IWW INSTITUT
INFORMATIONSDIENSTE

DIREKTZUGRIFF AUF ELEKTRONISCHE BEWEISMITTEL BEIM PROVIDER

Zugriff auf Cloud-Daten im Ausland? Die Reichweite des § 110 Abs. 3 StPO

von Diana Nadeborn, Strafverteidigerin, Berlin,
IT-Strafrecht Blog: www.iww.de/s2188

Ohne Zustimmung des Betroffenen können deutsche Ermittlungsbehörden nicht auf Grundlage des § 110 Abs. 3 StPO auf zugangsgeschützte Cloud-Daten im Ausland zugreifen. Am 17.4.18 stellte die EU-Kommission jedoch ihre Vorschläge für zwei neue Instrumente zur Strafverfolgung vor. Mit der Abkehr vom Territorialitätsprinzip sollen die Ermittlungsbehörden zukünftig auf das Kriterium des Speicherorts der Daten verzichten können.

1. Speicherort von Daten beim Cloud-Computing

Viele Unternehmen speichern ihre Daten auf Servern, die sie nicht selbst verwalten, sondern nutzen dafür Cloud-Dienste. Datenspeicherplätze werden beispielsweise von Amazon Drive, Apple iCloud, Google Drive und Microsoft SkyDrive angeboten. Der Cloud-Nutzer mietet die Speicherkapazität und hat einen Verfügungswillen hinsichtlich der Daten, der Cloud-Anbieter hat die faktische Verfügungsgewalt über die Datenträger, auf denen sich die Daten befinden. Damit sind Cloud-Nutzer und Cloud-Anbieter Mitgewahrsamsinhaber an den Daten.

Amazon ist weltweiter Marktführer und verantwortet 34 Prozent aller genutzten Cloud-Dienste. WikiLeaks veröffentlichte am 11.10.18 Amazon-Dokumente aus dem Jahr 2015, wonach Amazon über 100 Rechenzentren in 15 Städten bzw. 9 Ländern leitet. Google unterhält ebenfalls in verschiedenen Ländern Rechenzentren. Die großen US-Diensteanbieter verfolgen eine fundamental unterschiedliche Speicherpolitik (Burchard, ZIS 2018, 190, 200; www.iww.de/s2216). Beim Anbieter Google werden die Daten eines Nutzers je nach Auslastung des Netzwerks auf verschiedene Rechner in verschiedene Länder aufgeteilt und erst bei Abruf durch den Nutzer automatisch, basierend auf Algorithmen, zusammengeführt. Beim Anbieter Microsoft kann der Cloud-Nutzer entscheiden, wo seine Daten lokal gespeichert werden. Soweit der Cloud-Anbieter die Daten des Cloud-Nutzers auf verschiedene Server verteilt und selbst den physikalischen Speicherort nicht lokalisieren kann, stehen die Ermittlungsbehörden vor denselben Schwierigkeiten.

2. Online-Sichtung gemäß § 110 Abs. 3 StPO

Während einer Durchsuchung dürfen Ermittler gemäß § 110 Abs. 3 StPO auf Daten Zugriff nehmen, die von dem durchsuchten Computer aus über ein Netzwerk zugänglich sind, sich aber auf einem räumlich getrennten Speichermedium – z. B. eines Cloud-Anbieters – befinden. Ergibt die Durchsicht, dass die extern gespeicherten Daten für die Untersuchung von Bedeutung sind, dürfen diese gesichert, also auf einen Datenträger der Ermittlungsbehörde kopiert werden.

Maßnahmeadressat ist zunächst der Cloud-Nutzer. Wird der Datenbestand des Cloud-Nutzers beim Cloud-Anbieter durch Einloggen in die entsprechenden Dateien ermittelt, handelt es sich um eine Durchsuchung bzw. Durch-

sicht beim Cloud-Nutzer gemäß § 110 Abs. 3 StPO. Betroffen ist aber auch der Cloud-Anbieter, der ebenfalls Zugriff auf die Daten hat. Dieser muss Kenntnis von der Maßnahme erlangen. Dem Inhaber des externen Speichermediums ist gemäß § 33 Abs. 3 StPO vor der Maßnahme Kenntnis zu verschaffen. Unterbleibt die Mitteilung, so verliert die Durchsicht ihm gegenüber den Charakter als offene Maßnahme und wird zu einem unzulässigen heimlichen Zugriff (Obenhaus, NJW 2010, 651, 653). Der Inhaber des externen Speichermediums muss außerdem gemäß § 110 Abs. 3 S. 2 i. V. m. § 98 Abs. 2 StPO innerhalb von drei Werktagen nach der Maßnahme Kenntnis erhalten. Erteilt der Inhaber die Bestätigung nicht, sind die Daten zu löschen (Wohlers/Jäger in: SK-StPO, 5. Aufl. 2016, § 110 Rn. 9).

3. Zugriff auf Cloud-Daten im Ausland

Der Zugriff auf zugangsgeschützte Daten, die im Ausland gespeichert sind, darf gemäß Art. 32b der Cybercrime Convention nur mit Zustimmung des Gewahrsamsinhabers erfolgen. Ohne dessen Zustimmung kann der Zugriff auf die Daten nur im Wege der Rechtshilfe erfolgen. § 110 Abs. 3 StPO ist keine Rechtsgrundlage für einen grenzüberschreitenden Datenzugriff ohne Kenntnis und Zustimmung des Betroffenen. Denn nationale strafprozessuale Befugnisse erstrecken sich immer nur auf den Hoheitsbereich des eigenen Staates. Das Verbot der eigenmächtigen Beweiserhebung im Ausland folgt aus dem Territorialprinzip, nach dem die Hoheitsgewalt eines Staates an seinen Grenzen endet (Gless JR 2008, 317, 322).

Allerdings folgt aus einer Territorialverletzung kein Beweisverwertungsverbot zugunsten des Beschuldigten, da sein Rechtskreis nicht betroffen ist:

> „Aus dem Völkerrecht ergibt sich für den Beschuldigten ein Beweisverwertungsverbot hier auch nicht als Reflexwirkung aus der Verletzung von Interessen eines anderen Staates. Vielmehr ist anerkannt, dass der einzelne, der von einer völkerrechtswidrigen Maßnahme betroffen ist (insbesondere von der Verletzung eines völkerrechtlichen Vertrags, der ihm keine Rechte als Individuum gewährt), sich in einem anschließenden gegen ihn gerichteten inländischen Strafverfahren wegen einer im Inland begangenen Straftat grundsätzlich nicht auf die vom Gewahrsamsstaat verübte Völkerrechtswidrigkeit berufen kann, um daraus strafprozessuale Vorteile für sich herzuleiten.“ (BGH 30.4.90, 3 StB 8/90, BGHSt 37, 30, www.iww.de/s2217).

4. Unbekannter Speicherort

Teilweise wird vertreten, die Online-Sichtung gemäß § 110 Abs. 3 StPO sei zulässig, wenn unklar ist, ob und in welchem ausländischen Staat sich der Server befindet (Hegmann in: Graf, StPO, 3. Aufl. 2018, § 110 Rn. 15; Wohlers/Jäger in: SK-StPO, 5. Aufl. 2016, § 110 Rn. 9b), weil der zufällige Auslandsstandort eine willkürliche Missachtung der ausländischen Souveränität ausschließe (Wicker MMR 2013, 765, 769; Wohlers/Jäger in: SK-StPO, 5. Aufl. 2016, § 102 Rn. 15a).

Auch der Bundesrat meint in seiner Stellungnahme zum Vorschlag über Europäische Herausgabe- und Sicherungsanordnungen vom 6.7.18:

> „Gemäß § 110 Abs. 3 der Strafprozessordnung ist nach deutschem Recht derzeit ein Zugriff auf extern inländisch gespeicherte Daten zulässig. Soweit rein tatsächlich auf im Ausland gespeicherte Daten zugegriffen wird, ist hinsichtlich der gewonnenen Beweismittel solange kein Beweisverwertungsverbot anzunehmen, als bei der Erhebung der Daten der (ausländische) Speicherort der Daten nicht bekannt war.“ (BR-Drs. 215/18, www.iww.de/s2218).

Der Rückgriff auf einen angeblich unbekannten Speicherort verbietet sich aber schon mit Blick auf die Mitteilungspflichten gemäß § 33 Abs. 3 StPO und § 110 Abs. 3 S. 2 i. V. m. § 98 Abs. 2 StPO (s. o.). Bei großen Cloud-Anbietern, bei denen allgemein bekannt ist, dass deren Rechenzentren im Ausland belegen sind, drängt sich die Exterritorialität auf (Brodowski/Eisenmenger, ZD 2014, 119, 123). Die Ermittlungsbehörden sind daher verpflichtet, den Inhaber des Servers zu ermitteln. Auskunftsverlangen können sie zunächst an den inländischen Standort des ausländischen Cloud-Anbieters richten. Dieser Vorgang ist in der Ermittlungsakte zu dokumentieren.

5. Fazit

Ohne Zustimmung des Betroffenen können deutsche Ermittlungsbehörden nicht auf Grundlage des § 110 Abs. 3 StPO auf zugangsgeschützte Cloud-Daten im Ausland zugreifen. Am 17.4.18 stellte die EU-Kommission jedoch ihre Vorschläge für zwei neue Instrumente zur Strafverfolgung vor (COM(2018) 225 final). Der Vorschlag sieht zusammengefasst vor, dass Strafverfolgungsbehörden Unternehmen, die elektronische Kommunikationsdienstleistungen in anderen Mitgliedstaaten anbieten (Diensteanbieter), unabhängig vom Speicherort der Daten (sogenanntes Marktortprinzip) sanktionsbewährt direkt dazu verpflichten können, Daten für das Strafverfahren zu sichern (Europäische Sicherungsanordnung) und an die anfragende Strafverfolgungsbehörde herauszugeben (Europäische Herausgabeanordnung) (vgl. Nadeborn, Einführung der Europäischen Sicherungs- und Herausgabeanordnung [e-evidence]). Mit der Abkehr vom Territorialitätsprinzip sollen die Ermittlungsbehörden zukünftig auf das Kriterium des Speicherorts der Daten verzichten können.