Vodafone GmbH, 40543 Düsseldorf RxD

Der Bundesbeauftragte für den Datenschutz und
die Informationsfreiheit
z.H. [redacted]
Graurheindorfer Straße 153

53117 Bonn

Ihr Zeichen: 24-193 II#6195
Ihre Nachricht vom 29.02.2024
E-Mail: [redacted]
Datum: 26.03.2024

per E-Mail: poststelle@bfdi.bund.de

Stellungnahme zur Eingabe von [redacted] vom 4. Oktober 2023

Sehr geehrte[redacted],

in vorbezeichneter Angelegenheit nehmen wir Bezug auf Ihre Rückfrage vom 29. Februar 2024 und dem darin geschilderten Angriffsszenario eines „Man-in-the-Middle“ Angriffs.

Nach Rücksprache mit der zuständigen Fachabteilung geben wir hierzu die folgende Stellungnahme ab:

Wir können bestätigen, dass das von dem Petenten unter Bezugnahme auf IETF RFC 7672, Abschnitt 1.3, dargelegte Risikoszenario technisch möglich ist. Wie bereits im Rahmen unserer Stellungnahme vom 27. Dezember 2023 bezüglich der Eingabe des Petenten zu Aktenzeichen 24-193 II#6079 dargelegt, ist jedoch eine praktische Durchführbarkeit eines „Man-in-the-Middle“ Angriffs als absoluter Ausnahmefall anzusehen. Unter Nr. 2. des durch den Petenten angeführten Risikoszenarios wird einleitend festgestellt: „Angreifer T befindet sich bereits im Netzwerkverkehr zwischen A und B.“ Dabei wird verkannt, dass das Eindringen eines Angreifers in den Netzwerkverkehr zwischen A und B das zentrale technische Problem für die Täter eines „Man-in-the-Middle“ Angriffs darstellt.

Im Rahmen der zitierten Stellungnahme zu Aktenzeichen 24-193 II#6079 wurde hierzu dargelegt, dass der „Man-in-the-Middle“ Angriff ein hochkomplexes und besonders aufwändiges Szenario darstellt. Grund hierfür ist, dass ein solcher Angriff im Regelfall die Zusammenarbeit mit einem Mittäter voraussetzt, der Administratorrechte besitzt und aus dem versendenden Unternehmen heraus, hier dem Vodafone Konzern, handelt. Ein reiner „Man-in-the-Middle“ Angriff von außen ist auch nicht auszuschließen. Jedoch setzt dieser außergewöhnliche technische Fähigkeiten sowie ein Höchstmaß an Aufwand und krimineller Energie voraus. Zur Erreichung des gewünschten Ziels gäbe es technisch deutlich weniger aufwändige Möglichkeiten. Insofern ist dieses Szenario auch unplausibel.

Eine ähnliche Bewertung ergibt sich für die im letzten Absatz der Eingabe vorgeschlagene Überprüfung unbekannter, auf die Domain vodafonemail.de ausgestellter Zertifikate (Certificate Transparency). Dieser Ansatz verkennt, dass das missbräuchliche Ausstellen eines Zertifikates für eine Domain unseres Konzernes einen hochgradig aufwändigen und sehr hohe krimineller Energie erfordernden Vorgang darstellt.

Trotz der obigen Bewertungen können wir mitteilen, dass die im letzten Absatz der Eingabe vorgeschlagene Schutzmaßnahme der Signierung der verwendeten TLS-Zertifikate durch eine anerkannte PKI-Zertifizierungsstelle (Certificate Authority) angewandt wird. In diesem Zusammenspiel aus Schutzmaßnahmen und Risikobewertung kommt unser Unternehmen zu dem Ergebnis, ein hohes und damit ausreichendes Schutzniveau für den Emailverkehr sicherzustellen.

Wir hoffen mit den unseren Ausführungen die in der Eingabe aufgeworfenen Fragen hinreichend beantwortet zu haben und stehen für Ihre Rückfragen gerne zur Verfügung.

Mit freundlichen Grüßen

[redacted]
Rechtsanwalt