PRIVAZYPLAN®
BRINGT IHREN DATENSCHUTZ AUF KURS.

# Nachweis der sicheren Konfiguration von E-Mail-Servern

[Dieses Formular wurde am 26.06.2021 aus dem Kapitel 12.16.5 des PrivazyPlan® entnommen. In der Zwischenzeit könnte es sich geändert haben. Bitte prüfen Sie dies vorab.]

## Sichere Konfiguration von E-Mail-Servern

Im Juni 2021 wurde hinsichtlich der **Sicherheitseinstellungen von E-Mail-Servern** eine **Orientierungshilfe** von den deutschen „Datenschutz-Konferenz“ beschlossen. Die hier vorliegende Checkliste soll helfen die Anwendung jener Orientierungshilfe zu erleichtern.

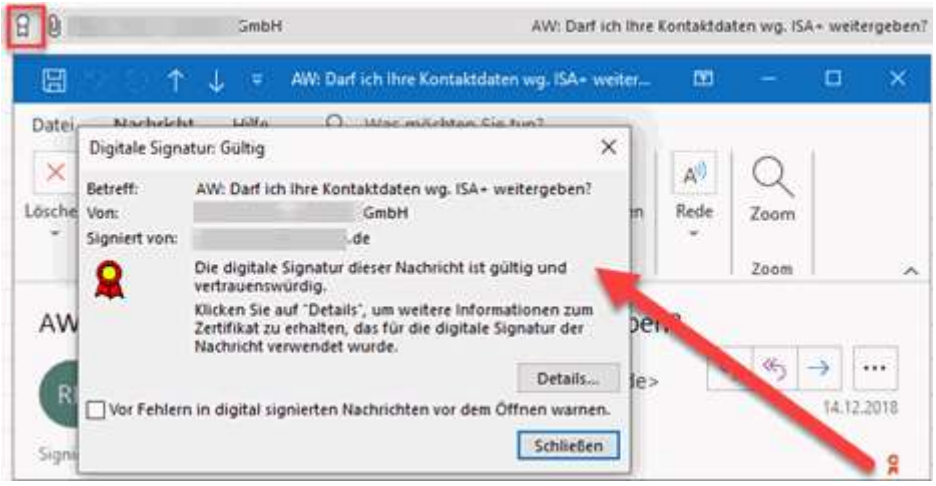
Es ist sehr gut denkbar, dass ein von Ihnen genutzter E-Mail-Provider (bzw. ihr eigener E-Mail-Server) nicht über die erforderlichen Technologien zur Authentizität bzw. Vertraulichkeit verfügt. In diesem Falle müssten Sie über Alternativen nachdenken.

☐ Die DSK-Orientierungshilfe vom 16.06.2021 hat die IT-Abteilung zur Kenntnis genommen. Ergänzend ist die 70-seitige Erklärung/Anleitung des „Bundesverband IT-Sicherheit e.V.“ empfehlenswert.

☐ Auch **E-Mail-Signaturen** werden in der obigen Orientierungshilfe vom Juni 2021 thematisiert. Mit qualifizierten elektronischen Signaturen kann ein Absender von E-Mails die technischen Voraussetzungen schaffen, dass Manipulationen seitens des E-Mail-Empfängers entdeckt werden können. Diese Manipulationen können u.a. darin bestehen, dass **(a)** der Inhalt einer E-Mail auf dem Weg der Übertragung verändert wird oder **(b)** dass ein Dritter sich für eine andere Person ausgibt. Gute Erläuterungen finden sich u.a. hier.

WICHTIG: Die Signatur an sich ist keine Verschlüsselung. Es geht also allein um die Authentizität und Integrität der E-Mails.

Die folgende Abbildung zeigt die Darstellung einer signierten E-Mail in MS-Outlook. Links neben der E-Mail findet sich das (rot umrandete) Signatur-Logo, wodurch der Empfänger sicher sein kann, dass der Absender und der Inhalt korrekt sind. Wenn man in der E-Mail auf das rote Signet klickt, so erfährt man mehr Details zum Inhalt der Signatur.




Manchmal ist die Darstellung der Signatur hingegen **unübersichtlich**. Dies ist z.B. dann der Fall, wenn man ein selbst erstelltes PGP-Zertifikat nutzt… dann sieht der Empfänger nur kryptische Dateien etc. und ist völlig verunsichert. Aus diesem Grund empfiehlt sich ein „offiziell bestätigtes S/MIME-Zertifikat" (z.B. hier); die Einbindung in MS-Outlook wird hier erklärt). Eine Anleitung aus dem TOM-Guide® findet sich hier. WARNUNG: Der Umgang mit S/MIME-Zertifikaten ist alles andere als trivial!

Für eine hohe Authentizität empfehlen sich „Identitätsvalidierte Zertifikate" ab 29 € jährlich pro E-Mail-Adresse (dort muss eine Personalausweis-Kopie hochgeladen werden). Es gibt auch Abteilungs-Zertifikate ab 179 € jährlich, wo auch Abteilungs-E-Mail-Adressen enthalten sind (dann muss man nicht für jeden Mitarbeiter ein eigenes Zertifikat erwerben).
Tipp: In allen Fällen sollten Sie die „privaten Schlüssel" dieser Zertifikate sichern, um auch nach Ablauf des Zertifikats auf ggf. verschlüsselte Inhalte zugreifen zu können.

Eine **E-Mail-Verschlüsselung** ist mit den meisten S/MIME-Zertifikaten möglich. Insofern wäre dann meist auch die Vertraulichkeit gewährleistet (siehe Seite **Fehler! Textmarke nicht definiert.** im PrivazyPlan® zu den verschiedenen Verschlüsselungsmöglichkeiten).

Die folgenden **Nachteile** dieser Signaturen im Arbeitsalltag kann man feststellen: **(a)** Jede E-Mail hat im Posteingang des Empfängers das Büroklammer-Symbol, sodass man denken würde, die E-Mail hätte einen echten Dateianhang. Hat sie aber nicht (sondern nur die Signatur). Insofern kann der Empfänger nicht mehr auf einen ersten Blick im Posteingang die Existenz von Dateianhängen erkennen, **(b)** Die Validierung von Signaturen durch den E-Mail-Client des Empfängers (z.B. MS-Outlook) kann fehlschlagen, wenn die Zwischen-Zertifikate der Anbieter nicht auffindbar sind. Das ist sehr ärgerlich, weil dann z.B. MS-Outlook vor manipulierten E-Mails warnt, **(c)** wenn ein S/MIME-Zertifikat sein Gültigkeitsende erreicht hat, so wird es ungültig und der E-Mail-Client könnte warnen, dass die E-Mail möglicherweise manipuliert worden sei.... ein sehr unangenehmer Effekt; daher sollte man von Anfang an die maximal mögliche Laufzeit (meist drei Jahre) kaufen.

☐ Dies ist die Liste unserer **E-Mail-Domains** (diese Liste soll helfen die weiter unten aufgeführten Fragen zu beantworten): …

☐ Bei welchen E-Mail-Domains droht ein **erhöhte Risiko**, weil „sensible Daten" zu erwarten sind, bzw. wo die Rechte und Freiheiten der betroffenen Personen gefährdet sein könnten? Hier wären dann die in der Orientierungshilfe erwähnten Sicherheitseinstellungen für E-Mail-Server zu erwarten („qualifizierte Transportverschlüsselung" [1] bzw. „Ende-zu-Ende-Verschlüsselung).

[1] Hinsichtlich der „**qualifizierten Transportverschlüsselung (qTLS)**" bietet www.ComCrypto.de eine technische Lösung an. Ein zwischengeschaltetes „Mail eXchange Gateway (MXG)" untersucht die Sicherheit beim Versenden Ihrer E-Mais. Das MXG prüft ähnlich einem Webbrowser bezüglich https://. Ein automatischer Passwortschutz von Anhängen ist möglich, falls der Empfänger-Server unsicher ist und die E-Mail ein hohes Risiko in sich birgt (ein SMS-Gateway kann das Passwort übertragen). Normalerweise bleibt eine qualifizierte Signatur (siehe Seite 486) unverletzt. Im Betreff kann ein Schlosssymbol eingeblendet werden, damit der Empfänger die Sicherheit erkennt. Ein Outlook-AddIn ist in Arbeit. Der Server ist als „virtuelle Maschine" oder als Cloud-Lösung („externes Relay" in

Dies wäre insbesondere der Fall, wenn wir
a) der beruflichen Schweigepflicht gemäß § 203 StGB unterliegen (eine Zusammenfassung der Besonderheiten von Berufsgeheimnisträgern findet sich im PrivazyPlan® auf Seite 548. )
b) als berufsmäßig tätiger Gehilfe bzw. DSB für den Obigen tätig sind
c) betroffene Personen ihre Persönlichkeitsrechte per E-Mail wahrnehmen
d) das Passwort-Rücksetzen von Web-Accounts per E-Mail geschieht
e) etc.

(**Hinweis:** Insbesondere der Punkt „c" dürfte sehr oft gegeben sein!)

und dies gilt für verschiedene **Nutzungs-Szenarien**, wo die jeweiligen Risiken zu untersuchen sind:
a) bei der Übertragung vom Client vom/zum E-Mail-Server
b) bei der Übertragung zwischen den E-Mail Severn (Stichwort „TLS")
c) bei der Einschaltung externer Dienstleister (z.B. externe SPAM-Filter oder Virus-Prüfungen oder Archiv-Diensten)
d) bei eventuellen E-Mail-Weiterleitungen seitens des Empfängers (bzw. ggf. vorliegenden Familien-Accounts, so eigentlich unbefugte Dritte Zugriff haben)
e) beim Zugriff auf die E-Mails von ausgeschiedenen Mitarbeitern, wo im Nachhinein andere Kollegen das E-Mail-Postfach übernehmen.
f) im Rahmen der steuerlich relevanten Archivierung, wo ggf. die Buchhaltung und externe Prüfer auf unverschlüsselte E-Mails zugreifen müssen (oder eben nicht dürfen)
g) etc.

Diese „sensiblen Sachverhalte" gelten für die folgenden E-Mail-Domains: …

Das **Verwaltungsgericht Mainz** hat hier ein sehr interessantes Urteil gesprochen: Rechtsanwälte können sich bei „normaler" E-Mail-Korrespondenz auf die normale TLS-Transportverschlüsselung verlassen. (Az. 1 K 778/19.MZ vom 17.12.2020). Besonders interessant ist die RdNr. 40: „*Ebenso gehört die etwaige (unbefugte) Kenntnisnahme Dritter von Inhalten der elektronischen Kommunikation – wie auch bei anderen (analogen) Kommunikationsformen – zum **allgemeinen Lebensrisiko***".
Neu im Juli 2021: Auf diesen Aspekt der Risikoabwägung geht die im Juni 2021 überarbeitete Orientierungshilfe im (neuen) Kapitel 4.2.3 ein.

Der Datenschutz-Berater 03/2021 beleuchtet das Gerichtsurteil ausführlich auf Seite 88-90: Der Knackpunkt an TLS ist die Tatsache, dass nicht unbedingt alle Empfänger TLS unterstützen. Eine „obligatorische" Transportverschlüsselung wäre sinnvoll (oder man nutzt die qualifizierte Transportverschlüsselung per DANE).

Mittels „**MTA-STS**" kann ein Verschlüsselungs-Zwang beim Empfang von E-Mails mit relativ wenig Aufwand konfiguriert werden. Mehr Details und eine konkrete Anleitung finden sich im PrivazyPlan® auf Seite 513.

☐ Werden die **Software-Updates** des E-Mail-Servers schnellstmöglich installiert? Am 03.03.2021 war es ein Sicherheits-Update zum MS-Exchange-Server, welches unmittelbar eingespielt werden musste (siehe BSI und hier). Allein in Deutschland war eine fünfstellige Anzahl an MS-Exchange-Server betroffen. Die Auswirkungen der Sicherheitslücken sind so drastisch, dass die Datenschutz-Aufsichtsbehörden in Niedersachsen und Bayern es schon als meldepflichtige Datenschutzverletzung ansehen (siehe Kapitel 5.4 und 12.17.1), wenn dieses Update nicht spätestens am 05.03.2021 installiert wurde. Eine Kompromittierung der IT kann aber auch schon Wochen vorher passiert sein, insofern gilt es weitere Untersuchungen anzustellen. Es scheint, dass erfolgreiche Attacken nicht möglich waren, falls ausschließlich VPN-Verbindungen von außen eingerichtet wurden.
(Nebenbei: IT-Administratoren sind gut beraten die BSI-Cyber-Sicherheitswarnungen täglich im

---

Form einer Auftragsverarbeitung) verfügbar. Im Falle der Cloud-Lösung liegen die E-Mails in der Regel nur eine Sekunde auf dem MXG-Server. Die Kosten liegen bei 30 € (für 5 Postfächer) pro Monat. Prüfen Sie schnell und kostenlos, ob Ihr E-Mail-Server die gleiche Sicherheit bietet über test@evaluation.comcrypto.de. [Am 09.09.2020 haben wir an einem ausführlichen Webinar teilgenommen.]

Blick zu haben.)

☐ Welche E-Mail-Domains können wir derzeit **angemessen schützen**? Die Schutzmaßnahmen werden jeweils konkret nachgewiesen.
…

☐ Welche E-Mail-Domains können wir derzeit **nicht angemessen schützen**, sodass wir auf Alternativen ausweichen müssen? Dies wäre beispielsweise ein Webportal zum Austausch von Nachrichten und Dateien. Die folgende Liste nennt die betroffenen E-Mail-Domains und die jeweilige technische Alternative:
…