



Deutsche Telekom AG, Friedrich-Ebert-Allee 140, 53113 Bonn

Der Bundesbeauftragte für den Datenschutz  
und die Informationsfreiheit  
Postfach 1468

53004 Bonn

[REDACTED] | Law & Integrity – Tribe Group Privacy | Chapter Privacy Tech & Digital

**25. April 2024 | 24-193 II#1721 | Datenschutz in der Telekommunikation**

Sehr geehrter [REDACTED]

vielen Dank für Ihre ergänzende Anfrage vom 29.02.2024 zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail (Transportverschlüsselung) und die von Ihnen gewährte Fristverlängerung.

In Ihrem Schreiben haben Sie uns als Risikoszenario einen „Man in the Middle“ (MitM) Angriff geschildert und uns gebeten zu beschreiben, wie wir als Anbieter des E-Maildienstes das Risiko einer Verletzung der Vertraulichkeit oder Integrität beim Mailempfang bewerten und welche Schutzmaßnahmen hiergegen vorgesehen sind, wie z.B. MTA-STS (IETF RFC 8461), die Signierung der verwendeten TLS-Zertifikate durch eine anerkannte PKI-Zertifizierungsstelle (Certificate Authority) oder die Überprüfung unbekannter auf die Domain „t-online.de“ ausgestellter Zertifikate (Certificate Transparency).

Zu Ihren Fragen haben wir die zuständigen Fachseiten und die Kollegen der Security erneut in die Erörterung involviert.

Wir nutzen auf allen Kanälen TLS als Transportverschlüsselung. Dies wird auf den verschiedenen Protokollen durch unterschiedliche Workflows gewährleistet. Unsere Server unterstützen im Regelfall TLS 1.3. Sofern die Programme unserer Kunden kein TLS 1.3 unterstützen, wird zwischen den Servern TLS 1.2 ausgehandelt. Eine unverschlüsselte Datenübertragung wird von unseren Mailservern nicht akzeptiert.

Im Zusammenhang mit „E-Mail made in Germany (EmiG)“ haben wir uns dazu verpflichtet Zertifikate einer deutschen Zertifizierungsstelle bzw. Certificate Authority (CA) zu verwenden.

Die Teilnehmer von „E-Mail made in Germany“ überprüfen generell die Zertifikate der anderen Parteien. Eine solche Überprüfung ist auch außerhalb von EmiG möglich, hierfür ist allerdings der absendende Mailserver verantwortlich.

Die Zertifikate, die unsere Mailserver präsentieren, sind von der Telekom Security GmbH. Damit verwenden wir Root-Zertifikate bzw. Wurzelzertifikate, welche einer deutschen Root CA zuzuordnen sind und sich im Besitz der Telekom Security befinden.

Sofern ein Nutzer sich nicht nur auf die Transportverschlüsselung verlassen, sondern auch den Inhalt seiner E-Mail verschlüsseln möchte, unterstützen wir als Telekom jegliche Art einer externen Inhaltsverschlüsselung, wie z.B. PGP, ohne Einschränkungen.

Mit den oben genannten Maßnahmen erfüllen wir mit unserem E-Maildiensten „@t-online.de“ und „@magenta.de“ schon jetzt die Anforderung zum „Recht auf Verschlüsselung“, die augenblicklich im Rahmen eines Referentenentwurfes zur Änderung des TTDSG diskutiert wird.

Da DANE und DNSsec zwischenzeitlich von anderen Anbietern angeboten werden, die mit uns EmiG eingeführt haben, sind wir auch zu diesem Punkt nochmals in die Diskussion mit den zuständigen Fachseiten gegangen. Aus den Rückmeldungen ergeht, dass DNSsec und damit auch DANE nicht einfach auf den Domains „t-online.de“ und „magenta.de“ eingeführt werden kann. Der Grund liegt darin, dass DNSsec und DANE immer nur für die gesamte Domain eingeführt werden kann und dass die o.g. Domains für unterschiedliche Dienste genutzt werden, so z.B. für das Onlineportal [REDACTED]. Hier unterscheiden wir uns zu anderen Anbietern von E-Maildiensten.

Fazit:

Aufgrund der oben beschriebenen technischen Maßnahmen und insbesondere, weil wir schon heute eine individuelle Inhaltsverschlüsselung unterstützen, kommen wir zur Bewertung, dass sich unsere Kunden bei der Nutzung unseres E-Maildienstes, angemessen vor einem „Man in the Middle Angriff“ schützen können. Diese Auffassung wird auch dadurch unterstützt, dass wir damit die Anforderungen des Referentenentwurfes zur Änderung des TTDSG erfüllen.

Wir hoffen, Ihre Anfrage damit beantwortet zu haben. Sollten Sie aber noch Fragen haben, so stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

Im Auftrag

[REDACTED]

Datenschutzberater, Group Privacy