mail made in Germany“

- Seit > 15 Jahren wird über sichere SSL/TLS-Verbindungen kommuniziert
- Jahrelang wurde „den Großen“ angekreidet, dass Sie kein oder nur sehr lückenhaft SSL/TLS anbieten
- Oft noch nicht einmal POP3/IMAP/SMTP-Verbindungen mit Passwörtern verschlüsselt

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

EMIG:
Was ist letzten Sommer geschehen?

- SSL/TLS wurde aktiviert
  - smtp_use_tls=yes
  - smtpd_use_tls=yes

- Und dann war da noch:
  - cat $$$ >> /dev/marketing
  - cat $$$ >> /dev/marketing
  - cat $$$ >> /dev/marketing
  - cat $$$ >> /dev/marketing

heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Was taugt „E-Mail made in Germany“?

Marketing

- E-Mail made in Germany ist ein g[illegible]ialer Marke[illegible]ng-Trick
  - Zur rechten Zeit am re[illegible]ten Ort m[illegible]ri[illegible]tig fi[illegible]wesen! Respekt.
- Technisch ist es nichts a[illegible]es a[illegible]

  20 Jahre nach alle[illegible]ande[illegible]n aktivieren auch web.de, GMX, T-Online und E[illegible]eene[illegible]ba[illegible]nbr[illegible]chende Technologien wie SSL/TLS.
  - *A[illegible]da m[illegible]s es [illegible]och ganz bestimmt noch mehr geben?*
  - N[illegible]ibt [illegible]zeit zumindest) nicht.
  - *[illegible]r s[illegible]as wie eine Verifizierung der Gegenstelle?*
  - Nei[illegible]. An Konzept wird noch überlegt…
  - *Aber dann kann ein man-in-the-middle das ja aufbohren?*
  - Ja. Kann er.

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Aber bei EMIG sind meine Mails sicher verschlüsselt.

- EMIG macht (jetzt endlich) SSL, andere Provider machen das auch.
- Mails von EMIG an EMIG werden mit SSL verschlüsselt
- Mails von EMIG an andere werden mit SSL verschlüsselt
- Mails von anderen an EMIG werden mit SSL verschlüsselt
- Mails von anderen an andere werden mit SSL verschlüsselt

- Muß ich zu EMIG gehen damit ich SSL-verschlüsselte Mails habe?
  - Nein. Man muß zu einem Anbieter gehen, der Verschlüsselung ernst nimmt.
  - Idealerweise auf technischer Ebene, statt nur im Marketing

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

EMIG im Detail: Es ist unsicher und „broken by Design“

- EMIG-Systeme tauschen eine Liste der beteiligten Mailserver aus.
  - Aber: Sie tauschen keine Liste der beteiligten Empfängerdomains
- Was passiert, wenn ein Man-in-the-Middle Mails entführt?
  - Das DNS von EMIG ist nicht durch DNSsec geschützt
  - Injiziert ein MITM im DNS eigene MX-Records, gibt es für die injizierten Mailserver des Angreifers keine SSL-Policy
    - Ob EMIG-Server also eine CA teilen oder ihre SSH-Fingerprints kennen, ist egal!
  - Die EMIG-Mailserver würden an die injizierten Fremd-Mailserver zustellen (verschlüsselt oder auch unverschlüsselt).
- Postfix: Dieses Konzept ist broken by design, out-of-the-box nicht konfigurierbar
  - SSL-Policy darf/kann nur empfängerbasiert konfiguriert werden

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

EMIG:
Technische Lösung oder reines Marketing?

- Die Frage ist: Wer darf bei EMIG mitmachen?
  - Lange wurden alle Anfragenden hingehalten
  - Wir selbst werden seit Monaten vertröstet
- Wird es eine integrative Initiative, die die Sicherheit erhöht und andere ISPs mitmachen läßt?
- Oder wird eine ausschließende Abgrenzung betrieben, um möglichst gut ein (scheinbares) Alleinstellungsmerkmal vermarkten zu können?
- Was ist mit ausländischen Providern?

heinlein

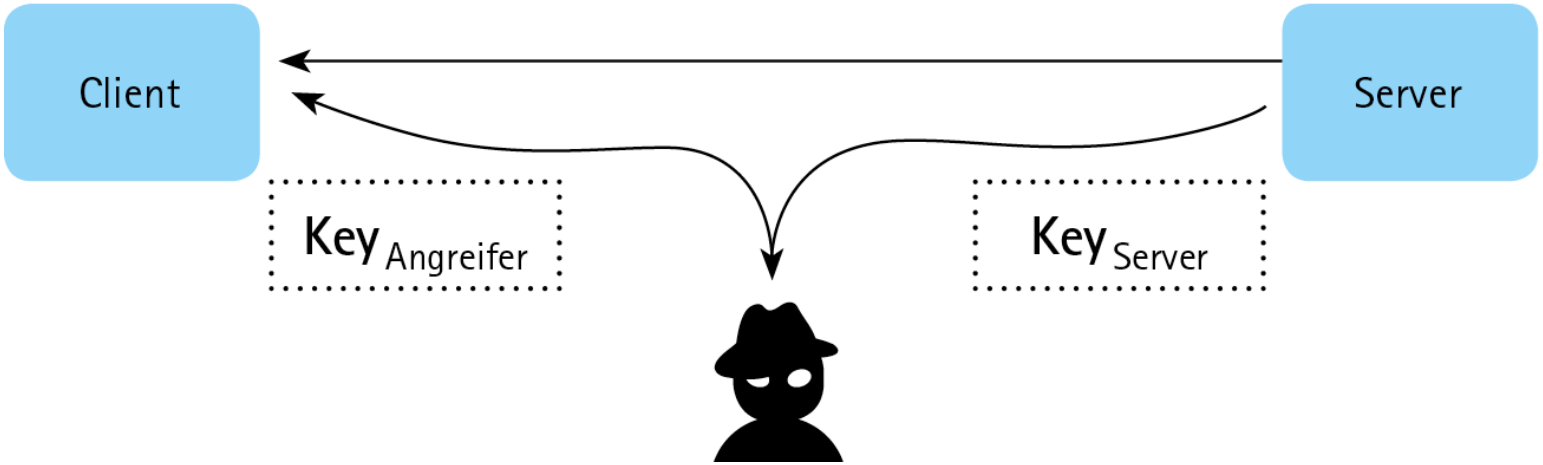
Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Warum SSL/TLS aber nicht ausreicht

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Warum SSL/TLS nicht ausreicht

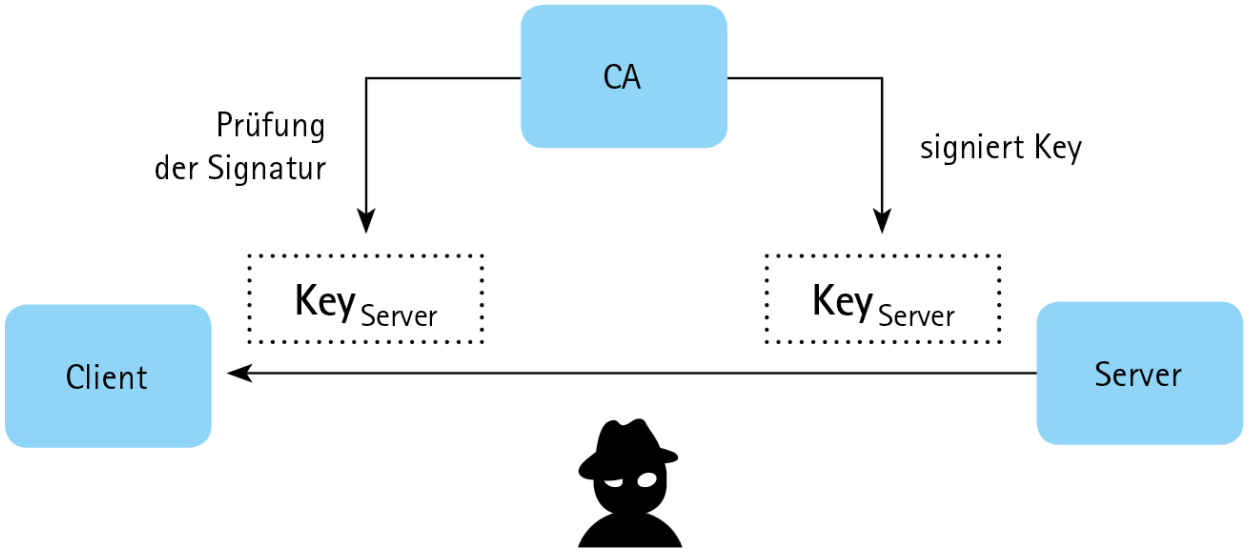
→ Ein man-in-the-middle könnte das SSL-Zertifikat austauschen.



Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Warum SSL/TLS nicht ausreicht

- Darum braucht man eine CA.



- Welcher CA kann man trauen?

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Warum SSL/TLS nicht ausreicht

- Mit welchen Servern rede ich?
  - Über DNS-Poisening könnten andere MX-Records untergeschoben werden.
  - Kann ich mich ohne DNSsec auf das DNS verlassen?
- Viele Provider haben nur selbstsignierte Zertifikate.
  - Kann man ändern, muß man dann aber auch!
- Was ist, wenn kein SSL/TLS möglich ist? Was ist, wenn der MitM das SSL-Announcement unterdrückt?
  - Dann normalerweise Fallback auf Klartextübertragung
- SSL/TLS ist nur Nexthop-Verschlüsselung. Danach liegt die Mail zunächst wieder im Klartext vor (siehe DE-Mail)
  - Kann man seinem Provider trauen?

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Warum SSL/TLS trotzdem sinnvoll und gut ist

- Es schützt vor ungewollten Mitlesern
- Es erhöht den Aufwand für jemanden, der mitlesen will
- Es ist eine selbstverständliche Grundabsicherung
- Das Problem: Es ist halt immer nur optional. Ein MitM kann SSL unterdrücken.
  - Hier eventuell Vorteil von EMIG
  - Dafür gibt es neuerdings jedoch auch DANE TLS
- Rund 40% unserer SMTP-Verbindungen laufen über SSL/TLS
  - Das ist deprimierend. Warum?!

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Demnächst kommt DANE TLS

- Wie gesagt: Ein MitM könnte SSL-Announcements unterdrücken
- Die CA könnte unterwandert sein.
- DANE TLS führt einen neuen TLSA-Record ein (TLS Association), die definieren, welche Zertifikate der Client akzeptieren darf.
  - Die Zertifikate einer bestimmten CA
  - Bestimmte genannte Zertifikate
  - Zertifikate, die von einem bestimmten Vertrauensanker abstammen
- Der TLSA-Record wird dann für _25._tcp.example.com definiert
  - Also individuell pro Dienst/Port
  - Und individuell pro Empfängerdomain (und damit anders als EMIG nicht Broken by Design!)
  - Port kann auch Wildcard sein *._tcp_example.com
    - Ein Mailserver hat viele Ports: 25, 465, 587, 110, 143,993, 995, 2000, 4190

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Technische Spezifikation des TLSA-Records

```
_25._tcp.mx1.example.com. IN TLSA 3 1 1 5c1502a6549c423b
e0a0aa9d9a16904de5ef0f5c98c735fcca79f09230aa7141
```

- Feld 1: Certification Usage (hier: 3)
  - 0 = PKIX-TA: CA-Zertifikat, das in der Validierungskette auftauchen muss (?)
  - 1 = PKIX-EE: CA-Root-Zertifikat, gegen das die CA-Kette validiert (?)
  - 2= DANE-TA: CA-Zertifikat mit dem der Key unterschrieben sein muß
  - 3= DANE-EE: Konkreter exakter Public Key des Servers (self signed!)
- Feld 2: Selector Field
  - 0 = Certificate Binary Structure 1 = DER-encoded Binary Structure
- Feld 3: Machting Tye (hier: 1)
  - 0 = Ganzes Zertifikat
  - 1 = SHA-256 Hash des Zertifikats 2 = SHA-512-Hash des Zertifikats
- Feld 4: Zertifikatswert (hier: 5c1502a...)
- Default: „TLSA 3 1 1“

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Probleme von DANE TLS

- DNS selbst wäre durch einen MitM leicht angreifbar
  - Die TLSA-Records könnten unterdrückt und ausgetauscht werden
  - Anschließend wäre der Client wieder blind und naiv wie früher
- Also: Absicherung der DNS-Records über DNSsec
  - Theoretisch: Kein Problem. „Muß man nur machen“
  - Praktisch: DNSsec hat sich bis heute nicht fläckendeckend durchgesetzt. Zahlreiche Fallstricke, komplexeres Handling der Records, große Sorgfalt notwendig.
  - DANE TLS sorgt im Prinzip für den ersten flächendeckenden Einsatz von DNSsec!
- Problem: Hohe Latenz bei Überprüfung der zahlreichen DNSsec-RR
  - Schwierig bei HTTP, XMPP & Co!

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Und DNSsec?

→ Mehr dazu im Vortrag am Dienstag Nachmittag!

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Das Howto zu TLSA

- Hash-Wert aus dem Zertifikat erzeugen

```
$ openssl x509 -in mailbox.org.crt -outform DER | openssl sha256
(stdin)= 6658356da26618a0cbd2547509c0690b60accf4c05c6cee778309d11cb985b6a
```

- TLSA-Record einrichten

```
_25._tcp.mailbox.org. 3600 IN TLSA 3 1 1 (
6658356da26618a0cbd2547509c0690b60accf4c05c6cee778309d11cb985b6a )
```

- Mit „dig +dnssec“ testen => Flag „aa/ad“ zeigt DNSsec an
- Postfix scharfschalten!

```
smtp_tls_security_level = dane
smtp_dns_support_level = dnssec
```

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Das RFC zu DANE

- http://tools.ietf.org/html/rfc6698#section-2.1.2

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

DANE TLS und E-Mail made in Germany

- Wenn DANE TLS eingeführt ist: Was bringt dann noch EMIG?
  - EMIG ist eine proprietäre geschlossene Lösung, die festlegt, daß bestimmte Server nur mit SSL und bestimmten Fingerprints zu erreichen sind.
  - DANE ist ein offenes System, bei dem jeder über DNS-Records festlegen kann, daß bestimmte Server nur mit SSL und bestimmten Fingerprints zu erreichen sind.
  - Postfix kann DANE ab Version 2.11 bereits.
  - 100% sicher ist DANE jedoch nur mit DNSSec.
    - (EMIG ist ohne DNSsec ebenso unsicher...)

heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Die Alternative:

Echte Ende-zu-Ende-Verschlüsselung Mit PGP oder S/MIME

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

http://vimeo.com/86736532

Wie funktioniert eigentlich E-Mail-Verschlüsselung?

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Möglichkeiten und Grenzen von PGP & S/MIME

- Hier kontrollieren Absender und Empfänger die Ver-/Entschlüsselung
- Auch auf den Servern liegt die E-Mail nur verschlüsselt vor
  - Aber: Meta-Daten (=Mailheader) einer E-Mails bleiben unverschlüsselt: Wer redet mit wem wozu.
- Nötig ist die Kombination mehrerer sich überlagernder Mechanismen:
  - Verschlüsselte E-Mails, die über SSL/TLS-Tunnel transportiert werden

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Wer ist wer?

- Das Problem: Man muß auch sicherstellen, daß man den richtigen Schlüssel des Empfängers benutzt. Sonst „man in the middle“-Angriffe möglich..
- Andererseits will man auch anonym kommunizieren können.

- PGP: Gegenseitige Unterschriften, ein „web of trust“, kein einzelner Vertrauensanker
  - Achtung, Sozialprofil: Wer kennt wen?
- S/MIME: Zentrale Zertifizierungsstelle, „anchor of trust“.
  - Ist die vertrauenswürdig?

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Unser Projekt:

mailbox.org

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

mailbox.org

- Wir bieten spezielle Mailadressen, die definitiv nur per SSL/TLS erreichbar sind. Damit kann ein User durch Auswahl seines Mailaliases steuern, wie versandt werden muß.
  - Sichere Mails nicht nur innerhalb EMIG, sondern mit allen!
- Unsere Domain sind über DNSsec abgesichert
  - Sichere MX-Records!
- Als Provider wollen wir informieren, aufklären und auch erziehen.
  - Wir produzieren Stiftfilme, leben die Nutzung von PGP vor und pflegen umfangreiche Dokumentation im Support-Bereich
- mailbox.org kann noch viel mehr, aber das müssen Sie selbst entdecken. :-)

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

- Snowden sagte im Guardian Chat:

  Starke Verschlüsselung ist das einzige, worauf Sie sich verlassen können.

  > *"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."*

- Zeit, das endlich mal anzugehen.

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Darum meine Bitte an Sie

- Nutzen Sie die zur Verfügung stehenden Möglichkeiten.
  - Jeder Baustein trägt zur Absicherung bei.
- Verschlüsselung ist weder kompliziert, noch etwas für Klein- oder Großkriminelle.
  - Verschlüsselung ist aber auch nichts für die Marketing-Abteilung!

- Verschlüsselte sichere Kommunikation ist ein Ausläufer des Menschenrechts auf Gedanken- und Meinungsfreiheit. Dieses Recht dürfen wir uns nicht nehmen lassen.

Mailserver-Consulting seit > 20 Jahren

- Natürlich und gerne stehen wir Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich über Feedback!

Peer Heinlein

Mail: mail@heinlein-support.de

Telefon: 030/40 50 51 - 0

- Wenn's brennt:

  Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Wir suchen Kollegen für:

Helpdesk, Administration, Consulting!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Schauen Sie doch mal vorbei:
  - https://mailbox.org
- Und viel Erfolg an der Tastatur...

Bis bald.

heinlein

Johannes Rundfeldt <j.rundfeldt@heinlein-support.de>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln in Training und Schulung die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances für Archivierung, IMAP und Anti-Spam und speziell für den Serverbetrieb konzipierte Software rund ums Thema E-Mail.