Post-Snowden Mail-Security 2016
[CLT 2016]
Peer Heinlein <p.heinlein@heinlein-support.de>

„Post Snowden“

E-Mail-Security 2016

Peer Heinlein <p.heinlein@heinlein-support.de>

„Erst verschlüsseln sie die Mail mit PGP und dann laden sie es auf Dropbox hoch."

(Logan CIJ Symposium 2016 Berlin)

Peer Heinlein <p.heinlein@heinlein-support.de>

Geht's um E-Mail-Security...

- Heinlein Support GmbH / Peer Heinlein
  - Linux Security Consultant seit 1995
  - Spezialist für Mailserver und Anti-Spam/Anti-Virus seit 1992
  - Diplom-Jurist / Prädikatsexamen
  - Kunden:
    - ISPs > 100.000 Kunden (EWEtel, Strato)
    - Universitäten, Forschungseinrichtungen
    - diverse Landesrechenzentren (ITDZ, Stuttgart, Baden-Franken, Thüringen)
    - Div. politische Instititionen und Stiftungen
    - Spezialfälle >> n-Millionen Mails/Tag (XING, StudiVZ)
  - Heinlein Support GmbH: 28 Mitarbeiter mit Sitz in Berlin

E-MAIL

IST

TOT.

(Und dann kamen welche, die haben das einfach nicht gewusst.)

4 Mrd. Accounts in 2015!

	2011	2012	2013	2014	2015
Worldwide Email Accounts (M)	**3,146**	**3,375**	**3,606**	**3,843**	**4,087**
Corporate Email Accounts	**788**	**850**	**918**	**991**	**1,070**
% Corporate Email Accounts	*25%*	*25%*	*25%*	*26%*	*26%*
Consumer Email Accounts	**2,358**	**2,525**	**2,688**	**2,852**	**3,017**
% Consumer Email Accounts	*75%*	*75%*	*75%*	*74%*	*74%*

Corporate vs. Consumer Email Accounts, 2011–2015

Quelle: Ridacti Group

Peer Heinlein <p.heinlein@heinlein-support.de>

Social media didn't kill email

where US citizens start their online day

Sources

EmailStatCenter.com ReadWriteWeb.com PewInternet ccloop.com CampaignMonitor Office Blogs The Radicati Group, Inc. Skype LinkedIn Microsoft Wrike

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 1995:

Mach Spam-/Virenschutz!

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 2005:

Mach Spam-/Virenschutz!
Mach TLS!

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 2015:

Post-Snowden Mail-Security 2016
[CLT 2016]
Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 2015:

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil I:
Wer macht derzeit was?

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail made in Germany

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail made in Germany: Was machen die?

- Regelt, daß EMIG-Teilnehmer untereinander SSL einsetzen müssen.
  - Hätten Sie einfach so SSL aktiviert, wäre das auch der Fall. :-)
- Stellt per Policy sicher, daß SSL eingehalten wird.
  - Würde DANE/DNSSEC auch machen
  - EMIG enstand vor DANE.
  - Fordert kein DNSSEC – wäre per MX-Record-Injection angreifbar.
- Zeigt dem User an, daß die Mail per SSL an einen EMIG-Partner versendet wird
  - EMIG verschweigt, daß auch Mail an andere ISPs genauso sicher per SSL rausgehen.
  - Anbieter wie mailbox.org zeigen bei jedem Empfänger den SSL-Status an und stellen SSL-Versand sicher :-)

E-Mail made in Germany

E-MAIL MADE IN GERMANY
Eine Initiative von GMX, Telekom und WEB.DE

Start | Verschlüsselung | Datenverarbeitung | Kennzeichnung | De-Mail | Outlook Add-In | Teilnehmer | Jetzt wechseln!

TEILNEHMER

GMX · Telekom · WEB.DE · freenet · 1&1 · STRATO · HORNETSECURITY · Weitere Unternehmen werden zertifiziert und geprüft durch: TÜVRheinland

E-Mail made in Germany ist eine Initiative von GMX, Telekom und WEB.DE.

Unsere Initiative ist offen für weitere Partner, die bereit sind, sich unter ihrer E-Mail-Domain dauerhaft zur Einhaltung unserer Sicherheitsregeln zu verpflichten.

Bei Interesse wenden Sie sich bitte an:
teilnehmer@e-mail-made-in-germany.de

Impressum | Presse

Eine Initiative von GMX · WEB.DE · Telekom

Peer Heinlein <p.heinlein@heinlein-support.de>

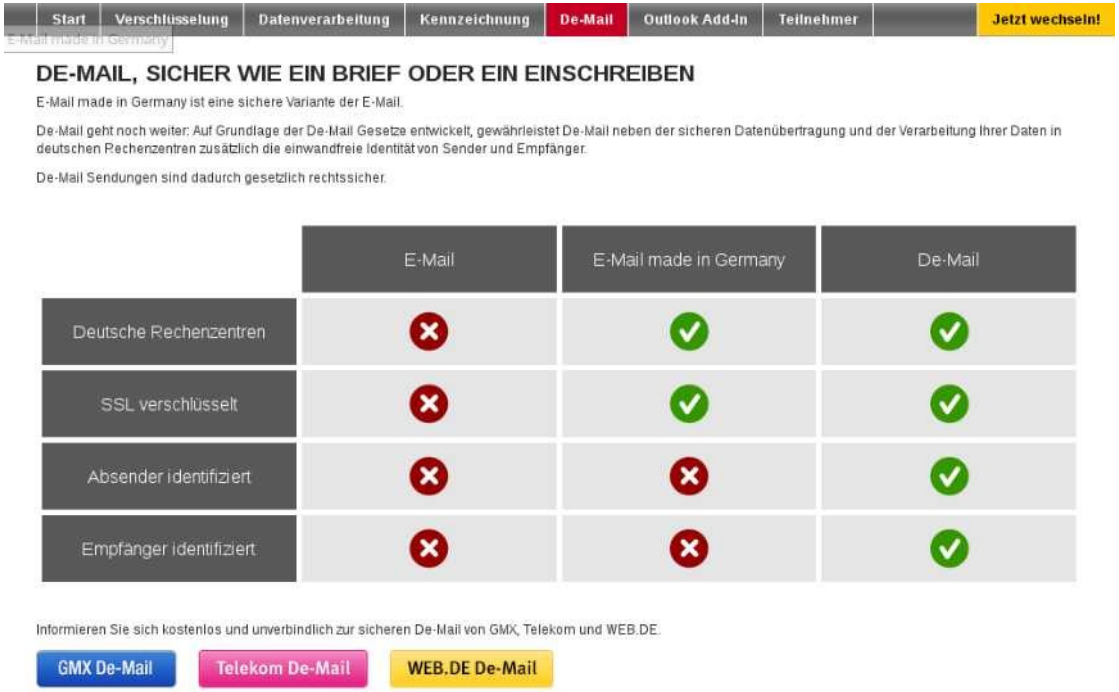
E-Mail made in Germany: Wer macht mit?

- Weiterhin nur sehr beschränkter Teilnehmerkreis
  - GMX, web.de, T-Online, freenet, 1&1, Strato, Hornet Security, Mediabeam
  - Ca. 30 Partner in Umsetzung (Versicherung, Großversender)
- Kostspielige Zertifizierung durch TÜV Rheinland notwendig

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail made in Germany:

- Wird massiv als Werbe-/Marketingmaßnahme genutzt, insb. zum Vorteil der „Erfinder“ GMX, web.de, T-Online
  - Leitet auch Werbung zu DE-Mail ab.



Peer Heinlein <p.heinlein@heinlein-support.de>

BSI: Technische Richtlinie „Sicherer E-Mail-Transport“

Peer Heinlein <p.heinlein@heinlein-support.de>

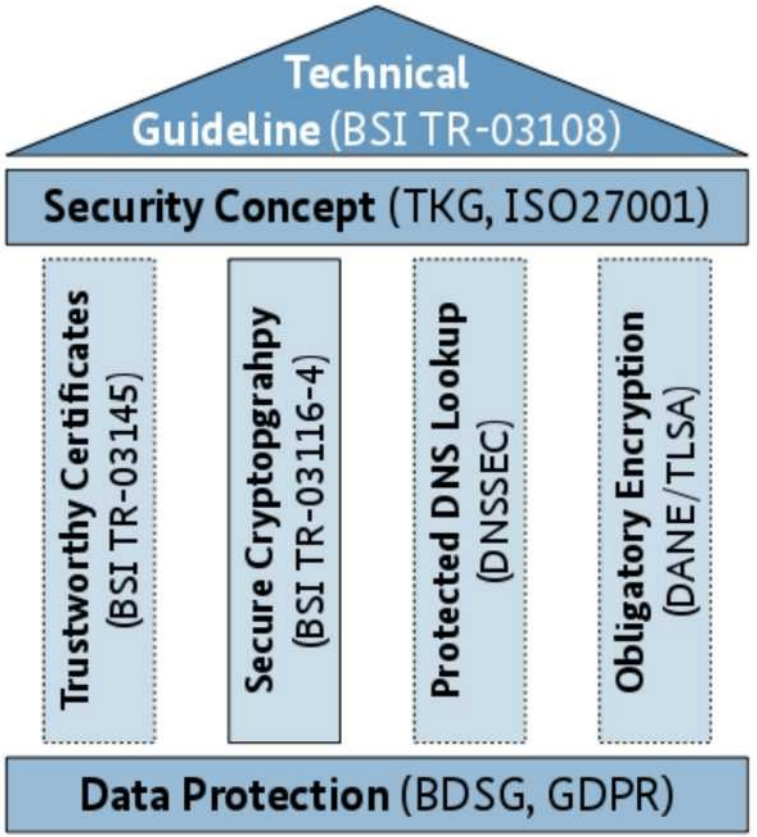
TR Sicherer E-Mail-Transport

- Mitte 2015 startete das BSI die Erarbeitung der Technischen Richtlinie „Sicherer E-Mail-Transport“ (BSI TR-03108)
  - BSI entwickelte Entwurf
  - Arbeitsgruppensitzungen mit Providern und Mail-Experten
  - Demnächst 12. April 2016 abschließendes Treffen der Arbeitsgruppe
- Secunet begleitet das BSI bei der Erstellung und ggf. Umsetzung

Peer Heinlein <p.heinlein@heinlein-support.de>

Das definiert die TR:

- Nutzung „guter“ CAs für SSL
- Verwendung sicherer Ciphers
- DNSSEC
- DANE/TLS
- Aufklärung der Nutzer durch Anzeige?
- Nachweis eines Sicherheitskonzepts nach TKG (eh vorhanden) oder ISO27001.



- „EMIG + DANE + Besseres SSL = TR-03108“

Peer Heinlein <p.heinlein@heinlein-support.de>

TR-Zertifizierung als Anreiz zum Mitmachen

- Provider können sich nach der TR zertifizieren lassen
  - Genauer Ablauf und Kosten noch unklar
- TR-Zertifizierung darf zu Werbezwecken als Auszeichnung genutzt werden!
- Auch Providern aus dem Ausland soll die TR-Zertifzierung offen stehen
  - (Darum: RZ Deutschland und BDSG oder vergleichbar)
- Internationale Aufmerksamkeit für TR E-Mail erwünscht
  - BSI tritt damit auf Konferenzen im In- und Ausland auf

Peer Heinlein <p.heinlein@heinlein-support.de>

Die Volksverschlüsselung („VV“)

Peer Heinlein <p.heinlein@heinlein-support.de>

Volksverschlüsselung („VV“)

- Zentrale S/MIME-Zertifizierungsstelle des Fraunhofer Instituts
  - S/MIME hat anders als PGP eine zentrale Zertifizierungsstelle!
  - Telekom ist Volksverschlüsselungspartner, aber am Ende kann sich jeder Nutzer jedes Providers ein Zertifikat holen
- Software/App richtet alle Komponenten ein und erzeugt Schlüssel – Fraunhofer stellt Schlüssel-Server
  - Derzeit: Windows. Geplant: MacOSX, Linux, iOS, Android
- Schlüssel & Betrieb für Private kostenlos, aber ggf. Kosten zur Identitätsprüfung

Peer Heinlein <p.heinlein@heinlein-support.de>

Volksverschlüsselung („VV“)

- Das leisten die Fraunhofer-Beiträge zur Volksverschlüsselung:
  - Zertifizierungsstelle für Schlüsselbeglaubigung
  - Verzeichnisdienst, um Schlüssel abrufen zu können
  - Sperrdienst für verloren gegangene Schlüssel
  - Aufbau und kontinuierliche Pflege einer kostenlosen Infrastruktur zur flächendeckenden Ausrollung von Schlüsseln
  - Benutzerfreundliche Software für Windows
  - Versionen für Mac OS X, Linux, iOS und Android sind geplant

Peer Heinlein <p.heinlein@heinlein-support.de>

Volksverschlüsselung: Keine anonyme Nutzung

- Zertifikate sind Class-3-Zertifikate!
- D.h. Identität des Inhabers ist eindeutig feststellbar
  - Keine anonyme Nutzung wie bei PGP möglich!
  - Derzeit: Registrierung über Personalausweisenummer.
  - Später auch PostIdent & Co geplant.

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Vertrauenswürdige Verteilung von Verschlüsselungs-Schlüsseln („VVV“)

Peer Heinlein <p.heinlein@heinlein-support.de>

Vertrauenswürdige Verteilung von Verschlüsselungs-Schlüsseln („VVV“)

- Konsortium von Fraunhofer SIT, Provet/Uni-Kassel, ULD, DesignLab der UdK Berlin und mailbox.org
  - Projektlaufzeit: Ab jetzt bis Ende 2017
  - Gefördert vom Bundesministerium für Bildung und Forschung (BMBF)

ULD provet Projektgruppe verfassungsverträgliche Technikgestaltung
Fraunhofer SIT
mailbox.org damit Privates privat bleibt
Design Research Lab

Peer Heinlein <p.heinlein@heinlein-support.de>

VVV: Unsere Aufgabe

- Entwickelt Standards zum Austausch von User-Schlüsseln zwischen Providern (weiter)
  - Entwickelt auch Plugins und Softwarekomponenten
- Die Projektpartner untersuchen die wissenschaftlichen und technischen Aspekte des Schlüsseltauschs:
  - Usability
  - Rechtsfragen
  - Datenschutzfragen
  - uvam.
- mailbox.org übernimmt Praxis- und Enduser-Tests

Peer Heinlein <p.heinlein@heinlein-support.de>

Transport E-Mail-Security („TES“)

Peer Heinlein <p.heinlein@heinlein-support.de>

TES: Transport E-Mail Security

- Konsortium initial gegründet von

- TES ist ausdrücklich offen für alle anderen Provider und sucht aktiv europa- und weltweit Kooperationen mit den „großen“ Providern.
  - Treffen in London, Madrid und dem WHD in den letzten 3 Monaten
  - Sehr positive internationale Resonanz der großen Player
  - OpenBIT wurde als Träger gewonnen.

Peer Heinlein <p.heinlein@heinlein-support.de>

Das macht TES

- TES-Mitglieder stellen nach einem bestimmten Verfahren PGP-Keys ihrer User zur Verfügung
  - Key im DNS über OPENPGPKEY oder Referenz auf HKP-Keyserver noch offen
  - Problem: Bislang kann jeder beliebig für alle Mailadressen Keys erzeugen.
  - TES reduziert das notwendige „Vertrauen“ in die Richtigkeit des Schlüssels wenigstens auf den Provider des Nutzers herunter
    - Ja, der Provider könnte für seinen Nutzer falsche Schlüssel herausgeben.
    - Aber eben nur noch dessen Provider und nicht jeder x-beliebige.
- Bestimmte DNS-Records zeigen an, ob TES für eine einzelne Domain nutzbar ist und über welchen TES-Provider die Keys abgewickelt werden.

TES: Keys für User ohne Keys

- TES regelt auch, daß Provider für ihre User selbst PGP-Schlüssel erzeugen sollen, wenn diese noch keine Keys haben.
  - Aber dann – und nur dann – kann der Absender die Mail nicht nur mit SSL, sondern auch mit PGP verschlüsselt lossenden.
  - Ja, dann hat der Provider den Private Key.
  - Ohne TES würde die Mail im Klartext versandt werden.
  - Der Provider kann dem User die Mail transparent decodieren und anzeigen.
  - Die Mail ist auf dem Transportweg nachhaltig und konträr zu SSL geschützt, für den Endanwender ist das aber transparent und ohne Aufwand nutzbar.
  - „Fortgeschrittene User“ können eigene PGP-Keys nutzen und können eigene Schlüssel nutzen bzw. den Private Key selbst verwalten
  - („alles kann, nichts muß“).

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil II:
Verschlüsseln im Alltag

Peer Heinlein <p.heinlein@heinlein-support.de>

PGP im Webmailer:

Wie macht man das?

Peer Heinlein <p.heinlein@heinlein-support.de>

Mailvelope:

Es lebe des Browser-Plugin

Peer Heinlein <p.heinlein@heinlein-support.de>

Mailvelope: Nicht immer alltagstauglich

- Mailvelope ist Browser-Plugin, muß explizit auf dem Nutzer-Rechner installiert sein.
  - Probleme im Urlaub / beim Kunden / bei Freunden / im Internet-Cafe.
  - Wenn das erste mal unterwegs der Zugriff auf wichtige Mails scheitert oder Urlaub ansteht läßt die Begeisterung für PGP schlagartig nach.
  - Was mache ich denn, wenn ich unterwegs an meine Mails muß?! Mailvelope im spanischen Internet-Cafe installieren?!

Peer Heinlein <p.heinlein@heinlein-support.de>

„Private-Keys sind nur auf dem privaten Rechner wirklich sicher“.

- Sind sie das?
- Auf einem privaten Rechner / Handy vertraue ich…
  - Dem Betriebssystem
  - Der Web-/Mailapplikation
  - Allen installierten Plugins
  - Den von mir besuchten Webseiten
  - Den Virenprogrammierern, die mich infiziert haben
  - Meinem Virenschutzprogramm
- Auf dem Handy auch noch:
  - Google/Apple
  - Allen beiläufig installierten Apps
  - Der Handy-Hardware (Samsung, LG uvam.)
- Puh. Ganz schön viele Leute.

Peer Heinlein <p.heinlein@heinlein-support.de>

Kann Mailvelope sicher sein?

- Mailvelope auf nicht-vertrauenswürdigen Rechnern würde Private Key sofort komplett kompromittieren.
  - Welcher Windows-Rechner / welches Android / welches iPhone ist denn nun vertrauenswürdig?
- Mailvelope speichert Private Key im Browser-Filestorage
  - Gut erreichbar für Browser, alle Plugins, Webseiten, Drive-By-Viren uvam.
  - Wir haben Viren „in the wild“ beobachtet, die gezielt die Private Keys von Mailvelope-Installationen abgreifen!
  - Keys können sogar über XSS-Angriffe geklaut werden!
  - Wieso hinterfragt das eigentlich niemand?
- JavaScript bietet nach Experten-Meinung keine vertrauenswürdige Umgebung für sichere Cryptographie und damit für Mailvelope

Peer Heinlein <p.heinlein@heinlein-support.de>

Mailvelope bei GMX & web.de

- PGP-Verschlüsselung von GMX & web.de basiert auf vorpaketierten erweiterten Mailvelope-Installationen.
  - Macht nix, die Presse hat‘s gefeiert wie Neu.
  - Private Schlüssel lagern mit einer Passphrase des Users geschützt auf dem Server des Providers
  - Mailvelope kann diesen Schlüsselcontainer herunterladen, lokal decodieren und verwenden. Schick!

Peer Heinlein <p.heinlein@heinlein-support.de>

Der Guard:

PGP mal serverseitig

Peer Heinlein <p.heinlein@heinlein-support.de>

Der Guard: Überall-PGP serverseitig

- Mailbox.org und Open-Xchange haben den „Guard“ entwickelt
  - Keys liegen mit Passphrase des Users auf dem Server (wie Mailvelope)
- Ver-/Entschlüsselung und Signierung findet komplett im Server statt nachdem der User seinen Schlüssel aktiviert hat
  - Schlüssel des Users ist zur Laufzeit immer mit einem dem Provider unbekannten Session-Key codiert.
  - Schlüssel wird nie auf den unsicheren Client (Desktop-PC, Browser, Android, iPhone) kompromittiert
- Jederzeit voller Zugriff auch von nicht-vertrauenswürdigen PCs
  - Worst Case: Konkrete Mail bekannt, aber Schlüssel bleibt unerreichbar!

Peer Heinlein <p.heinlein@heinlein-support.de>

Wem vertraue ich beim Guard?

- Auch beim Guard muß man jemandem vertrauen:
  - Der Server-Hardware
  - Dem Linux-OS
  - Den Programmierern des Guard

- Gretchenfrage:

  Welcher Computer ist gefährdeter? Server oder Desktop/Handy?

Peer Heinlein <p.heinlein@heinlein-support.de>

Guard und Mailvelope schließen sich nicht aus!

- Aber wem das alles nicht gefällt: Der Guard ist ein Angebot.
  - Alles ist weiterhin möglich.
- Der User kann auch weiterhin Mailvelope nutzen. Das ist ein Browserplugin, das geht prinzipiell „immer“.
  - Unabhängig davon interagiert Guard auch direkt mit Mailvelope, beispielsweise zum Schlüsselaustausch.
- Wir zwingen keinen zum Guard und unterstützen Mailvelope explizit.
  - (Aber wir warnen davor)

Peer Heinlein <p.heinlein@heinlein-support.de>

PGP-Keys sicher verteilen:

Das kann doch nicht so schwer sein?

Peer Heinlein <p.heinlein@heinlein-support.de>

HKP-Server

Der klassische Key-Server

Peer Heinlein <p.heinlein@heinlein-support.de>

PGP-Keys verteilen: HKP

- HKP-Server sind die klassischen „Key-Server“, wie man sie von den PGP-Schlüsselsuchen her kennt
  - HKP = HTTP Keyserver-Protokoll (HTTP 1.0 auf speziellen Ports)
- HKP-Server verteilen einfach nur Schlüssel. Sonst nichts.
  - Problem: Jeder kann einen Key-Server betreiben
  - Jeder kann einen Key mit beliebigen IDs/Mailadressen erzeugen!
  - Welcher Key ist vertrauenswürdig?
  - Was ist, wenn es mehrere Schlüssel bzw. widersprüchliche Schlüssel auf verschiedenen Servern gibt?
- gpg kann Keys von HKP-Servern fetchen!

Peer Heinlein <p.heinlein@heinlein-support.de>

DNS-Referenzen zum HKP-Server

- Über DNS TXT-Records kann abgefragt werden, welche HKP-Server für eine Domain genutzt werden sollen („PKA“)
  - Jeder Mailadresse hat einen Eintrag
  - Localpart des Usernamens dabei im Klartext
  - Record verweist auf ID des Keys
- Vorteil: HKP-Server können auch mehrere Zertifikate und Revokes managen
  - HKP-Server können auch abgelaufene Keys vorhalten um später noch Signaturen prüfen zu können.
- DNSSEC nicht vorgeschrieben, könnte kompromittiert sein.
  - Aber es hindert uns ja keiner, das heute mit DNSSEC zu betreiben.

Peer Heinlein <p.heinlein@heinlein-support.de>

PGPKEY:

Es lebe das DNS.

Peer Heinlein <p.heinlein@heinlein-support.de>

DANE/OPENPGPKEY: Die Keys direkt im DNS

- Ein RFC-Draft regelt, daß PGP-Keys als BLOB im DNS-Record der Maildomain veröffentlicht werden können
  - Mailadressen werden über einen Hash eingetragen
  - DNSSEC/DANE sichern
  - Problem: Handhabbarkeit im DNS für ISPs > 1 Mio User?
  - Problem: Revoke-Zertifikate?
  - Problem: Prüfung von Signaturen nachdem Keys abgelaufen sind?
- DNS-Provider könnte Schlüssel seines Users manipulieren
  - Trust ggü. Provider weiterhin notwendig
- gpg kann Keys aus dem DNS fetchen!
  - DANE/DNSSEC schützt das alles.

Peer Heinlein <p.heinlein@heinlein-support.de>

Provider die Mails verschlüsselt speichern.

Peer Heinlein <p.heinlein@heinlein-support.de>

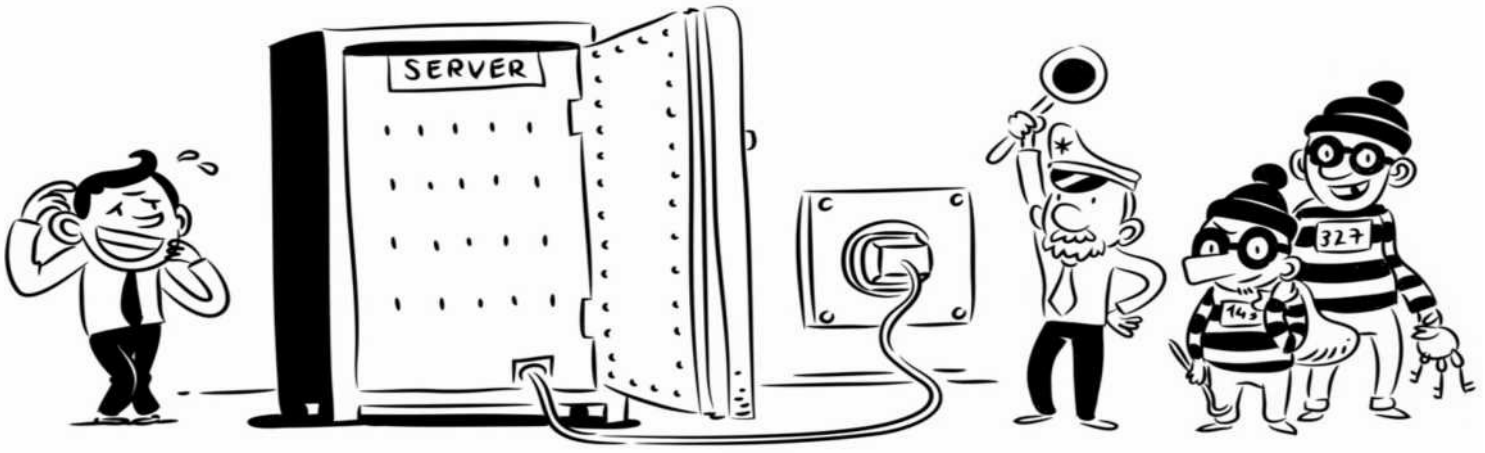
Die vollständig verschlüsselte INBOX

- Auf Wunsch der Nutzer verschlüsseln wir unverschlüsselt eingehende E-Mails sofort mit dem Public-PGP-Key des Nutzers.
  - Mails sind dauerhaft und komplett PGP-Verschlüsselt in der INBOX des Nutzers.
- Knacken Dritte das Postfach des Nutzers (Passwortklau!) haben sie weiterhin keinen Zugriff auf die E-Mails. Auch der Provider kann die E-Mails nicht mehr lesen.
  - Ja, in der Millisekunde des Empfangs hatte der Provider die Mail im Klartext und hätte sie kopieren können. Dagegen helfen nur vom Absender direkt verschlüsselt abgesandte E-Mails.
  - Darum haben wir ja TES gegründet!
  - Aber: Metadaten (wer redet mit wem wozu) bleiben bei PGP lesbar!

Peer Heinlein <p.heinlein@heinlein-support.de>

„Mein Provider speichert die Mails eh verschlüsselt“

- Manche Provider werben damit, die Mails auf verschlüsselten Festplatten zu speichern.
  - Etliche User im Support fragen uns aktiv danach.
- Eine verschlüsselte Datenpartition ist im laufenden Betrieb „entschlüsselt“ gemountet und schützt nicht gegen Angreifer zur Laufzeit.



Peer Heinlein <p.heinlein@heinlein-support.de>

„Mein Provider speichert die Mails eh verschlüsselt“

- Eine verschlüsselte Partition hilft, wenn jemand „die Festplatte klaut“.
  - Im Falle von uns heißt das: 2 Racks voll mit 200 Festplatten in 3 SANs unbemerkt aus einem RZ mit biometrischen Zugangskontrollen und Kameraüberwachung abbauen und abtransportieren.
  - Aber, okay: Prinzipiell könnte eine fremde Macht einen kompletten Provider im LKW abtransportieren um ein Postfach „zu knacken“.
  - Viel realistischer sind aber IT-Angriffe zur Laufzeit.
  - Achtung: LUKS erhöht Risiko von Totalverlust von Partitionen/Daten!

Peer Heinlein <p.heinlein@heinlein-support.de>

Wie kann man Mails zur Laufzeit doch noch verschlüsselt speichern?

- Auch wenn ein User nicht eingeloggt ist empfängt das Postfach Daten. Diese müssen verschlüsselt gespeichert werden können.
  - Durch ein System von asymetrischen Schlüsseln ist das möglich, siehe PGP. Schreiben = jeder. Lesen = nur der Postfachbesitzer.
  - Verschlüsselt wird dabei nicht die Mail, sondern der komplette Mailstorage des Nutzers als Container. Auch Metadaten damit nicht mehr lesbar!
  - ISP und Dritte sind von den Daten des Nutzers komplett ausgesperrt sobald Mail gespeichert ist.
  - Auf eine LUKS-Verschlüsselung der Festplatten kann verzichtet werden.
- Problem: Wir haben auch viele Daten, die sich mehrere Nutzer teilen. Beispielsweise „shared folders im IMAP“.
  - Wir haben ein System gefunden um auch damit klarzukommen und selbst dann noch Postfächer vor dem ISP verschlüsselt zu betreiben.
  - Der Rest ist leider Betriebsgeheimnis. :-)

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil III:
Wenn openssl das System gefährdet...

Peer Heinlein <p.heinlein@heinlein-support.de>

Und wieder mal: openssl

- Gleich mehrere schwere openssl-Bugs in den letzten Jahren. Downgrades unterwandern Cryptographie.
  - Poodle & Freak ermöglichten Cipher-Downgrades
  - BEAST war sogar Memory Leak!
- openssl-Upgrades für Distriubutionen extrem schwierig, weil vieles/alles dagegen verlinkt ist
  - Manchmal ist Abschalten verschiedener Ciphers der beste Workaround.
- Allgemein ist „openssl“ der Grund, warum man aktuelle Distributionen mit aktueller Software haben will!

Peer Heinlein <p.heinlein@heinlein-support.de>

Unsere Empfehlung für sicheres SSL/TLS

- NIST ist Mindeststandard, IETF ist bestmöglich
- openssl in mindestens Version 1.0.1 ff.
- Immer ECDHE und DHE verwenden, alles andere abschalten (=PFS)
  - ECDHE an sich gut, schnell, sicher aber Entwicklung von Quantencomputern läßt Zukunftssicherheit von ECDHE fraglich aussehen!
  - Im Zweifel ist DHE sogar die bessere Wahl
- Unsichere Ciphers abschalten
  - smtpd_tls_exclude_ciphers = aNULL, DES, RC4, MD5, EXPORT, LOW, SEED, CAMELLIA
- Wegen Logjam-Angriff DHE mit mindestens 2048 Bit verwenden
  - Postfix: „openssl gendh -out /etc/postfix/dh_1024.pem -2 **2048**“
  - Dovecot: ssl_dh_parameters_length = 2048

Peer Heinlein <p.heinlein@heinlein-support.de>

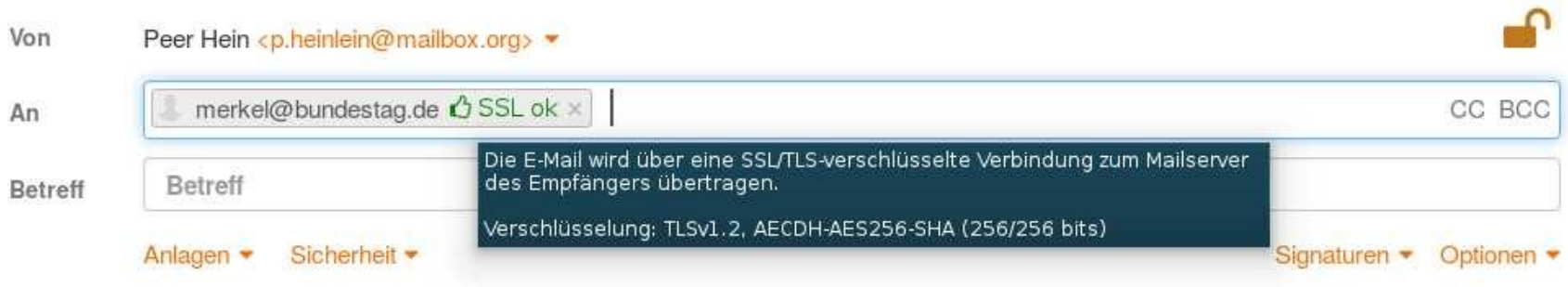
- Viel, viel mehr Details und sehr konkrete Konfigurationsempfehlungen in unserem Vortrag

  „Einführung in moderne Kryptografie für Nicht-Mathematiker“

  unseres Kollegen Karsten Ness.

Wissen was läuft:
Ist TLS bei Mailservern wirklich immer optional?

- Unsere User können Mails so versenden, daß diese definitiv nur über verschlüsselte Verbindungen rausgehen/empfangen werden.
- Wir zeigen schon vorher an, wie eine Mail versendet werden wird.



- Wir stellen sicher, daß ein einmal gesehenes Niveau nicht plötzlich unterschritten wird bspw. durch eine Man-in-the-middle-Attacke.
- Google zeigt das jetzt auch an. Eine gute Kopie ist ein gutes Lob. :-)
  - EMIG macht das quasi auch – aber nur intern bei EMIG-Partnern.

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil IV:
And now for something completly different.

Viren.

Peer Heinlein <p.heinlein@heinlein-support.de>

Wer vorne einen ordentlichen Spamschutz hat, dem reicht hinten auch ein ClamAV. (Peer Heinlein bis vor zwei Jahren)

Peer Heinlein <p.heinlein@heinlein-support.de>

Am Tag gibt es rund 325.000 neue Viren/Mutationen/Bedrohungen.

Aktuell ca. 7 Mio. Virensignaturen in der DB.
(Kaspersky)

Peer Heinlein <p.heinlein@heinlein-support.de>

Scanner im Live-Vergleich: Ich sehe was was Du nicht siehst?!

ClamAV:

Eicar-Test-Signature
Hacktool.Crack.CloneDVD
HTML.Phishing.Bank-143
Win.Trojan.Agent-979742
Win.Trojan.PowerShell-3
Win.Trojan.ZeusVM-1
Worm.Mydoom-27

- → ClamAV: 13 Befunde
- → Sophos: 585 Befunde

(Vergleiche mit TrendMicro, Kaspersky, Avira müßte man mal machen.)

Sophos:

EICAR-AV-Test
Exp/20120158-A
Exp/20120158-A
Exp/20141761-A
Java/Dldr-HX
JS/Dldr-LJ
JS/DwnLdr-NBY
JS/DwnLdr-NEY
JS/DwnLdr-NFA
JS/DwnLdr-NFP
JS/DwnLdr-NFX
JS/DwnLdr-NFY
Mal/DownLnk-D
Mal/DrodAce-A
MalDrodAce-A
Mal/DrodAce-A
Mal/DrodZp-A
Mal/MalitRar-H
Mal/MSIL-JX
Mal/Onkods-C,
Mal/Phish-A
Mal/RarMal-K
Troj/20141761-F
Troj/Agent-AQKZ
Troj/DocDrop-DT
Troj/DocDrop-FK
Troj/DocEx-B
Troj/FakeAle-RS
Troj/Inject-BVV
Troj/JSAgent-GV
Troj/JsDldr-ET
Mal/DrodZp-A
Troj/MDrop-GWI
Troj/PDFUri-C
Troj/PDF-Y
Troj/VBS-JJ
Troj/Zbot-JZT
W32/MyDoom-O

Peer Heinlein <p.heinlein@heinlein-support.de>

Kommerzieller Virenschutz ist bezahlbar

- Achtung, $$$$$:

  Sophos hat seit Sommer neue Lizenz ideal für Mailgates:

  „Pro Server-Installation bei unlimited Usern“
  - 1 Jahr: 3.500,- EUR / Server; bzw. 3 Jahre 7.000 EUR / Server
  - 2 Server-Cluster = 14.000 EUR für 3 Jahre unlimited User!
    - (Break-Even ggü. klassicher Lizenzierung bei ca. 1.200 Usern)

- Wir haben Amavis vor einigen Jahren die SSSP-Schnittstelle von Sophos beigebracht.
  - Amavis redet „direkt“ mit dem Sophos-SAVDI. Hochperformant. Rockt.
  - Sophos-SAVDI ist OEM-Lizenz; ggf. schwer zu kriegen; fragt uns.

Peer Heinlein <p.heinlein@heinlein-support.de>

Rechnungstrojaner über SpamAssassin filtern

- Seit zwei Jahren viele Viren als Rechnungs-PDFs, Packstation-Notifications und andere „bekannte Mails“ getarnt
- Inhaltlich schwer zu filternde Viren.
- Wir haben SpamAssassin-Pattern gefunden, die zwei Merkmale kombinieren und das gut filtern:

```
header          __HS_XM_BLAT_311_WIN32 X-Mailer =~ /^Blat v3\.1\.1, a Win32 SMTP\/NNTP
mailer http:\/\/www.blat.net/
header          __HS_XOLE_BLAT_311     X-MimeOLE =~ /Produced by Blat v3\.1\.1/
meta            HS_HEADER_SPAM_70      (__HS_XM_BLAT_311_WIN32 && __HS_XOLE_BLAT_311)
score           HS_HEADER_SPAM_70      3.5
```

- Seitdem eigentlich keine Rechnungstrojaner mehr gesehen. :-)
  - Regeln sind im Channel „spamassassin.heinlein-support.de“ enthalten!

Peer Heinlein <p.heinlein@heinlein-support.de>

Rechnungstrojaner über DKIM blocken

- Aber: Auch DKIM hilft.
  - a) Die wichtigsten Versender signieren alle ausgehenden E-Mails mit DKIM
  - b) Mails mit diesen Absendern ohne DKIM sind also ein Fake
- In Amavis-Config also:

  Mails dieser Absender mit harten Spam-Score bestrafen

  ABER

  Mails mit diesen DKIM-Absendern auf die Whitelist so daß der Score egal ist, wenn DKIM vorhanden ist!

```
$policy_bank{'WHITELIST'} = {
     bypass_spam_checks_maps => [1],
     spam_lovers_maps => [1],
};

@author_to_policy_bank_maps= ( {
     'rechnungsstelle@1und1.de'     => 'WHITELIST',
     '1und1.de'                  => 'WHITELIST',
     'rechnungonline@telekom.de'    => 'WHITELIST',
     'servicecenter.gk@telekom.de'  => 'WHITELIST',
     'buchungbestaetigung@bahn.de'  => 'WHITELIST',
     'bahn.de'                      => 'WHITELIST',
     'deutschebahn.com' => 'WHITELIST',
     'commerzbank.com' => 'WHITELIST',
     'paypal.com' => 'WHITELIST',
     'ebay.de' => 'WHITELIST',
     'dhl.de' => 'WHITELIST',
     'dhl.com' => 'WHITELIST',
     'ups.com' => 'WHITELIST',
     'kundenservice.vodafone.com'   => 'WHITELIST',
} );

@score_sender_maps = ({  # a by-recipient hash lookup table
# Mails mit Absendern die DKIM hätten haben müssen
     '.1und1.de'                    => 12.0,
     '.telekom.de'                  => 12.0,
     '.bahn.de'                     => 12.0,
     '.deutschebahn.de'             => 12.0,
     '.paypal.com'                  => 12.0,
     '.ebay.de'                     => 12.0,
     '.dhl.de'                      => 12.0,
     '.dhl.com'                     => 12.0,
     '.kundenservice.vodafone.com'   => 12.0,
});
```

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil V:
Und dann war da noch...

Peer Heinlein <p.heinlein@heinlein-support.de>

Der EU-US Privacy-Shield!

Peer Heinlein <p.heinlein@heinlein-support.de>

Das Ende von „safe harbour“

- EuGH hat Herbst 2015 das „Safe Harbour“ abkommen gekippt
  - Safe Harbour hatte kurzerhand „definiert“, daß US-Recht dem EU-Datenschutzrecht trotzdem gleichwertig ist.
  - Viele Experten und letzlich auch der EuGH sahen das komischerweise anders
  - Problematisch war insb. der anlaßlose Vollzugriff von US-Behörden auf alle Daten
- Firmen, die safe harbour vertrauen, befanden waren plötzlich nicht mehr Datenschutzkonform!
  - Der Hamburger Datenschützer Caspari hat Ende Februar '16 angekündigt, die ersten Bußfelder zu verhängen.
  - Betroffen sind drei große internationale Unternehmen.
  - Vertrauen Unternehmen blind auf safe harbour oder den Privacy Shield gehen sie ein hohes Geschäftsrisiko ein!

Peer Heinlein <p.heinlein@heinlein-support.de>

Also erfinden wir flugs den „Privacy Shield“

- Die EU-Datenschützer kündigten an, Anfang Februar 2016 über Konsequenzen daraus nachzudenken.
  - Ergo: Die Frist für einen Plan-B lief...
- Wenige Tage vor dem EU-Datenschutztreffen wurde der Privacy-Shield verkündet
  - Was für ein Glück, so mußte das gekippte safe harbour nicht mehr zu Konsequenzen führen...
  - Das Abkommen war zu dem Zeitpunkt noch gar nicht fertig, aber die Ankündigung verschaffte Fristverlängerung vor der Eskalation der Datenschützer. :-)

Peer Heinlein <p.heinlein@heinlein-support.de>

Woraus besteht der Privacy Shield?

„Teile des Abkommens könnten die Bevölkerung verunsichern“

Peer Heinlein <p.heinlein@heinlein-support.de>

Woraus besteht der Privacy Shield?

- Wesentliche Teile des Abkommens werden – wie gewohnt – geheim verhandelt und sickern nach und nach durch.
  - So macht man das bei demokratischen Prozessen.
- Vor einigen Tagen sind die ersten belastbaren Papier bekannt geworden.
  - https://netzpolitik.org/2016/dokumente-zu-privacy-shield-veroeffentlicht-safe-harbor-in-neuem-anstrich/

Peer Heinlein <p.heinlein@heinlein-support.de>

So benachteiligt der Privacy Shield die EU-Bürger

- Sie müssen „direkt betroffen“ sein um das Abkommen auf den juristischen Prüfstand stellen zu können.
  - Sprich: Sie müssen erst abgehört worden sein.
    - Woher weiß man das, das man jetzt klagen darf?
- Vor einer Klage müssen EU-Bürger zunächst den (zahnlosen) Verwaltungsweg beschreiten.
  - US-Bürger können direkt und jederzeit klagen.
- Durch US-Ministererlaß wird einseitig festgelegt, wo der Privacy Shield zur Anwendung kommt.
  - Ganze Länder können einseitig vom Schutz ausgenommen werden
- Überwacht wird alles durch einen „unabhängigen“ Ombudsmann.
  - Der gehört dummerweise dem US-Außenministerium an.

Peer Heinlein <p.heinlein@heinlein-support.de>

Räumt der Privacy Shield die Probleme des Safe Harbour-Abkommens aus?

- [T]he U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to **clear limitations, safeguards and oversight mechanisms, preventing generalised access to personal data.**

- Die „klare Begrenzung“ eines Datenzugriffs stellt sich so dar, dass Massenüberwachungsdaten nur noch in sechs Fällen genutzt werden dürfen. Dazu gehören dehnbare Begriffe wie „Cybersecurity“ und „länderübergreifende kriminelle Bedrohungen“.

Dank an / Zitat von: Netzpolitik.org

Und was sagt(e) unsere Bundeskanzlerin dazu?

- „Daten werden der **Rohstoff der Zukunft** sein in der digitalen Welt."
- [Wir werden] „darüber sprechen müssen, dass Big Data nicht eine Bedrohung ist, sondern Wertschöpfungsmöglichkeit der Zukunft ist."
- „Wir haben **das schöne Safe-Harbour-Abkommen** [...], das heißt, es können alle Daten aus Europa nach Amerika geschickt werden, dort zu neuen Produkten verarbeitet werden, und der europäische Kunde ist froh, mit diesen Produkten dann hantieren zu können."
- „In 'ner Debatte um die Datenschutzgrundverordnung, um das Big-Data-Management, und da müssen wir aufpassen, dass wir in Europa nicht ein kleines wenig, **ein klein wenig schizophren sind**."

Merkel auf dem Wirtschaftstag 2015 lt. netzpolitik.org

heinlein

Post-Snowden Mail-Security 2016
[CLT 2016]
Peer Heinlein <p.heinlein@heinlein-support.de>

Schöner Leben mit dem Privacy-Shield!

Peer Heinlein <p.heinlein@heinlein-support.de>

Peer Heinlein <p.heinlein@heinlein-support.de>

Das war mein Best-Of der Mailthemen 2015/2016.

Mehr gerne im persönlichen Gespräch.

(oder per Mail...)

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.

Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 – 42

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Post-Snowden Mail-Security 2016
[CLT 2016]
Peer Heinlein <p.heinlein@heinlein-support.de>

Ja, diese Folien stehen auch als PDF im Netz...
http://www.heinlein-support.de/vortrag

Peer Heinlein <p.heinlein@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Peer Heinlein <p.heinlein@heinlein-support.de>

Wir suchen:
Admins, Consultants, Trainer!

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

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

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

Peer Heinlein <p.heinlein@heinlein-support.de>

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

Bis bald.

Peer Heinlein <p.heinlein@heinlein-support.de>

heinlein

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.