



Pablo Bünger, Fachanwalt SAV Strafrecht, Zürich

Zur Verwertung von Sky ECC in der Schweiz: J'accuse ...!

Die Verwertbarkeit der Daten aus dem Server-Hack in Frankreich wird unter Juristen intensiv diskutiert. Wegen bekannt gewordener neuer Details ist deren Verwertbarkeit in der Schweiz zu verneinen.

Sky ECC war eine exklusive App auf einem speziell aufgesetzten Telefon, die es erlaubte, untereinander mit einer «End to End»-Verschlüsselung zu kommunizieren, ohne dass Geheimdienste und Strafverfolgungsbehörden in der Lage waren, mitzulesen. Unter anderem entdeckte auch die organisierte Kriminalität diese Technologie für sich.

Im Februar 2021 gelang es den französischen Behörden, den in Frankreich stehenden Server zu knacken. Von Frankreich aus wurden die gewonnenen Datensätze an die jeweiligen zuständigen Strafbehörden anderer Länder unaufgefordert rechtshilfeweise weitergegeben. Diese leiteten Strafverfahren gegen Nutzer von Sky ECC in ihrem Hoheitsgebiet ein.

Zu Beginn wurden die Akten zum Ablauf über den «Sky-ECC-Hack» von den französischen Behörden unter Verschluss gehalten. Mittlerweile sind sie teilweise freigegeben, wodurch eine eingehende gerichtliche Kontrolle des Vorgehens erst jetzt möglich ist.

Die Kommunikation zwischen den Sky-ECC-Nutzern erfolgte mit einer 512-Bit-Verschlüsselung. So war die Kommunikation, auch als sie über den Server in Frankreich lief, verschlüsselt. Um eine solche Verschlüsselung zu knacken, hätte man mit dem im Juni 2022 weltweit leistungsfähigsten Supercomputer «Frontier» mehrere Milliarden Jahre gebraucht. In der Folge griffen die französischen Behörden die Handys der Sky-ECC-Nutzer mit einer

Man-in-the-Middle-Attacke an. Dabei wurde einem Sky-ECC-Handy, sobald es sich jeweils beim Server angemeldet hatte, eine speziell entwickelte Push-Nachricht gesendet. Diese Push-Nachricht war für das Empfängerhandy unsichtbar und hatte den einzigen Zweck, das Handy dazu zu bringen, die für die Entschlüsselung der empfangenen Nachrichten notwendigen Verschlüsselungselemente freizugeben.

Die Einschleusung der Push-Nachricht erfolgte auf Handys, die sich auf Schweizer Territorium befanden. Allerdings besteht keine staatsvertragliche Grundlage, wonach französische Behörden verdeckte Ermittlungshandlungen auf Schweizer

Hoheitsgebiet durchführen können. Die Schweizer Behörden hätten somit über diesen Zugriff informiert werden müssen und das Vorgehen nach Artikel 269ter und Artikel 274 Strafprozessordnung durch ein Gericht bewilligen lassen müssen. Dies ist jedoch nicht geschehen. Infolgedessen wurden die Daten von Frankreich aus in Verletzung des Territorialitätsprinzips der Schweiz beschafft. Das Bundesgericht sieht in solchen Fällen ein absolutes Beweisverwertungsverbot im Sinne von Artikel 277 Absatz 2 und Artikel 141 Absatz 1 Strafprozessordnung vor (BGer 6B_1353/2023 vom 6. November 2024, E. 4.4.3).

Und was lernt man daraus: Wenn französische Behörden bei der Akteneinsicht knausrig sind, muss man in Anlehnung an die Dreyfus-Affäre im Jahr 1884 besonders skeptisch sein. Dort gab es ein Geheimdossier. Hätte die Verteidigung davon gewusst, hätte sie den Freispruch umsetzen können. ■