Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Deutsche Telekom AG
Group Headquarters
Group Privacy - Strategy & Steering -
[redacted]
Friedrich-Ebert-Allee 140
53113 Bonn

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL Referat24@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 29.02.2024
GESCHÄFTSZ. 24-193-2 II#1721

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Datenschutz in der Telekommunikation, Az. 24-193-2 II#1721**

Sehr geehrtes Telekom-Datenschutzteam,

viele Dank für die Rückmeldung vom 14.11.2023 in oben bezeichneter Angelegenheit. In der Sache geht es um die Frage, ob der DANE-Standard beim Empfang von E-Mails auf T-Online.de aktuell verpflichtend einzusetzen ist.

Sie hatten hierzu geantwortet, dass stattdessen „E-Mail made in Germany“ (EmiG) zum Einsatz kommt. Unabhängig von der Frage, ob EmiG einen vergleichbaren Schutz wie DANE bietet muss hier auch betrachtet werden, wie mit eingehenden E-Mails von Anbietern außerhalb Deutschlands umzugehen ist.

Hintergrund ist der Schutz der Vertraulichkeit beim Empfang von E-Mails. Ist eine Authentifizierung des T-Online-Empfangsservers für den sendenden Server nicht möglich, so besteht das Risiko, dass in dortige Mailkonten zuzustellende E-Mails abgefangen werden, worin eine Verletzung der Vertraulichkeit der Nachrichten läge. Dies kann durch einen MitM-Angriff, beispielsweise mittels BGP-Hijacking oder DNS-Spoofing, geschehen.

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Um das Problem zu verdeutlichen hier ein typisiertes Risikoszenario:

1. Sender A möchte eine E-Mail mit personenbezogenen Inhalten an die Mailadresse eines T-Online-Kunden B senden. Hierzu versucht der Server von A eine TLS-Verbindung zum Server von B aufzubauen.

2. Angreifer T befindet sich bereits im Netzwerkverkehr zwischen A und B. Er gibt dem Server von A vor, der Server von B zu sein und präsentiert zum Verbindungsaufbau ein eigenes Zertifikat.

3. Dem Server von A ist es nicht möglich das präsentierte Zertifikat auf seine Legitimität zu überprüfen. Ohne Möglichkeit zur Zertifikatsprüfung muss er daher den Verbindungsaufbau mit jedem Zertifikat akzeptieren, wenn er die E-Mail zustellen möchte.

4. Die Mail von A wird an T zugestellt, worin eine Verletzung der Vertraulichkeit und das Potenzial zu einer Manipulation der Integrität läge.

Eine ausführlichere Darstellung der Risiken ist in IETF RFC 7672, Abschnitt 1.3 zu finden.

Ich bitte Sie daher zu erläutern, wie der Verantwortliche das Risikoszenario einer Verletzung der Vertraulichkeit oder Integrität beim Mailempfang bewertet und welche Schutzmaßnahmen hiergegen vorgesehen sind, 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).

Ich bitte dazu um Rückmeldung bis zum 29.03.2024.

Mit freundlichen Grüßen
Im Auftrag

[redacted]