

USA: Neue FCC-Regeln bei Bruch der Datensicherheit und Meldepflicht

Dr. Axel Spies ist Rechtsanwalt in der Kanzlei Morgan Lewis & Bockius in Washington DC und Mitherausgeber der MMR.

Die Federal Communications Commission (FCC) hat am 6.1.2023 eine Notice of Proposed Rulemaking ([NPRM](#)) veröffentlicht. Die FCC will ihre bestehenden Vorschriften ändern, nach denen TK-Unternehmen verpflichtet sind, Kunden und Strafverfolgungsbehörden auf Bundesebene über einen Bruch der Datensicherheit von Kundendaten (CPNI) zu informieren. Diese Regeln sind auch für europäische Unternehmen mit Kunden in den USA von Belang. Das Verfahren wird Ende März 2023 abgeschlossen.

1. Ausweitung des Begriffs „Bruch der Datensicherheit“ (Datenpanne)

Das Verfahren betrifft sog. customer proprietary network information (CPNI) – zB die Uhrzeit, das Datum, die Dauer und die Zielnummer eines jeden Anrufs, die Art des Netzes, das der Verbraucher abonniert hat, und alle anderen Informationen, die auf der Telefonrechnung des Teilnehmers erscheinen. Ein Bruch der Datensicherheit von CPNI muss u.a. bei der FCC angezeigt werden (vgl. in Deutschland § 169 TKG).

Die FCC möchte ihre Definition des Begriffs „Bruch der Datensicherheit“ erweitern, um den versehentlichen Zugang, die Verwendung oder die Offenlegung von Kundendaten mit einzuschließen. Nach geltender Rechtslage definiert die FCC den Begriff enger („... wenn eine Person ohne Genehmigung oder über die Genehmigung hinaus vorsätzlich Zugang zu CPNI erlangt, diese verwendet oder offengelegt hat“). Die FCC meint, dass die unbeabsichtigte Offenlegung von Kundendaten zum Missbrauch sensibler Daten führen kann und dass die Feststellung, ob eine Verletzung tatsächlich vorsätzlich passiert ist, rechtlich zu unscharf ist. Die FCC hofft, dass die Meldepflicht für versehentliche Datenschutzverletzungen die Betreiber dazu veranlassen wird, strengere Datensicherheitspraktiken einzuführen, und der FCC helfen wird, systemische Netzschwachstellen zu erkennen und zu beseitigen.

Darüber hinaus bittet die FCC um Stellungnahme zu der Frage, ob auf eine Benachrichtigung der Kunden oder der Strafverfolgungsbehörden in den Fällen verzichtet werden soll, in denen ein TK-Unternehmen vernünftigerweise feststellen kann, dass den Kunden infolge der Verletzung kein Schaden entsteht. Nach den derzeitigen Vorschriften der FCC muss kein Schaden entstanden sein, sondern die Benachrichtigung ist in jedem Fall einer Verletzung von CPNI erforderlich. Die FCC bittet auch um Stellungnahmen dazu, wie die betroffenen Anbieter und die FCC die Wahrscheinlichkeit eines Missbrauchs oder Schadens durch verletzte CPNI bestimmen sollten.

2. Meldung „sobald wie praktisch möglich“ statt „sieben Werktage“

Die zurzeit geltende Meldefrist beträgt sieben Werktage. Die FCC schlägt vor, ihre derzeitigen Vorschriften zu überarbeiten und nicht mehr vorzuschreiben, dass CPNI-Verletzungen „sobald wie praktisch möglich“ („as soon as practicable“) nach der Feststellung einer Verletzung oder in Übereinstimmung mit anderen vorgeschlagenen Zeitrahmen (vgl. § 169 Abs. 1 TKG – „unverzüglich“) gemeldet werden müssen. Die betroffenen Anbieter würden derartige Verletzungen wie bisher der FCC, dem Secret Service und dem FBI melden müssen. Die FCC schlägt zur Präzisierung vor, von den betroffenen Anbietern zu verlangen, dass sie die FCC und andere Strafverfolgungsbehörden innerhalb von 24 oder 72 Stunden benachrichtigen, wobei der Zeitrahmen nach der Schwere des Verstoßes gestaffelt ist. Darüber hinaus bittet die FCC um

Stellungnahme zu der Frage, ob es angemessen ist, einen Mindestschwellenwert für die Anzahl der betroffenen Kunden festzulegen, ab dem eine Meldung an die FCC, den Secret Service und das FBI erforderlich ist, im Gegensatz zu der derzeitigen Regelung, wonach die Strafverfolgungsbehörden über alle meldepflichtigen Vorfälle informiert werden müssen. Die FCC will dazu ein zentrales Portal für die Meldung von Verstößen an die FCC und andere Bundesbehörden einrichten und unterhalten.

3. Frühere Benachrichtigung der Kunden

Die derzeitige Regelung verbietet es den betroffenen Anbietern, ihre Kunden zu benachrichtigen oder die Verletzung öffentlich bekannt zu geben, bis mindestens sieben Werktage nach der Benachrichtigung des Secret Service und des FBI vergangen sind. Die FCC schlägt vor, die obligatorische Wartezeit vor der Benachrichtigung der Kunden abzuschaffen und stattdessen von den Betreibern zu verlangen, dass sie ihre Kunden „ohne unangemessene Verzögerung nach der Entdeckung eines Verstoßes benachrichtigen, es sei denn, die Strafverfolgungsbehörden verlangen etwas anderes“.

Weitere Vorschläge der FCC betreffen die Mindestanforderungen an den Inhalt von Mitteilungen über den Bruch der Datensicherheit. Fazit: Die neuen Regeln werden in den USA bei der FCC zu ähnlichen Mechanismen führen, wie sie in § 169 TKG vorgesehen sind.