Per Mail sicher kommunizieren

Joachim Lindenberg

Betroffener, Verantwortlicher, Auftragsverarbeiter, Datenschutzbeauftragter,

Berater, Journalist, Informatiker -- kein Jurist

Schneier on Security

AI Will Increase the Quantity—and Quality—of Phishing Scams

A piece I coauthored with Fredrik Heiding and Arun Vishwanath in the *Harvard Business Review*:

> **Summary.** Gen AI tools are rapidly making these emails more advanced, harder to spot, and significantly more dangerous. Recent research showed that 60% of participants fell victim to artificial intelligence (AI)-automated phishing, which is comparable to the success rates of non-AI-phishing messages created by human experts. Companies need to: 1) understand the asymmetrical capabilities of AI-enhanced phishing, 2) determine the company or division's phishing threat severity level, and 3) confirm their current phishing awareness routines.

Here's the full text.

Tags: artificial intelligence, LLM, phishing

https://www.schneier.com/blog/archives/2024/06/ai-will-increase-the-quantity-and-quality-of-phishing-scams.html

Kundennummer: xxxxxxx752

Guten Tag [redacted],

gern senden wir Ihnen künftig wichtige Vertragsinformationen oder Ihre Rechnung an folgende E-Mail-Adresse:

[redacted]

Der Schutz Ihrer Daten ist uns sehr wichtig – ohne Ihre Bestätigung geht es daher nicht.
Wenn Sie schnell und komfortabel Informationen an die genannte E-Mail-Adresse erhalten möchten, klicken Sie bitte **innerhalb der nächsten 7 Tage** auf den Button

E-Mail-Adresse bestätigen

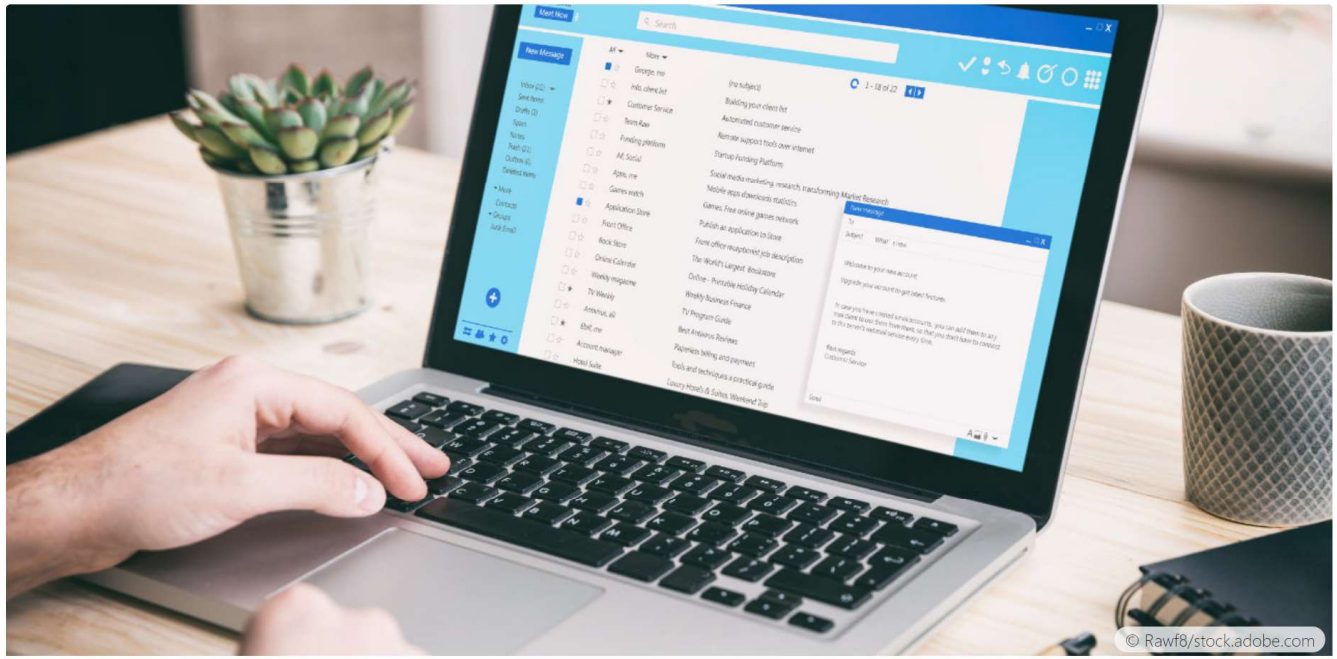
OLG Karlsruhe | E-Mail | Geschäftskorrespondenz | Sonstiges Bürgerliches Recht | Strafrecht

Händler-Mailaccount gehackt: Unternehmer muss doppelt für Auto zahlen

Muss ein Autohändler dafür sorgen, dass sein Mailaccount nicht gehackt werden kann? Das OLG Karlsruhe hält keine besonderen Sicherheitsvorkehrungen für nötig. Ein Autokäufer, der auf eine gefälschte Mail hereinfiel und auf das Konto des Betrügers zahlte, habe nicht erfüllt.

Ende-zu-Ende-Verschlüsselung | Mandantenmails |
EDV-, Multimedia-, Medien- und Postrecht | Berufsrecht der Rechtsanwälte und Notare

Mandantenmails: Bremens Anwälte wehren sich gegen maximale Verschlüsselungspflicht



Wenn es nach der Bremer Datenschutzbehörde geht, dürfen Anwälte mit Mandanten künftig nur noch Ende-zu-Ende verschlüsselt per E-Mail kommunizieren. Nur noch bis Ende des Jahres würden Übergangslösungen akzeptiert. Die Bremer RAK versucht zu vermitteln – bislang ohne Erfolg.

Ulf Buermeyer

Vorstandsmitglied

„Ende-zu-Ende-Verschlüsselung ist inzwischen der anerkannte Mindeststandard in der elektronischen Kommunikation. Der Gesetzgeber muss sicherstellen, dass dieser Mindeststandard bei der vertraulichen anwaltlichen Kommunikation nicht unterschritten wird."

https://freiheitsrechte.org/themen/freiheit-im-digitalen/bea-aber-sicher

Die Ende-zu-Ende-Verschlüsselung ist der Goldstandard, um die Vertraulichkeit von Daten zu gewährleisten, aber sie kann sowohl schwierig als auch zeitaufwändig zu implementieren sein. Oft versuchen Entwickler, Open-Source-Bibliotheken zu verwenden, um sie zu implementieren, aber da sie auf niedriger Ebene angesiedelt sind, eignen sie sich oft nicht für normale Anwendungen.

https://www.seald.io/de

Themen

- Verschlüsselung und Authentifizierung
- Anti-Spam|Viren|Phishing-Techniken
- Ende-zu-Ende-Verschlüsselung

- BSI Grundschutz Kompendium, BSI TR-03108 & TR-03182
- Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

- Erreichbarkeit von Bürgern in Deutschland und deren Sicherheit
- Urteile vs. Technik

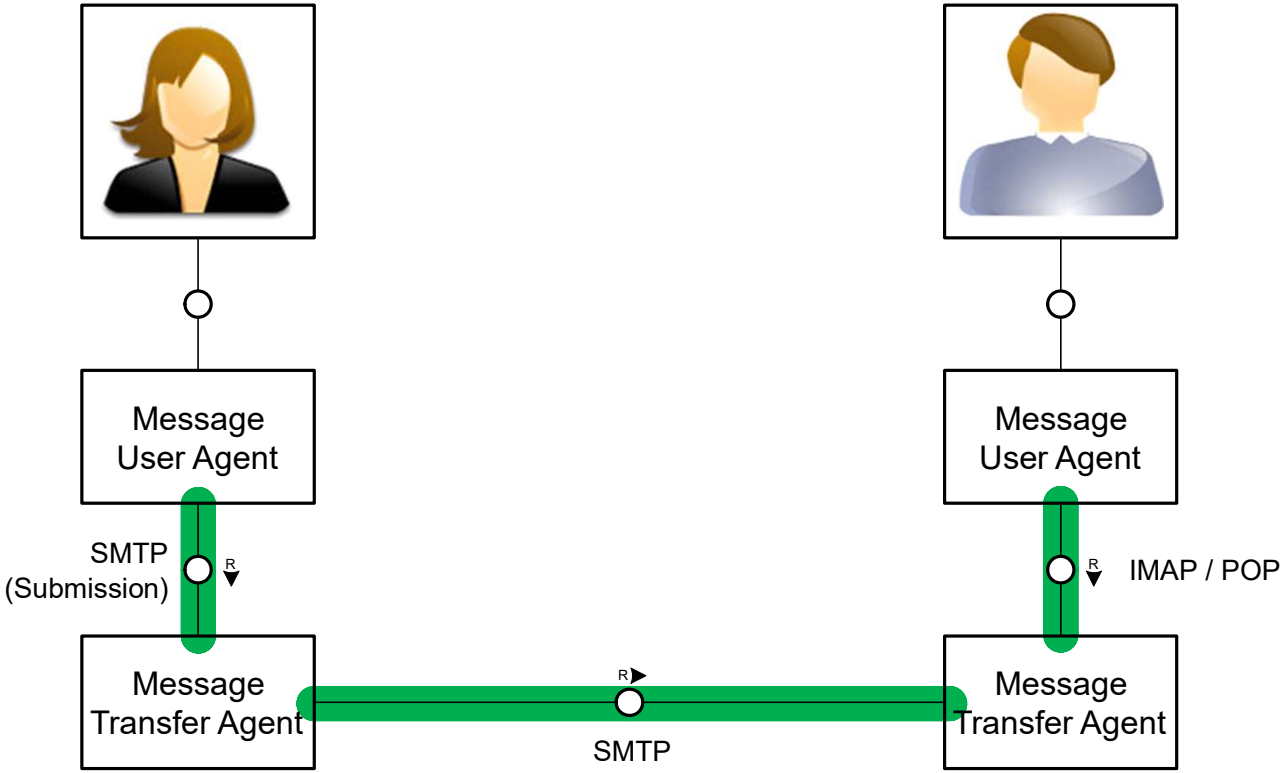
Themen

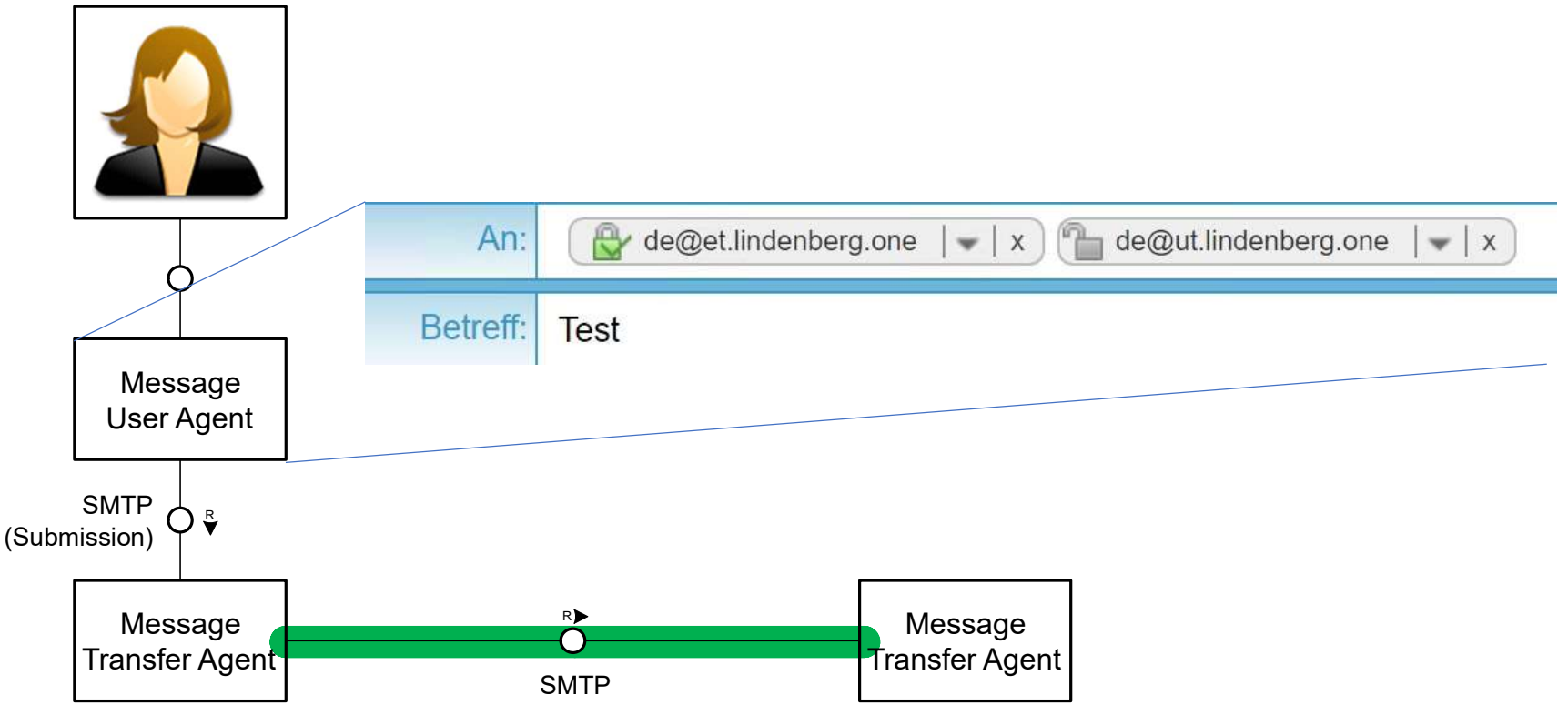
- Verschlüsselung und Authentifizierung
- Anti-Spam|Viren|Phishing-Techniken
- Ende-zu-Ende-Verschlüsselung

- BSI Grundschutz Kompendium, BSI TR-03108 & TR-03182
- Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

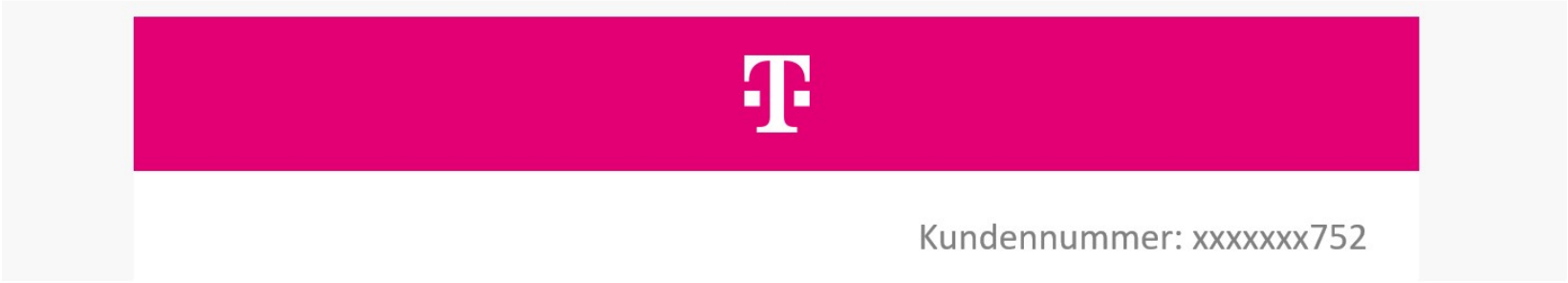
- Erreichbarkeit von Bürgern in Deutschland und deren Sicherheit
- Urteile vs. Technik

Die Erläuterungen dieses Teils finden Sie in https://blog.lindenberg.one/EmailVideo





Received: from mout.gmx.net (mout.gmx.net [212.227.17.22])
(using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
key-exchange ECDHE (P-256) server-signature RSA-PSS (4096 bits) server-digest SHA256)
(No client certificate requested)
by mx1.lindenberg.one (Postcow) with **ESMTPS** id 48549E0E76
for <…@lindenberg.one>; Wed, 20 Sep 2023 07:41:33 +0200 (CEST)
Authentication-Results: mx1.lindenberg.one;
dkim=pass header.d=gmx.de header.s=s31663417 header.b=dbKSl+yy;
dmarc=pass (**policy=none**) header.from=gmx.de;
spf=pass (mx1.lindenberg.one: domain of …@gmx.de designates 212.227.17.22 as permitted sender)
smtp.mailfrom=…@gmx.de
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=gmx.de; s=s31663417;
t=1695188487; x=1695793287; i=…@gmx.de;
bh=vHHGNBWKl0tNwHuBeRaKv6ZiRzKroeJvn3sophZDf8o=;
h=X-UI-Sender-Class:Date:To:From:Subject;
b=dbKSl+yySDhuHkQ1swl9fHLR2PeyfD72umdeFAQ53Cyj8cn71HoM0YwuYo87U5wRW5o1YaNB7ix
kjp3zaniLPspJZFXT+RsZa7GuD4+55BneGmH6/IIhZNAqagsCvrRAD6HPvwfv9czkhb4lxHpFuhZz
urVi+dKeSWtpv2ht1MHr0B0Xd7FwjEBDmDV5fWc+KgkbvXeKo2YoXz+m1IoO9iorSn9U3Scs6Irqf
Tv5KeNKRoNkgZAvaFEhkDT5odlgRtIhipftyoCOeC85yE8kKGtE+G0k2/0KefDAUvuKJy4GnAcvp9
WaLz+bU2BVtvzfn7A8pzYj4dNqwF6dzpuqaw==
Message-ID: <…@gmx.de>
Date: Wed, 20 Sep 2023 07:41:26 +0200
…



Kundennummer: xxxxxxx752

Authentication-Results: mx1.lindenberg.one;
dkim=pass header.d=telekom.de header.s=dtag1 header.b="d42f+/Ay";
dmarc=pass (policy=none) header.from=telekom.de;
spf=none (mx1.lindenberg.one: domain of TKID_DMS-jxRXVB2PT1ibMEtmX-Abrg@dms-bounce.telekom.de has no SPF policy when checking 194.25.225.151)
smtp.mailfrom=TKID_DMS-jxRXVB2PT1ibMEtmX-Abrg@dms-bounce.telekom.de
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=telekom.de; i=@telekom.de; q=dns/txt; s=dtag1;
t=1718797275; x=1750333275;…
Date: Wed, 19 Jun 2024 13:41:08 +0200 (CEST)
From: Telekom <**noreply@telekom.de**>
Reply-To: Telekom No-Reply <noreply@telekom.de>

E-Mail-Adresse bestätigen

Phishing Targobank (Kuketz-Forum)

Return-Path: <targobank@jobs.targobank.de>

Envelope-to:<meine E-Mail-Adresse>

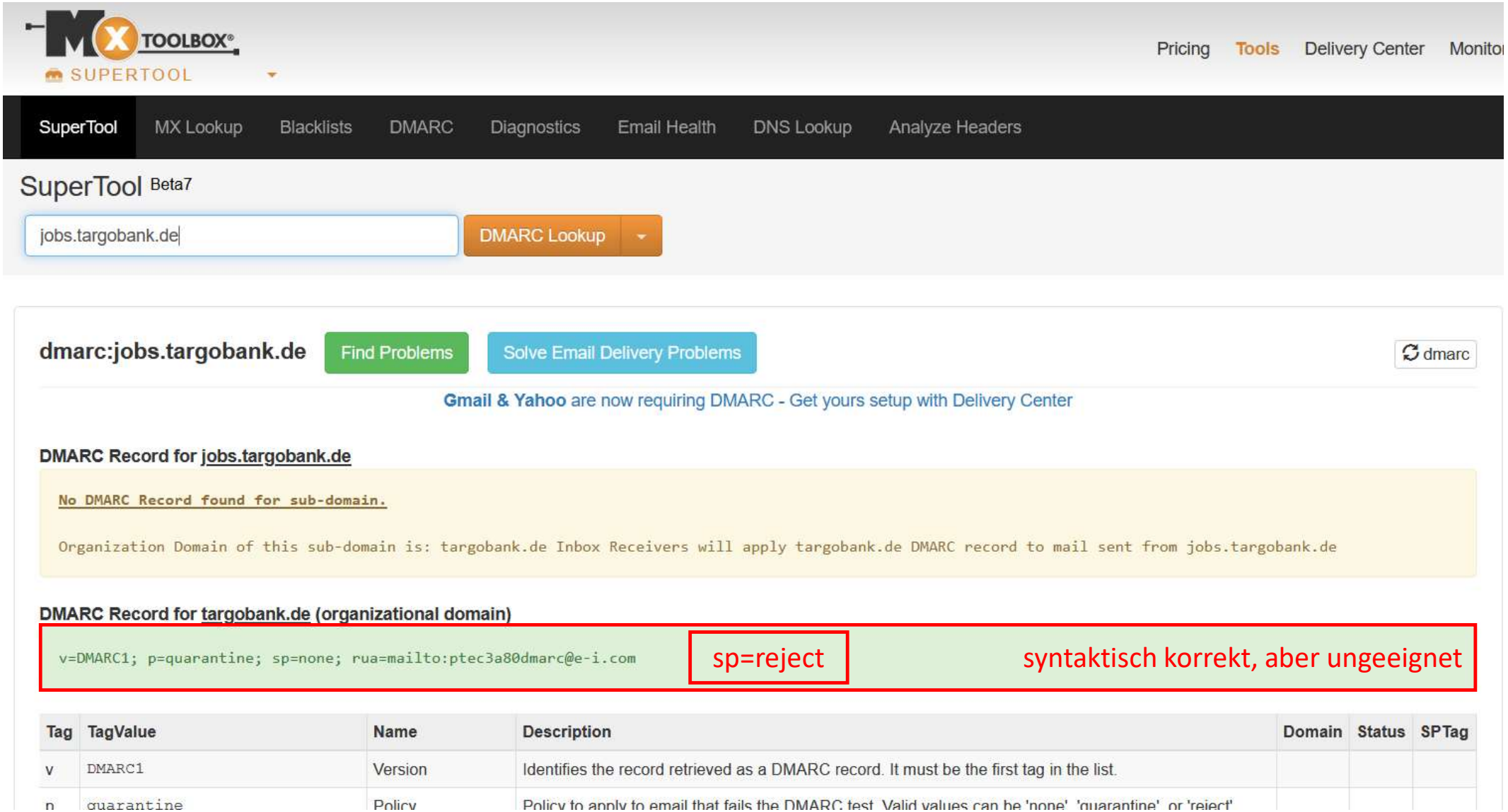
Authentication-Results: www205.<meine_domain>.de; iprev=pass (ip87-106-141-103.pbiaas.com) smtp.remote-ip=87.106.141.103; **spf=none** smtp.mailfrom=jobs.targobank.de; **dmarc=skipped**

From: Targobank-Kontos <**targobank@jobs.targobank.de**>

To: <meine E-Mail-Adresse>

Subject: Ihre Mithilfe ist gefragt: Aktualisieren Sie Ihre Daten

Date: 30 May 2024 04:59:00 +0000



Verschlüsselung und Authentifizierung

- Transportverschlüsselung (inklusive Authentifizierung empfangender Server)
  - RFC 7672 SMTP-DANE für beide Richtungen
  - RFC 8641 MTA-STS beide Richtungen?

- Authentifizierung des sendenden Servers:
  - SPF, DKIM, DMARC (policy ≠ none)
  - +ARC wenn Sie Mails weiterleiten, insbesondere Mailinglisten betreiben

- Bei Email leider (bisher) selten UI-Unterstützung 😣
- Test: https://blog.lindenberg.one/EmailSicherheitsTest

Anti-Spam|Viren|Phishing-Techniken (1)

- Gefälschter Absender
  → SPF, DKIM, DMARC (Unterdomänen nicht vergessen)

- Anderer aber ähnlicher Absender
  → Anti-Phishing Training
  → Greylisting & Blacklisting, Inhalts-Analyse aka Spam-Filter
  → Markierung externer Emails (z.B. Keywords Header für Outlook)

→Eigene Dienste
  →Authentifizierung: Kerberos, Client-Zertifikate, Single-Sign-On
  →konsistente Verwendung der eigenen Domäne

Anti-Spam|Viren|Phishing-Techniken (2)

- Vorsicht bei Miltern, die Mails ändern
  - (z.B. diese Mail kommt von Extern oder URL-Rewriting/Blocking)
  - brechen Signaturen (ggfs. ARC einsetzen)
- Virenscanner Mailserver ≠ Virenscanner Desktop
- Nutzen Sie Quarantäne
- Verbieten Sie die Privatnutzung von Emailkonten der Organisation
  - Phishing viel leichter zu erkennen
  - Keine Probleme mit Vertretungen oder Auskunft nach Artikel 15 DSGVO
  - https://blog.lindenberg.one/NutzungPrivat

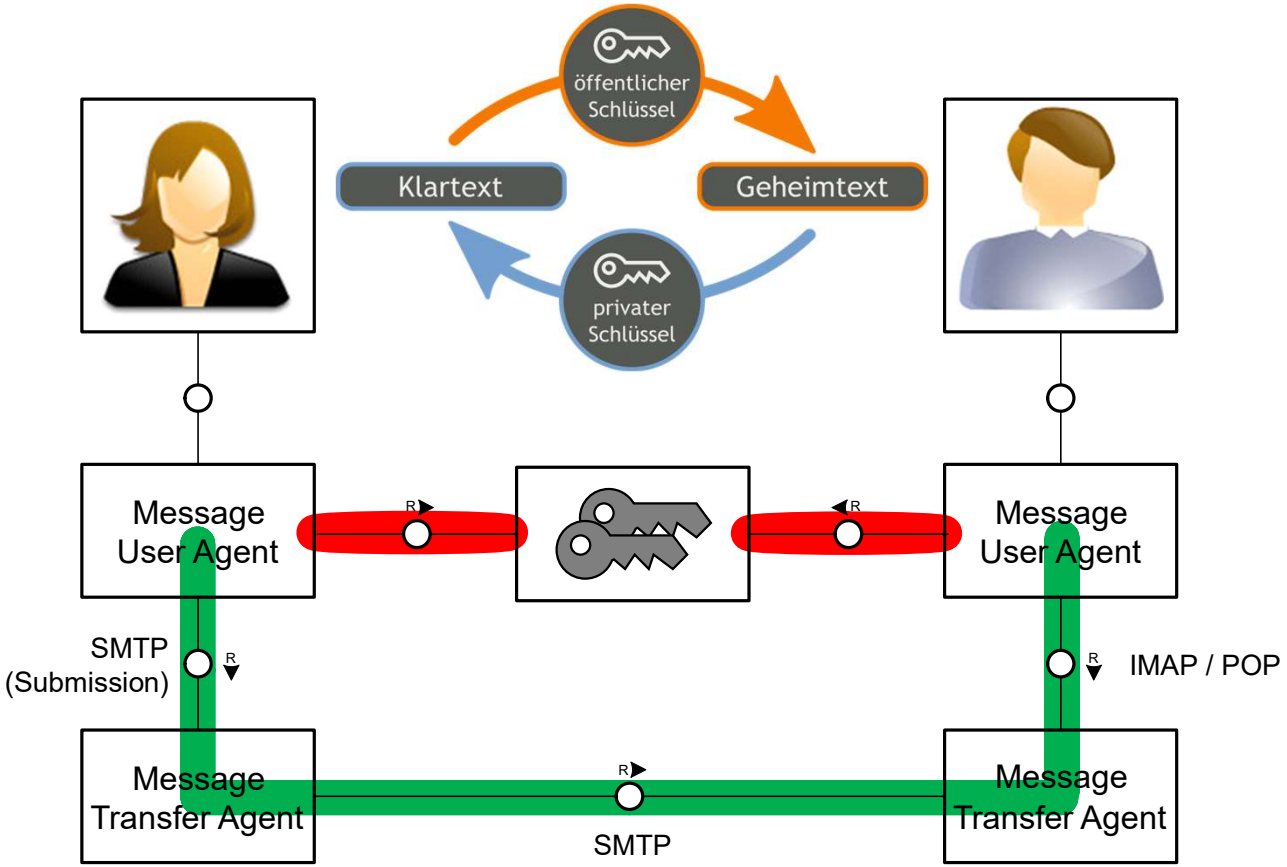
Themen

- Verschlüsselung und Authentifizierung
- Anti-Spam|Viren|Phishing-Techniken
- Ende-zu-Ende-Verschlüsselung

- BSI Grundschutz Kompendium, BSI TR-03108 & TR-03182
- Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

- Erreichbarkeit von Bürgern in Deutschland und deren Sicherheit
- Urteile vs. Technik

Die Erläuterungen dieses Teils finden Sie in https://blog.lindenberg.one/EmailVideo



Schlüsselmanagement für Ende-zu-Ende-Verschlüsselungen

- Geschlossenes System (z.B. WhatsApp, Signal, …)
  - wer kennt und wer sichert den privaten Schlüssel? Der Benutzer?
  - https://blog.lindenberg.one/MythosEndeZuEndeVerschlusselung

- DE-Mail, beA, … – „ein anderer unterschreibt für Sie“
  - Linus Neumann: „Bullshit made in Germany“: „es gibt für jedes technisches Problem eine juristische Lösung“

- Email
  - PGP Web-of-Trust (gebrochen)
  - PGP Web-Key-Directory (konzeptioneller Murks)
  - S/MIME - vertrauenswürdige (vorinstallierte) Zertifikate (teuer -> selten verwendet)
  - RFC 7929 (PGP) bzw. RFC 8162: (S/MIME) (erfordert DNSSEC und Vertrauen in den Domäneninhaber, verwendet kaum jemand)
  - Schlüsseltausch per Email ohne Validierung (Bad Practice)
  - Schlüssel auf Webseite (skaliert nicht)

„Ende-zu-Ende-Verschlüsselung“ PGP oder S/MIME

- Sehe ich kritisch
  - Kein etabliertes organisationsübergreifendes und sicheres Schlüsselmanagement
  - Landen die Daten nicht sowieso im CRM oder Dokumentenmanagement?
  - Probleme mit Vertretungen, Funktionspostfächern und Auskunft nach Artikel 15 DSGVO -> erfordert Schlüsselmanagement der privaten Schlüssel
  - Wenn extern, dann besser mit Gateway
  - Gefahr von verschlüsselter Spam/Malware

- Nischen:
  - Sicherheitsmeldungen
  - Vertraue meinem Anbieter nicht (besser wechseln)
  - Enthusiasten und Datenschutzaufsichten

Themen

- Verschlüsselung und Authentifizierung
- Anti-Spam|Viren|Phishing-Techniken
- Ende-zu-Ende-Verschlüsselung

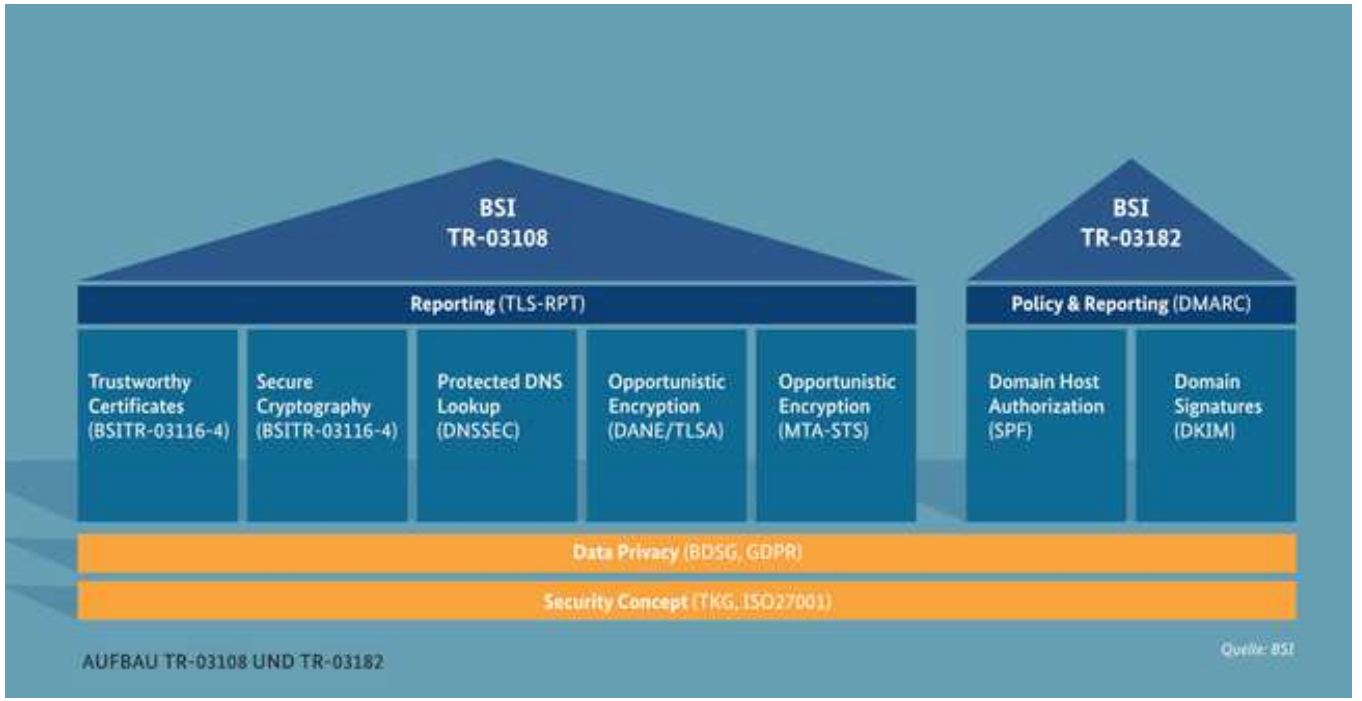
- BSI Grundschutz Kompendium, BSI TR-03108 & TR-03182
- Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

- Erreichbarkeit von Bürgern in Deutschland und deren Sicherheit
- Urteile vs. Technik

BSI Grundschutz Kompendium (Edition 2023)

Modul	Fundstelle	Text / Zusammenfassung
NET.1.1	**A7 (B)**	Schützenswerte Informationen MÜSSEN über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden~~, falls nicht über vertrauenswürdige dedizierte Netzsegmente (…) kommuniziert wird.~~
ORP.4	Einleitung	Benutzende und IT-Komponenten müssen zweifelsfrei identifiziert und authentisiert werden.
APP.5.3	Gefährdungslage 2.6	E-Mails werden in der Regel unverschlüsselt und ohne digitale Signatur versendet. Deswegen können bei einem Angriff E-Mails mitgelesen und sogar beliebig verändert werden. …
	A1 (B)	E-Mail-Clients MÜSSEN für die Kommunikation mit E-Mail-Servern über nicht vertrauenswürdige Netze eine sichere Transportverschlüsselung einsetzen.
	A2 (B)	Für den E-Mail-Empfang über nicht vertrauenswürdige Netze MÜSSEN E-Mail-Server eine sichere Transportverschlüsselung anbieten. Der Empfang von E-Mails über unverschlüsselte Verbindungen SOLLTE deaktiviert werden.
	A9 (S)	***SOLL: DKIM, SPF, DMARC, DANE und MTA-STS***
	A10 (H)	Die Institution SOLLTE eine Ende-zu-Ende-Verschlüsselung sowie digitale Signaturen für E-Mails einsetzen. …

BSI TR-03108 & TR-03182



Ein "E-Mail-Diensteanbieter" oder "Betreiber eines E-Mail-Dienstes in seiner Organisation" kann mit der Konformität zur TR auch einen unabhängigen Nachweis über die Sicherheitsleistung seines E-Mail-Dienstes erbringen. Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03182/TR-03182_node.html

- Vertrauenswürdige Zertifikate? Nur bei MTA-STS? Oder via DANE?
- Sonst nichts unerwartetes
- Zielgruppe unklar, ggfs. TK-Anbieter (Bundesnetzagentur)?

Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

- Autoren: Datenschutzkonferenz Deutschland = 18 Aufsichten
  - Gegenstimme: Bayern (und sind stolz darauf)
  - Abstimmung im Sinne von Artikel 60ff DSGVO? M.W. Fehlanzeige
  - Details in https://blog.lindenberg.one/AufsichtOhneOrientierung und https://blog.lindenberg.one/AufsichtEmail
- Keine Anweisung im Sinne von Artikel 58 Abs. 2 lit. d DSGVO
- Umsetzbar, durchsetzbar?
  - Die meisten Aufsichten halten sich selbst nicht daran
  - keine aktive Durchsetzung bekannt, auch nicht bei Bremer Rechtsanwälten
- Beschwerden werden nicht bearbeitet oder abgewiesen

Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

- Anforderung für öffentliche TK-Anbieter
  - BSI TR 03108 (v1) ≈ SMTP-DANE = opportunistische authentifizierte Transportverschlüsselung
- Anforderung für Verantwortliche risikobasiert (DSK Kurzpapier Nr. 18)
  - Niedrig -> keine Aussage
  - Normal -> obligatorische Transportverschlüsselung
  - Hoch -> qualifizierte = obligatorische und authentifizierte Transportverschlüsselung + Ende-zu-Ende-Verschlüsselung mit PGP oder S/MIME
- Probleme:
  - Fehlende Unterstützung für obligatorische Transportverschlüsselung
  - Fehler in Hintergrundverarbeitung
  - Alle von PGP und S/MIME plus welches davon?

Zusammenfassung und Handlungsempfehlung

- Transportverschlüsselung und Authentifizierung
- Anti-Spam|Viren|Phishing-Techniken
- Vermeiden Sie Ende-zu-Ende-Verschlüsselung

- Bei hohem Risiko:
  - s.o. + Formular mit Prüfung auf Transportverschlüsselung / SMTP-DANE
    … auch wenn die Orientierungshilfe etwas anderes nahelegt

- Disclaimer: meine persönliche Meinung, Sie bleiben verantwortlich

Themen

- Verschlüsselung und Authentifizierung
- Anti-Spam|Viren|Phishing-Techniken
- Ende-zu-Ende-Verschlüsselung

- BSI Grundschutz Kompendium, BSI TR-03108 & TR-03182
- Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

- Erreichbarkeit von Bürgern in Deutschland und deren Sicherheit
- Urteile vs. Technik

Sicherheit der Email-Kommunikation mit Bürgern in Deutschland

- Auswahlkriterien für den Emailanbieter bei Bürgern
- Marktanteile Emailanbieter & Aktuelle Sicherheit
- PGP?

Bei der privaten Kommunikation im Internet kommt es vor allem auf drei Faktoren an:

Sicherheit & Vertrauenswürdigkeit
Vertrauenswürdiger Dienst
Hoher Schutz vor Phishing
Seriöser Dienst
Hoher Schutz der Privatsphäre
Hohe Sicherheit der übermittelten Nachrichten

Zuverlässigkeit & Usability
Hohe Stabilität des Dienstes
Einfache Bedienung
Servicequalität

Verfügbarkeit & Popularität
Verfügbar auf dem Smartphone/ Tablet
Hohe Nutzerzahl
Bekannter Dienst

Basis: n(DACH)=3.000, n(DE)=1.000, n(AT)=1.000, n(CH)=1.000
Frage: Im Internet kann man über unterschiedliche Kanäle mit anderen Personen kommunizieren, z.B. per E-Mail, über Soziale Netzwerke, Foren etc. Wie wichtig sind Ihnen ganz allgemein die folgenden Punkte in der privaten Kommunikation über das Internet? Skala: 1 „sehr wichtig" bis 6"überhaupt nicht wichtig"
Reduzierung der Dimensionen und Zuordnung der Items zu den einzelnen Faktoren erfolgte mithilfe einer exploratorischen Faktorenanalyse
17 Quelle: United Internet Media 2017

Die Wahl des E-Mail-Anbieters basiert auf drei wesentlichen Faktoren:

Einfach & bequem
Kostenloses Angebot/gratis
Leicht und überall zugänglich
Einfache Handhabung/Navigation
Einfach zu merkende Adresse/URL

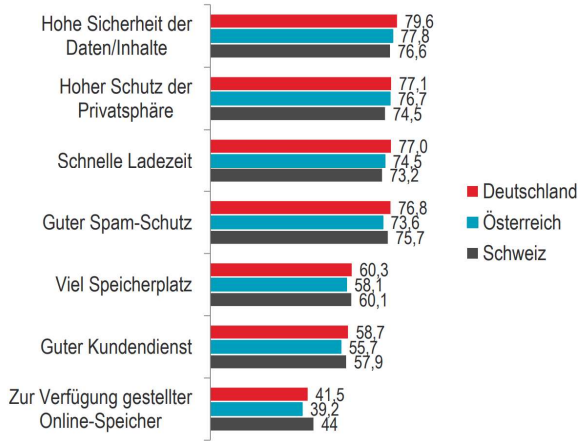
Produktleistung & Sicherheit
Hohe Sicherheit der Daten / Inhalte (z.B. E-Mail Inhalte, Anhänge, ...)
Hoher Schutz der Privatsphäre (z.B. Name, Geburtsdatum, ...)
Guter Spam-Schutz
Guter Kundendienst
Schnelle Ladezeit
Viel Speicherplatz
Zur Verfügung gestellter Online-Speicher (=Cloud Services)

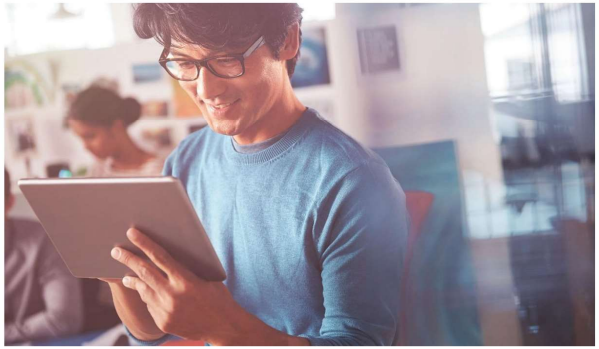
Empfehlung/Image
Empfehlung aus dem Freundes- und Bekanntenkreis
Empfehlung von Experten (z.B. aufgrund von Testberichten, ...)
Große Popularität/Bekanntheit
Internationaler Anbieter

Basis: n(DACH)=3.000
Frage: Wie wichtig sind bzw. waren folgende Gründe bei der Wahl Ihrer E-Mail-Adresse von *Anbieter*?
Reduzierung der Dimensionen und Zuordnung der Items zu den einzelnen Faktoren erfolgte mithilfe einer exploratorischen Faktorenanalyse
56 Quelle: United Internet Media 2017

80% legen hohen Wert auf die Sicherheit der Daten, drei Viertel auf einen hohen Schutz der Privatsphäre.

Gründe für die Wahl des E-Mail-Anbieters – Produktleistung & Sicherheit – Top-2-Werte



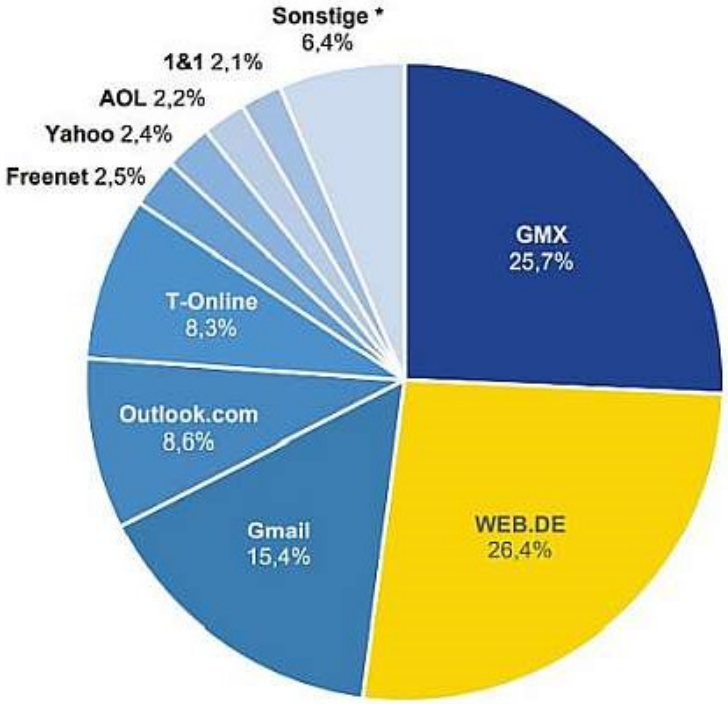


Basis: n(DE)=1.000, n(AT)=1.000, n(CH)=1.000, Angaben in Prozent, Antworten sortiert nach Deutschland
Frage: Wie wichtig sind bzw. waren folgende Gründe bei der Wahl Ihrer E-Mail-Adresse von *Anbieter*?
58 Quelle: United Internet Media 2017

Was versteht ein Anwender unter „Hohe Sicherheit der Daten/Inhalte“ oder „Guter Spam-Schutz“?
(die Antworten waren vorgegeben)

Quelle: https://www.united-internet-media.de/fileadmin/uim/media/home/downloadcenter/studien/UIM_Research_E-Mail-fuer-Dich_Gesamt.pdf (2017)

Marktanteile Emailanbieter (2022)
Email-Sicherheit von Bürgern in Deutschland



Quelle: https://www.united-internet-media.de/ch/newsroom/vermarkterblog/blog/show/e-mail-markt-deutschland-52-prozent-nutzen-primaer-gmx-und-webde/

	Web.de	Gmx	Gmail	Outlook	T-Online
SMTP-DANE	✓(1) / ✓	✓(1) / ✓	✗ / ✗	✓ / ✗	✗ / ✗
MTA-STS	✗ / ✗	✗ / ✗	✓(2) / ✓	✓ / ✓	✗ / ✗
SPF	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✗ / ✗
DKIM	✓ / ✓	✓/ ✓	✓ / ✓	(3) / ✓	✗ / ✓
DMARC	(4) / ✗	(4) / ✗	(4) / ✓	(4) / ✓	✗ / ✗

abgehend / eingehend , ✓ vorhanden, ✗ nicht vorhanden.

(1) SMTP-DANE fehlerhaft aber mit vertrauenswürdigen Zertifikaten ok
(2) MTA-STS policy caching nicht konform zu RFC 8461
(3) *.com und Kundendomänen ja, bei anderen ARC
(4) Policy enthält (s)p=none

Für Kundendomänen müssen Anbieter und Inhaber kooperieren.

PGP?

500.000 Adressen/ Schlüssel weltweit, bei 4-8 Mrd Emailadressen

=> vernachlässigbar

https://keys.openpgp.org/about/stats

Themen

- Verschlüsselung und Authentifizierung
- Anti-Spam|Viren|Phishing-Techniken
- Ende-zu-Ende-Verschlüsselung

- BSI Grundschutz Kompendium, BSI TR-03108 & TR-03182
- Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“

- Erreichbarkeit von Bürgern in Deutschland und deren Sicherheit
- Urteile vs. Technik

OLG Karlsruhe | E-Mail | Geschäftskorrespondenz | Sonstiges Bürgerliches Recht | Strafrecht

Händler-Mailaccount gehackt: Unternehmer muss ~~doppelt~~ dreifach für Auto zahlen

Muss ein Autohändler dafür sorgen, dass sein Mailaccount nicht gehackt werden kann? Das OLG Karlsruhe hält keine besonderen Sicherheitsvorkehrungen für nötig. Ein Autokäufer, der auf eine gefälschte Mail hereinfiel und auf das Konto des Betrügers zahlte, habe nicht erfüllt.

Kosten des Verfahrens

Position	€
Auto an Angreifer	13.500
Auto an Verkäufer	13.500
Prozesskosten	10.445
Zinsen (*)	2.000
Gesamtsumme	39.445

* 9% über Basiszins, ca. 20 Monate

alles ohne Umsatzsteuer

LG Mosbach 1 O 271/21 vom 24.05.2022 vs. OLG Karlsruhe 19 U 83/22 vom 27.07.2023

Angriff auf was?

- Hacker…

unverbindlich

- ~~Orientierungshilfe~~…

unpräzise

nicht beantwortet

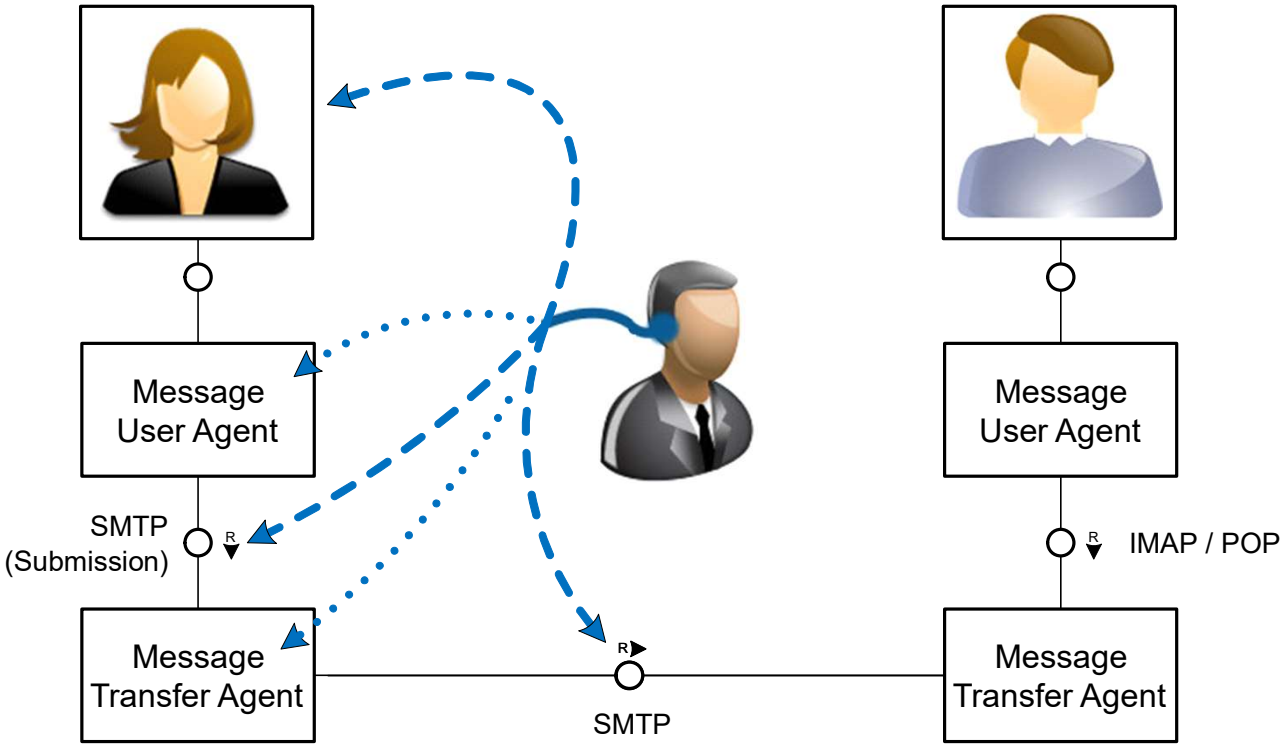
- keine Verwendung des „Sender Policy Framework (SPF)“
- keine ~~Ende-zu-Ende-Verschlüsselung oder~~ Transportverschlüsselung

wenig benutzt, sicher?

obligatorisch? *authentifiziert?*

Ist die Email signiert? (DKIM?)

nicht gefragt



Sorgfaltspflichten / Schadensersatz?

- Angriff auf das Emailkonto des Versenders -> Versender
  - Erkennbar ggfs. an einer korrekten DKIM-Signatur
  - Dass Emailanbieter gehackt wurde eher unwahrscheinlich

Sicht des Technikers, keine Rechtssprechung dazu

- Angriff auf die Übermittlung zwischen Sender und Empfänger
  - Konnte Eve bzw. Mallory die Nachricht mitlesen? W… …en? Wurde STARTTLS oder SMTP-DANE verwendet?
  - Konnte die Nachricht vo… …Mallory als Spam erkannt werden? Wurden DKIM, SPF, DMARC verwendet und ausgewertet?

Im Zivilprozess ist jede Partei selbst verantwortlich, das für sie günstige zu behaupten, belegen, beweisen

- Im konkreten Fall:

Standard	Sender = web.de	Empfänger = netplans.de
STARTTLS, SMTP-DANE	✓, ✓	✓, ✗
DKIM, SPF, DMARC	✓, ✓, ✗	???

Was schreiben Juristen (1)?

„Die Entscheidung ist zu begrüßen. Dem erheblichen Aufwand der Absicherung eines E-Mail-Postfachs steht der deutlich geringere Aufwand eines Schuldners gegenüber, einfach beim Gläubiger nachzufragen, ob wirklich an einen Dritten gezahlt werden soll. Eine 100%ige Absicherung wird es aus rein technischen Gründen ohnehin nicht geben können. …“

Dr. Dirk Diehm, Betriebs-Berater 2023, 2644.
Richter am OLG Bamberg, ZPO- und BVerfGG-Kommentator

Was schreiben Juristen (2)?

„Dem Empfänger vor diesem Hintergrund die volle Beweislast dafür aufzuerlegen, dass es gerade innerhalb des Einflussbereichs des Absenders zur Kompromittierung der E-Mail kam, ist daher beachtlich. Letztlich müsste er beweisen, dass die E-Mail nicht bei seinem E-Mail-Provider oder sonstigen beteiligten Internet-Service-Providern, die nicht als Erfüllungsgehilfen des Absenders anzusehen sind, kompromittiert wurde. Diesen Anforderungen zu genügen, wird in den wenigsten Fällen gelingen. ...“

Dr. Lutz Keppeler/Manuel Poncza/Dr. Ruben Schneider,
Computer & Recht 12/2023, S. 787ff
RAe ua. für IT-(Sicherheits)-Recht bei Heuking Kühn Lüer Wojtek

Was schreiben Juristen (3)?

„Das Urteil ist in der Literatur teilweise mit der Begründung begrüßt worden, man könne bei der E-Mail-Kommunikation „aufgrund des erheblichen Aufwands“ keine Ende-zu-Ende-Verschlüsselung erwarten.“

„Sowohl E-Mail-Signaturen mit GPG und S/MIME als auch Ende-zu-Ende-Verschlüsselung von E-Mails sind Stand der Technik und müssen maßgeblich sein für die gemäß § 276 BGB geschuldete Sorgfalt in der E-Mail-Kommunikation. Nicht nachvollziehbar ist, dass das OLG Karlsruhe stattdessen von „berechtigten Sicherheitserwartungen des Verkehrs“ ausgeht ... .“

Dr. Florian Deusch/Prof. Dr. Tobias Eggendorfer,
Kommunikation & Recht 4/2024, S. 242ff

Résumé

- Kein Zwang
- Showcase guter Sicherheit
- Machen Sie Juristen das Leben schwer(er)

Q&A, Diskussion

Sichere Kommunikation bei Email – auch bei Ihrer Organisation?

Scannen und Email absenden, wenn Sie mehrere Konten haben auch gerne mehrfach.

Sollten Sie eine Fehlermeldung bekommen bitte solange wiederholen bis keine mehr kommt.

Windows / Android

MacOS / IOS