FRAMA
mail. message. managed.

E-MAIL 4.0

E-Mail Sicherheit und Compliance

FRAMA
mail. message. managed.

AGENDA

- Geschichtliches
- Verbreitete E-Mail Irrtümer
- DSGVO 2018 und Anforderungen an sichere E-Mail Übertragungen
- BSI Richtlinie(n) und Technologien
- Praxisüberlegungen / Empfehlungen
- Fazit

FRAMA
mail. message. managed.

ZAHLEN, DATEN, FAKTEN: E-MAIL

- Logische Weiterentwicklung: Brief → Telegramm → Fernschreiben → Telex → Fax
- Ende 1980er Jahre Start Erfolgsweg der E-Mail im Arpanet (***A****dvanced* ***R****esearch* ***P****rojects* ***A****gency* ***Net****work)*
- Erste E-Mail in Deutschland: 3. August 1984 um 10:14 Uhr MEZ an Michael Rotert von der Universität Karlsruhe (TH)
- Im Jahr 2014 wurden in Deutschland rund 506,2 Milliarden E-Mails versendet
- 81 % der Deutschen nutzten E-Mail im Jahre 2015
- Im Jahr 2015 waren weltweit schätzungsweise 4,353 Milliarden E-Mail-Konten von 2,586 Milliarden Nutzern in Gebrauch

FRAMA
mail. message. managed.

WIE WAR DAS 1984 …

Schneider CPC

Macintosh 128K

Amiga 1000

KC85/2

Charts:
Jenseits von Eden
Self Control
Big in Japan

BTX

E-MAIL IN DER PRAXIS …

- … ermöglicht es, ohne Medienbruch Dateien und Nachrichten weltweit zu versenden
- … ist bequem, schnell und extrem weit verbreitet
- … ist für Unternehmen das Kommunikationsmedium Nummer 1
- … ist die meistgenutzte Anwendung im World-Wide-Web
- … wird von den meisten Anwendern nicht hinterfragt

E-MAIL IRRTÜMER

- Falls Ihnen das eine oder andere Statement bekannt vorkommt, oder es sogar gängige Praxis in Ihrem Unternehmen ist, sollten Sie die bestehenden Prozesse hinterfragen und neu definieren!

- Die DSGVO fordert insbesondere bei der Übertragung von persönlichen Daten neue Vorgehensweisen!

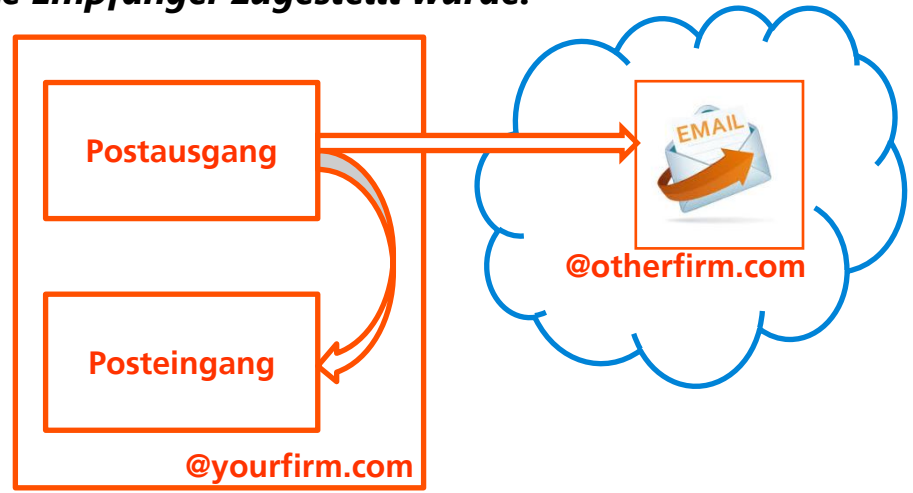
- Normale E-Mail hat vor Gericht nur wenig Beweiskraft, wenn es darum geht festzustellen, wer was wann an wen gesagt hat!

E-MAIL IRRTÜMER (1)

- ***Anwender: Ich kopiere (cc'd oder bcc'd) mich immer in das E-Mail und wenn ich eine Kopie erhalte weiss ich, dass meine Nachricht an alle Empfänger zugestellt wurde.***

- Wenn der Sender und der Empfänger die gleiche E-Mail Domain haben (Beispiel „@yourfirm.com"), kopiert der E-Mail Server gleich lokal die E-Mail .

- Zwischen interner Domain und externer Domain bestehen also unterschiedliche Transportwege!



- Das Einkopieren der eigenen E-Mailadresse ist also **nutzlos!**

FRAMA
mail. message. managed.

E-MAIL IRRTÜMER (2)

- ***Anwender: Ich habe keine Fehlermeldung erhalten, also weiss ich, mein E-Mail wurde zugestellt.***

- Szenario: Spams über unbekannte ISPs versuchen durch Try and Error an gültige E-Mail Adressen zu gelangen.

- Da die meisten von diesen Adressen nicht echt sind, würde ein E-Mail Server Tausende von Meldungen senden.

- Der eigene Server könnte „Black-Listed“ werden!

E-MAIL IRRTÜMER (3)

- ***Anwender: Ich kopiere meinen Mitarbeiter in das E-Mail und dieser druckt eine Kopie (auf Papier oder PDF). Somit kann ich nachweisen, wer, wann, was gesagt hat.***

- Eine gedruckte Kopie ist keinerlei Nachweis, was tatsächlich versendet wurde und kann leicht bestritten werden. Es ist sehr einfach den Inhalt und Zeitstempel einer E-Mail zu ändern und diese dann zu drucken, ohne einen Unterschied zu sehen. → Demo

- Der Empfänger kann einfach sagen, er hätte die Mitteilung nicht empfangen.

- Wenn die Kopien des Kunden und des Empfängers nicht übereinstimmen, wird es schwierig nachzuweisen, wer wann was gesagt hat.

E-MAIL IRRTÜMER (4)

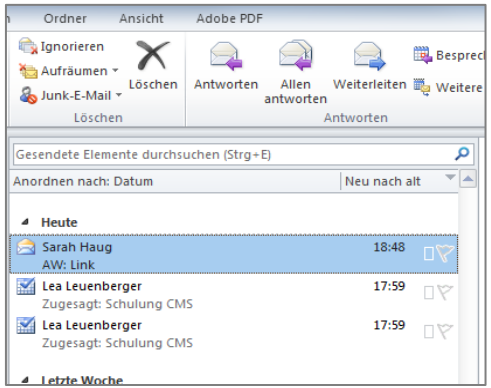
- ***Anwender: Ich speichere alles in meinem Archiv, im gesendeten Elemente Ordner oder im Posteingang. Somit kann ich beweisen, wann die E-Mail versendet wurde und was drin stand.***

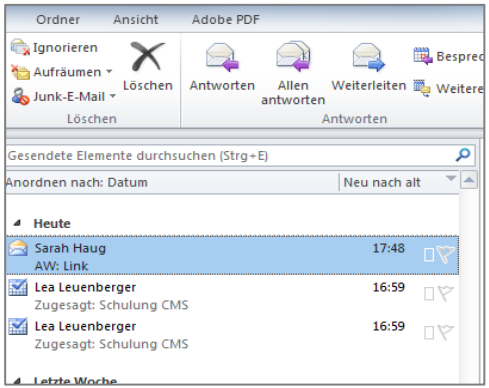
- Fast alle E-Mail Archive speichern weniger als die Hälfte der gesendeten Daten. Das Archiv zeigt an was Sie meinen, gesendet zu haben.

- Ausserdem können die Nachrichten in Ihren Ordnern «Gesendete Elemente» oder Posteingang ganz leicht mit wenigen Klicks manipuliert werden!

E-MAIL MANIPULATION (OUTLOOK)

- **Zeitstempel manipulieren**
  Um den Zeitstempel der E-Mail Kopie in Ihrem gesendeten Ordner oder im Ordner des Empfängers zu ändern, braucht man nur die Computerzeit verstellen. Wenn Sie danach die Mitteilung senden, werden der Zeitstempel und die chronologische Platzierung der E-Mail in Ihrem «Gesendete Elemente» angepasst sein.





E-MAIL MANIPULATION

- **Inhalt verändern:**
  In üblichen E-Mail Programmen kann jeder ganz einfach den Inhalt der Nachricht verändern (→ Demo)

- Die E-Mail bleibt für immer abgewandelt in den «Gesendeten Elementen» oder im «Posteingang», ohne dass eine Spur der Manipulation erkennbar wäre.

- Auch wenn die E-Mail später auf Papier oder PDF gedruckt wird, kann man nicht sagen, was tatsächlich im originalen Text stand.

E-MAIL IRRTÜMER: ZUSAMMENFASSUNG

- Stellen Sie sicher, dass Sie nachweisen können, **wer was wann an wen** gesagt hat.

- Mit der DSGVO kommt ein neues Element hinzu, das WIE!
  Es heißt also neu: **Wer hat wann was wie an wen** gesagt?

- Wer = Absenderauthentifizierung
  Wann = Zeitstempel
  Was = Inhalt
  Wie = Art der Übermittlung
  an wem = Empfänger E-Mail Adresse

  } **Dokumentation**

- Es kommen neue Anforderungen auf uns zu!

BEGRIFFE

- **Vertraulichkeit:** Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschliesslich Befugten in der zulässigen Weise zugänglich sein

- **Integrität:** bezeichnet die Korrektheit / Unversehrtheit von Daten und die korrekte Funktionsweise von Systemen

- **E2E:** Verschlüsselung von Daten von Desktop zu Desktop (in etwa: E-Mail wird verschlüsselt und kann somit über unsicheren Kanal übertragen werden)

- **TLS:** Transport Layer Security: Verschlüsselung von Daten auf dem Transportweg (in etwa: E-Mail wird normal über verschlüsselten Transportweg übertragen)

DSGVO 2018 UND E-MAIL (AUSZUG)

- Beispiel: Artikel 5: Personenbezogene Daten müssen […]

- *(§1f) … in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);*

- **Das heißt konkret: E-Mails mit personenbezogenen Daten müssen in geeigneter Weise geschützt übertragen werden!**

DSGVO 2018 UND EMAIL (AUSZUG)

- Beispiel: Artikel 5

- (§2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

- **Das heißt konkret: Die Einhaltung der DSGVO (Compliance) muss dokumentiert sein. Im Gegensatz zum BDSG fordert die DSGVO *„to demonstrate“*, also eine aktive Rechenschaftspflicht!**

…UND JETZT?

- Einsatz geeigneter Verschlüsselungsmethoden
  - Grundsätze: by Design oder by Default / Technologie
  - Ausschließen menschlichen Versagens
  - Schulungen

- Rechenschaftspflicht
  - Grundsätze: by Design oder by Default?
  - Risikovermeidung: Dokumentation des Versandes mit Fokus auf Compliance (Kette Anwender – E-Mailserver Anwender – Internet – E-Mailserver Empfänger – Empfänger)
  - Archivierungssysteme

RICHTLINIEN FÜR E-MAIL ÜBERTRAGUNG

- BSI TR-03108-1: Secure E-Mail Transport (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108-1.pdf?__blob=publicationFile&v=4)

Requirement	Regulation
EMLREQ_1: TLS (user to EMSP)	Required
EMLREQ_2: TLS (incoming)	Required
EMLREQ_3: TLS (outgoing)	Required
EMLREQ_4: DANE (incoming)	Required
EMLREQ_5: DANE (outgoing)	Required
EMLREQ_6: PKI certificates	Recommended

Table 1: Regulations for the Technical Requirements

VERSCHLÜSSELUNGSTECHNOLOGIEN E2E (1)

- **Symmetrische Verschlüsselung:** Einfach, aber effizient: Symmetrische Verschlüsselung setzt darauf, dass Absender und Empfänger einer Geheimbotschaft den gleichen Schlüssel verwenden. Jeder, der über diesen Schlüssel verfügt, kann daher die Nachricht entschlüsseln - auch dann, wenn er oder sie diese gar nicht lesen dürfte.

Quelle Text: BSI

VERSCHLÜSSELUNGSTECHNOLOGIEN E2E (2)

- **Asymmetrische Verschlüsselung:** Aufwändig, aber übersichtlich: Asymmetrische Verschlüsselung beseitigt das Problem der Verteilung geheimer Schlüssel. […] Man verwendet asymmetrische Verfahren in der Praxis meist zur Verteilung geheimer symmetrischer Schlüssel. Zudem bleibt das Problem einer manipulationssicheren Verteilung von öffentlichen Schlüsseln bestehen.

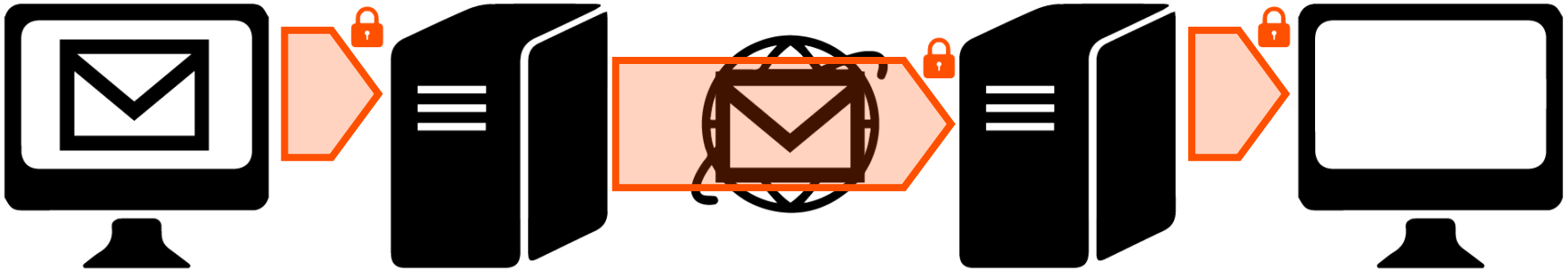
Quelle Text: BSI

VERSCHLÜSSELUNGSTECHNOLOGIEN E2E (3)

- **PKI und Digitale Signatur:** Schlüssel mit Fingerabdruck: Mit einer Public Key Infrastruktur und Digitalen Signaturen kann sichergestellt werden, dass Nachrichten zwischen den richtigen Sendern und Empfängern ausgetauscht und auf dem Weg nicht manipuliert werden. **Achtung: Betreffzeilen werden im Klartext übertragen!**

Quelle Text: BSI

VERSCHLÜSSELUNGSTECHNOLOGIE NETZWERK: TLS



Absender | Mailserver Absender **(TLS)** | Internet | Mailserver Empfänger **(TLS)** | Empfänger

ACHTUNG!

- Funktioniert nur, wenn Sende- und Empfangspunkt TLS unterstützen/aktiviert haben
- Wenn der Empfänger Empfangsserver oder E-Mail-Applikation nicht korrekt eingerichtet hat, wird die Nachricht im Klartext übertragen
- Kommunikation mit dem E-Mail-Server kann TLS-geschützt sein, während die Nachricht trotzdem unverschlüsselt im Internet übertragen wird

FRAMA
mail. message. managed.

ZUSAMMENFASSUNG

- DSGVO: E-Mails mit personenbezogenen Daten müssen geschützt übertragen werden (E-Mail Encryption)
- DSGVO: Es besteht eine aktive Rechenschaftspflicht (Compliance Record)
  - Compliance by Design / by Default
  - Prozesse / Datenmanagement
  - Strafbewehrung!
- DSGVO: Bestehende Vorgehensweisen müssen überprüft und ggf. angepasst werden (E-Mail Irrtümer)
  - Menschen sind das schwächste Glied in der Sicherheitskette
  - Vermeidung von Human Error
  - Aus- und Weiterbildung (personalisierte Angriffe)

FRAMA
mail. message. managed.

PRAXIS E-MAIL ÜBERTRAGUNG

- Es gibt viele verschiedene Verschlüsselungslösungen und bereits viele Initiativen dazu
  - E-Mail made in Germany (TLS Netzwerk. Gründungsmitglieder: United Internet, Deutsche Telekom. Weitere zertifizierte Mitglieder: Freenet, 1&1 Internet, Strato [Quelle: Wikipedia]
  - Volksverschlüsselung (Fraunhofer-Institut)
  - BSI (Richtlinien, Empfehlungen)
  - PGP Initiativen
  - De-Mail
  - usw.
- Anwender? Wo liegt das Problem?

PRAXIS: DER EMPFÄNGER

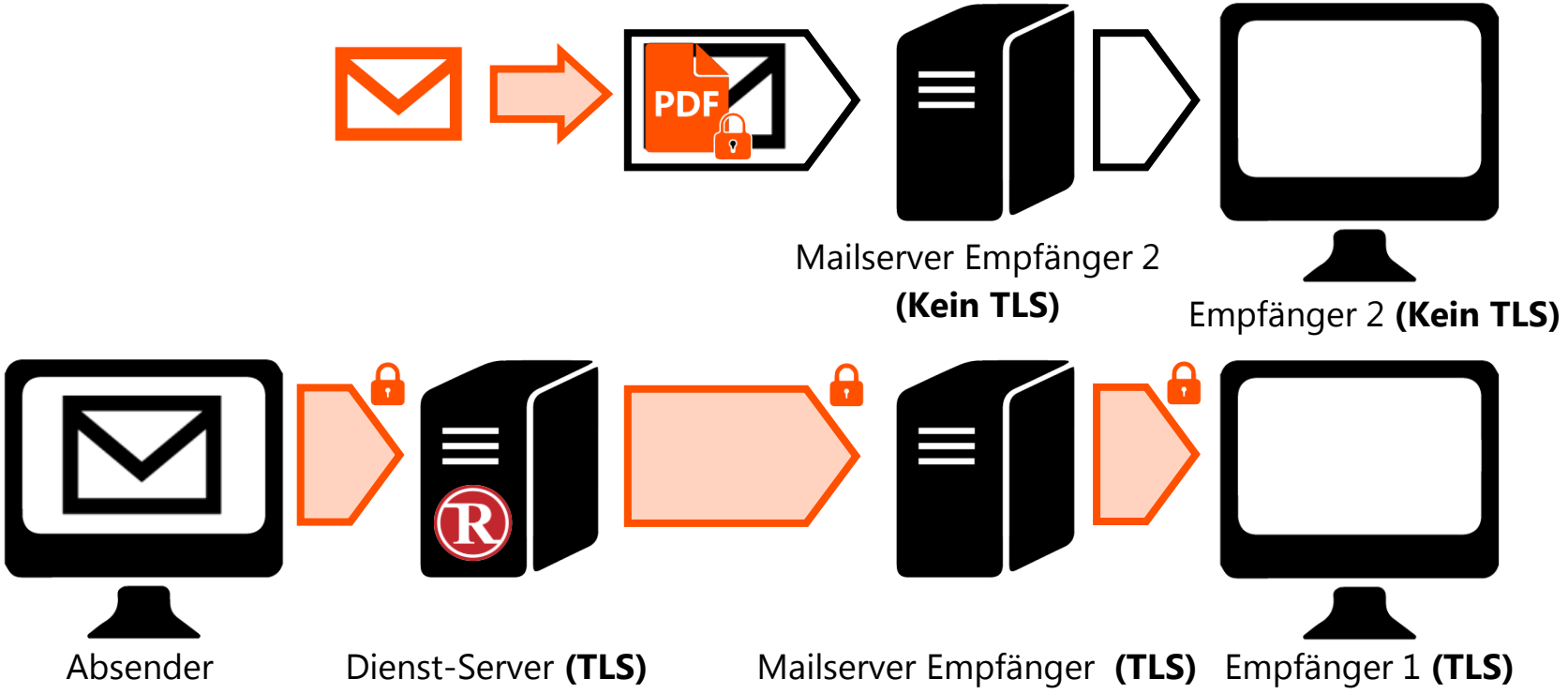
- Viele Lösungen scheitern schlicht am Empfänger (Kunde, Lieferant, Partner)!
  - PKI – Lösungen (PGP, Volksverschlüsselung etc.) überfordern private Kunden
  - De-Mail überfordert De-Bürger (und ist ein geschlossenes System)
  - Store and Forward Systeme überfordern private Kunden (WebMailer, IncaMail)
  - E-Mail made in Germany: TLS ist nicht überall in jedem (EU) Land an jedem Netzwerkpunkt (Server, Client) verfügbar

Fazit: Das Benutzererlebnis auf Empfängerseite entscheidet über die flächendeckende Akzeptanz der Lösung

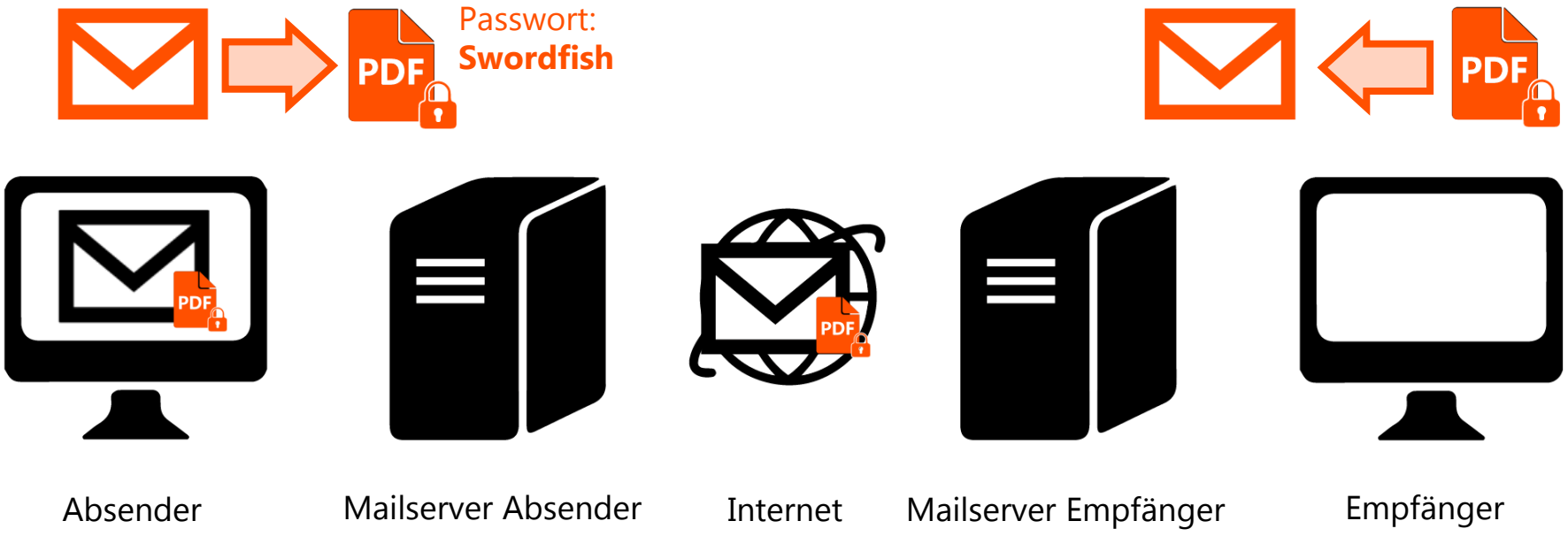
PRAXIS: LÖSUNGSANSATZ

- Mindestanforderungen
  - Grundsätzlich **TLS** auf der gesamten Strecke bis zum Empfänger erzwingen
  - Falls **TLS nicht möglich** ist, Nutzung einer **E2E** Verschlüsselungsmethode (ohne den Empfänger zu überfordern)
  - **Protokollierung** der Übertragung (Rechenschaftspflicht)
  - User Experience auf Empfängerseite: arbeitet mit allen **gängigen E-Mailclients** auf Empfängerseite zusammen
  - User Experience auf Absenderseite: Mitarbeiter nutzen ihre **gewohnte Umgebung**

PRAXIS UMSETZUNGSMÖGLICHKEIT AUTO-TLS

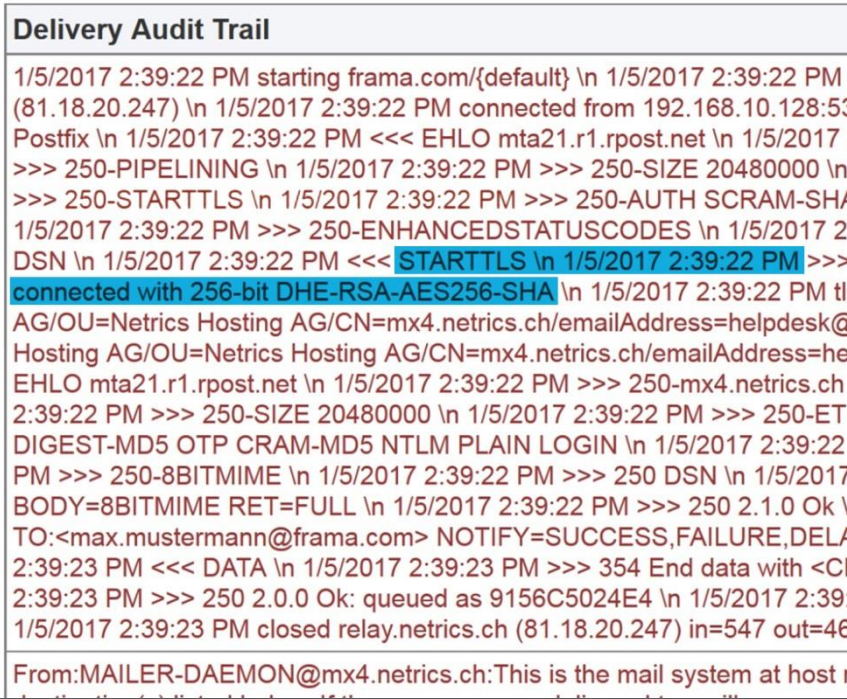


PRAXIS UMSETZUNGSMÖGLICHKEIT: SECURE PDF



PRAXIS: RECHENSCHAFTSPFLICHT

- Verwendung von Diensten zur Protokollierung der Übertragung
  - Server Logs
  - Verschlüsselungsmethodik
  - Verschlüsselte Zustellung
  - Zeitstempel
  - Inhaltsversiegelung
  - Archivierungsmöglichkeit



FRAMA
mail. message. managed.

FAZIT

- DSGVO fordert die geschützte Übertragung von E-Mails mit personenbezogenen Daten bei gleichzeitiger aktiver Rechenschaftspflicht
- Die Empfängerakzeptanz entscheidet über den Erfolg Ihrer geplanten Umsetzung (Muss der Empfänger sich registrieren, ein Konto eröffnen, auf Links klicken, etwas herunterladen oder installieren?)
- Das BSI fordert TLS und DANE und setzt dies konsequent im Bund um (siehe insbesondere BSI TR-03108 ff)
- TLS ist noch nicht flächendeckend bei allen EU E-Mail Empfängern vertreten und daher kann die verschlüsselte Zustellung nicht garantiert werden.
  Sie benötigen ein automatisches Fallback-Szenario, z.B. SecurePDF.
- Die DSGVO konforme Zustellung muss protokolliert werden (Compliance Record)

FRAMA
mail. message. managed.

KUNDENMEINUNGEN

« **Das ist die benutzerfreundlichste Lösung, die ich bisher gesehen habe!** » MITGLIED GESCHÄFTSLEITUNG SCHWEIZER GROSSBANK

« **I think that the one-click-send operation is fantastic, then product will be even more easy to use. And looking out in the future you are able to differentiate, so if some user in Finance want to use the Hand-sign option, they can have another configuration, that open up for use of that module/option.** » IT MANAGER DER GRÖSSTEN REISEVERSICHERUNG IN DK / SW

FRAMA
mail. message. managed.

VIELEN DANK
FÜR IHRE AUFMERKSAMKEIT

Volker Sommerfeld
Product Management
Frama Communications AG
volker.sommerfeld@fra-com.ch