



Bundeskriminalamt

POSTANSCHRIFT Bundeskriminalamt • 65173 Wiesbaden

Per E-Mail

Bundesministerium des Innern

Arbeitsgruppe ÖS I 3

Alt-Moabit 101 D

10559 Berlin

HAUSANSCHRIFT Thadenstraße 11, 65183 Wiesbaden

POSTANSCHRIFT 65173 Wiesbaden

TEL +49(0)611 55- [REDACTED]

FAX +49(0)611 55- [REDACTED]

ERARBEITET VON [REDACTED]

EMAIL [REDACTED]

AZ SO AS 207 -

DATUM 24.03.10

BETREFF **Fallbeispiel für die Vorratsdatenspeicherung**
hier: [REDACTED]

BEZUG Erlass ÖS I 3 vom 23.03.10

ANLAGEN

Zu den durch [REDACTED] erbetenen Fallbeispielen zur Vorratsdatenspeicherung, insbesondere im Hinblick auf den bei der fraktionsoffenen Sitzung geschilderten Missbrauchsfall, berichtet das Bundeskriminalamt wie folgt:

I. Bekämpfung der Kinderpornografie sowie des sexuellen Missbrauchs von Kindern

Grundsätzlich ist es regelmäßig im Rahmen der Identifizierung von Tätern und Opfern im Bereich der Bekämpfung von Kinderpornografie sowie des sexuellen Missbrauchs von Kindern erforderlich, auf der Grundlage richterlicher Beschlüsse gemäß § 100g StPO bei den Providern Verkehrsdaten nach § 113a Telekommunikationsgesetz (TKG) sowie auf Basis von (polizeilichen) Auskunftersuchen nach § 113 TKG Bestandsdaten zu E-Mail-Adressen und IP-Adressen zu erheben.

BKA

ZUSTELL- UND URSERANSCHRIFT: BKA, Thadenstraße 11, 65183 Wiesbaden

Überschreibungsempfänger: Bundeskassette Team

Briefverbindung: Deutsche Bundesbank
Filiale Saarbrücken (Bek Saarbrücken)
BLZ 530 000 00 Kto-Nr. 150 000 20

Seit der Entscheidung des BVerfG zur Vorratsdatenspeicherung konnten in einer Vielzahl der Fälle des sexuellen Missbrauchs von Kindern bzw. der Verbreitung von Kinderpornografie, in denen lediglich eine IP-Adresse als Identifizierungsansatz bekannt ist, die jeweiligen Tatverdächtigen nicht identifiziert werden.

Beispiel a)

Im Rahmen des aktuell bearbeiteten Falles, der im Rahmen der fraktionsoffenen Sitzung am 17.03.10 geschildert wurde, erhielt das Bundeskriminalamt zuerst auf dem Interpol-Weg, im Weiteren ergänzend in direkten bilateralen Kontakten einen Hinweis, wonach auf Grund von verdeckten Recherchen im Internet eine IP-Adresse eines deutschen Providers festgestellt wurde, über die kinderpornografisches Material angeboten und verbreitet wurde. Darüber hinaus gab der Nutzer der IP-Adresse im Internet an, Zugang zu zwei Kleinkindern zu haben, die er regelmäßig missbrauche. Der Inhaber der mitgeteilten IP-Adresse konnte zunächst nicht identifiziert werden, da die Verkehrsdaten, über die der Kunde an Hand der zugehörigen Bestandsdaten hätte ermittelt werden können, durch den zuständigen deutschen Provider nicht gespeichert wurden. Zur Identifizierung des Tatverdächtigen war es daher erforderlich, dass die Kundendaten zur tatrelevanten IP-Adresse beim Provider angefragt werden, während die IP-Adresse an den Tatverdächtigen vergeben ist, d. h. der Tatverdächtige muss zum Zeitpunkt der Anfrage an den Provider weiterhin im Internet aktiv („online“) sein. Das hierzu notwendige Vorgehen wurde mit dem polizeilichen Kooperationspartner im Ausland abgestimmt und führte letztlich (unter erheblichem Mehraufwand, u. a. Einrichtung einer Rufbereitschaft des hiesigen Fachreferates) zur Identifizierung des Tatverdächtigen.

Mit der Vorratsdatenspeicherung hätte der Tatverdächtige bereits bei Eingang der Information durch den mitteilenden Staat zweifelsfrei und mit wesentlich geringerem Aufwand identifiziert und damit der Hinweis auf einen (aktuell andauernden) Missbrauchsfall schneller bearbeitet werden können. Wäre es dem ausländischen polizeilichen Kooperationspartner nicht mehr gelungen, den Tatverdächtigen bei weiteren Aktivitäten im Internet festzustellen, hätte dieser auf Basis der vorhandenen Daten nicht ermittelt werden können.

Beispiel b)

In einem weiteren Sachverhalt der Bekämpfung von Kinderpornografie sowie des sexuellen Missbrauchs von Kindern ermittelt das Bundeskriminalamt gegen eine Gruppierung, die stark abgeschottete und hierarchisch strukturierte Internetforen und korrespondierende Internet-chats betrieben hat. Über diese virtuellen Plattformen tauschten deren Mitglieder millionenfach – teilweise durch eigenen sexuellen Missbrauch selbst produzierte – kinderpornografische Dateien (Bilder, Videos, Geschichten). Die Mitglieder kommunizierten darüber hinaus über ihre pädosexuellen Neigungen und Erfahrungen – auch über eigene vorgenommene Missbrauchshandlungen –, Anonymisierungs- und Verschlüsselungstechniken sowie polizeiliche Ermittlungsmethoden.

Die Gruppierung umfasste etwa 500 Mitglieder, von denen 145 – überwiegend in Deutschland – identifiziert werden konnten. Die neun Haupttäter wurden am 29.09.2009 aufgrund von Haftbefehlen in Deutschland festgenommen. Zeitgleich wurden im Rahmen einer bundesweiten und internationalen polizeilichen Aktion gegen die anderen identifizierten Mitglieder Durchsuchungsbeschlüsse vollstreckt und zahlreiche Beweismittel sichergestellt.

Aufgrund der Ermittlungen wurden laufende sexuelle Missbrauchstaten zum Nachteil von Kindern beendet. Zu etwa einem Drittel der identifizierten Mitglieder liegen Hinweise auf sexuellen Missbrauch von Kindern vor. Ein Teil der Missbraucher ist zwischenzeitlich zu hohen Haftstrafen verurteilt bzw. sitzt in Untersuchungshaft.

Die Ermittlungen belegen, dass der bekannt gewordene „Tätertypus“ sich nicht nur auf den massenhaften Austausch von kinderpornografischen Dateien spezialisiert und beschränkt, sondern weit über Einzelfälle hinaus schwere Sexualstraftaten zum Nachteil von Kindern begeht.

Ohne die Vorratsdatenspeicherung wäre nur ein Bruchteil der Tatverdächtigen identifiziert worden.

Da sich ein Verfahrenskomplex im Stadium des Zwischenverfahrens befindet, andere Teilkomplexe nach wie vor Gegenstand von Ermittlungen sind, ist eine dezidiertere Darstellung für die Diskussion im politischen Raum nicht möglich.

II. Sonstige Kriminalitätsfelder

Neben den explizit erbetenen Fallbeispielen aus dem Bereich der Bekämpfung von Kinderpornografie sowie des sexuellen Missbrauchs von Kindern werden folgend weitere Fallbeispiele aus anderen Kriminalitätsfeldern dargestellt, die auch mit Bericht des Bundeskriminalamtes vom 24.03.10 an das BMI (Argumentationspapier) übermittelt wurden:

1. Kategorie: Anschlussinhaberdaten zur IP-Adresse

Die Problematik der IP als ersten und einzigen Ermittlungsansatz ist im **IuK-Bereich besonders offenkundig**, die Unerlässlichkeit ist aber z. B. auch im Bereich **Kinderpornografie** erkennbar, ebenso in Gefahrenabwehrfällen (Bsp.: **Amok- oder Suizidankündigung**).

Mit dem Konsens, dass es keine rechtsfreien Räume geben kann, muss der Konsens einhergehen, dass es auch keine verfolgungsfreien Räume geben kann. Strafverfolgung und Gefahrenabwehr müssen daher zur Durchsetzung materiellen Rechts wirksam sein. **Der Zugriff auf bei Diensteanbietern gespeicherte Daten ist für diese Zwecke wirksam und unverzichtbar.** Ohne Zugriff auf diese Daten wären nach hiesiger Schätzung etwa in ca. 80 % der 38.000 Fälle (PKS) allein im Bereich der **IuK-Kriminalität im engeren Sinne - die für 2008 polizeilich registriert wurden - keine Ermittlungsansätze vorhanden gewesen**, denn in diesem Kriminalitätsfeld agieren die Täter fast ausschließlich in elektronischen Netzen und hinterlassen dementsprechend auch nur dort -elektronische- Spuren. Angesichts der Steigerungsraten des Deliktsfeldes von über 100 % seit 2002 ein nicht hinnehmbares Ergebnis¹.

¹ 2002: 17.700 Fälle; 2008: 37.900 Fälle

Die Fallzahlen zur luK-Kriminalität im engeren Sinne gliedern sich dabei wie folgt auf:

- Computerbetrug, strafbar gem. § 263a StGB (17.006 Straftaten in 2008)
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (5.244 Straftaten in 2008)
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung, strafbar gem. §§ 269, 270 StGB (5.716 Straftaten in 2008)
- Datenveränderung, Computersabotage, strafbar gem. §§ 303a, 303b StGB (2.207 Straftaten in 2008)
- Ausspähen von Daten, strafbar gem. §§ 202a, 202b, 202c StGB (7.727 Straftaten in 2008)

In den folgenden Beispielen aus dem Bereich der luK-Delikte stellen festgestellte IP-Adressen jeweils die ersten Ansatzpunkte für weitere Ermittlungsschritte dar. Weitere durch die Täter genutzte Infrastrukturen (Anonymisierungsservices etc.) erschweren in vielen Fällen die Täterermittlung über die genutzte IP-Adresse.

Beispiel für ein Verfahren in dem sowohl die Delikte Computerbetrug, Datenveränderung, Computersabotage als auch das Ausspähen von Daten festgestellt wurden

In einem Großverfahren des Bundeskriminalamtes, in welchem die IP-Adressen zur Identifizierung der Beschuldigten genutzt wurden, waren o. g. Deliktsbereiche Gegenstand der Ermittlungen. Ziel des Verfahrens war die Aufhellung eines deutschsprachigen Underground-Forums, in welchem insbesondere Straftaten mit Bezug zu

- a) DDoS-Attacken (Distributed Denial of Service-Attacke: Datenveränderung, Computersabotage),
- b) Malware (Datenveränderung, Ausspähen von Daten) sowie
- c) Missbräuchlichem Einsatz von Kreditkartendaten im Internet (Ausspähen von Daten/Computerbetrug)

verabredet wurden.

Hierbei konnten insbesondere über die Überwachung einer Webseite Zuordnungen zwischen relevanten Usern (in Bezug auf Straftaten) und den genutzten IP-Adressen getroffen werden. Ohne die Vorratsdatenspeicherung wären nach Einschätzung der Ermittlungsführung ca. 80 % der Hauptbeschuldigten nicht identifiziert worden.

Beispiel Computerbetrug (Carding)

Durch die Täter werden über den missbräuchlichen Einsatz von Kreditkartendaten hochwertige Elektronikartikel bei einem Webshop gekauft. Durch den Webshop erfolgt eine Speicherung der IP-Adresse zum Kauf des Artikels. Diese IP-Adresse wird der Polizei im Rahmen des Ermittlungsverfahrens mitgeteilt. Über eine Zuordnung der IP-Adresse zum Inhaber können somit erste Anhaltspunkte zur Ermittlung des Bestellers der Ware und damit zum Täter erlangt werden.

Beispiel der Datenveränderung/Computersabotage (DDoS-Attacke)

Über eine Distributed Denial of Services-Attacke durch ein Botnetz wird eine Webseite im Internet attackiert. Diese ist daraufhin im Internet nicht mehr erreichbar. Über die Auswertung der Logdaten der angegriffenen Seite kann ein Command&Control-Server identifiziert werden, der das Botnetz, das zum Angriff genutzt wurde, steuerte. Über eine Auswertung des Command&Control-Servers können täterseitige administrative Zugriffe auf diesen festgestellt werden. Die hierbei genutzten IP-Adressen können erste Anhaltspunkte zur Identifizierung der Täter liefern.

Beispiel Datenveränderung/Ausspähen von Daten (Verteilung von Schadsoftware)

Über eine Webseite wird Schadsoftware verteilt. Diese dient primär dem Ausspähen von Daten. Über eine Auswertung der Webseite kann festgestellt werden, durch welche täterseitigen IP-Adressen die Schadsoftware auf dem Server der Webseite platziert wurde. Somit könnten erste Anhaltspunkte für eine Identifizierung von Tätern erlangt werden.

Beispiel Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung, strafbar gem. §§ 269, 270 StGB

Durch einen beliebigen Nutzer (Täter) werden bekannte Daten einer anderen Person, wie

- a) Rechnungsadresse und
- b) Name, Vorname

dazu genutzt, sich bei kostenpflichtigen Internetdiensten anzumelden. Hierbei kann eine Identifizierung des Täters nur über die beim Internetdienst mitgeloggten IP-Adressen erfolgen. Ohne eine Zuordnung der Bestandsdaten zur entsprechenden IP-Adresse seitens der Access-Provider können somit keine Anhaltspunkte zur Identifizierung der Täter erfolgen.

Beispiel: Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

Hierzu gehört das Einloggen bei Internet-Providern mit fremden oder gefälschten Zugangsdaten, aber auch das unbefugte Entsperren von sog. „SIM-Locks“ bei Mobiltelefonen sowie Zugangerschleichungen zu Telefonanschlüssen mit illegalem Anwählen von mit hohen Kosten verbundenen 900er-Nummern.

Gerade bei der Zugangerschleichung zu Telefonanschlüssen/Telefonanlagen kann hierbei unter Umständen eine Auswertung von Logdaten der entsprechenden Anlage erfolgen, um so den täterseitigen Zugriff festzustellen. Die hierbei festzustellenden IP-Adressen geben erste Hinweise, die zur Identifizierung des Täters führen könnten. Ohne ein entsprechendes Vorhalten der Daten ist dies von vornherein ausgeschlossen.

Die Problematik der Identifizierung von IP-Adressinhabern betrifft nicht nur den Bereich Cybercrime (InK-Kriminalität), sondern in der Zwischenzeit auch viele weitere Deliktsbereiche der Allgemeinkriminalität.

Dies verdeutlichen die folgenden Beispiele:

Beispiel Erpressung

In einem Fall aus dem Jahr 2009 wurde ein namhafter deutscher Autohersteller über den Versand von E-Mails erpresst. Die E-Mails wurden über eine E-Mailadresse beim Provider "Google" verschickt. Nach dem Erlass eines Beschlusses gem. § 100g StPO

mit dem Adressaten Google wurden von dort die IP-Adressen der Zugriffe auf das täterseitig genutzte E-Mail-Account mitgeteilt. Über die IP-Adressen konnten weitere Anhaltspunkte bezüglich des Beschuldigten erlangt werden.

Beispiel Betrugstaten

- Der Täter eröffnete mit mindestens 7 falschen Personalausweisen 11 Konten bei 6 verschiedenen Banken und wickelte darüber in 1.700 Fällen betrügerische Finanztransaktionen ab. Den einzigen Ermittlungsansatz stellten die Anschlussinhaberdaten hinter den dynamischen IP-Adressen dar, die allerdings mangels Mindestspeicherungspflicht nicht mehr vorhanden waren.
- Hackingangriffe auf den Zentralrechner des Pentagon führten vermutlich zur Veränderung bzw. Ausspähung sensibler Daten. Die Angriffe erfolgten mit einer deutschen IP-Adresse. Das Rechtshilfeersuchen der US- Behörden führte nicht zur möglichen Erhebung von Verbindungsdaten, da beim Provider keine Speicherung erfolgt war. Der Verursacher des Hackingangriffs konnte nicht ermittelt werden.

Beispiel Amoklauf

Durch einen User wurde in einem Onlinespiel eine Nachricht geposted, wonach der User angab am folgenden Tag in Deutschland einen Amoklauf in München durchführen zu wollen. Über US-amerikanische Behörden wurden IP-Adressdaten mitgeteilt, die gerade einmal wenige Stunden alt waren.

Durch den Provider wurde jedoch mitgeteilt, dass die Daten zu der IP-Adresse bereits gelöscht wurden.

Eine Identifizierung des Users konnte dann nur noch über Bestandsdaten zu einer E-Mailadresse erfolgen, die glücklicherweise mit Klardaten angelegt wurde. Ohne diese Daten wäre eine Identifizierung nicht möglich gewesen.

Beispiel Suizidankündigung

Wie bedeutsam die Zuordnung einer IP-Adresse etwa in Fällen von Suizidankündigungen ist, kann aktuell mit einem tragischen, in den Medien bereits bekannt gewor-

denen Fall, in dem ein 18-jähriger Mann aus dem Münsterland in einem Internetforum seinen Suizid angekündigt hatte, belegt werden. Die Telekom verweigerte hier die Auskunft über die bekannt gewordene IP-Adresse, da dort keine unmittelbare Gefahr für Leib und Leben gesehen worden war. Da der Mann nicht identifiziert worden war, konnte er später nur tot aufgefunden werden. Die zuständige StA führt derzeit ein Ermittlungsverfahren gegen Telekommitarbeiter wegen des Verdachts der unterlassenen Hilfeleistung.

2. Kategorie: Verkehrsdatenerhebung i. Z. m. Telefonie

Beispiel: Bombendrohungsfälle

- Eine **Klinik** wird anonym per Telefon mit einer Bombendrohung konfrontiert. Nach dem zweiten Anruf wurde die Klinik mit erheblichem Aufwand geräumt. Mehrere schwere Tumoroperationen mussten abgesagt werden. Kosten in Höhe von 90.000 EUR entstanden. Mit Hilfe der noch am Tag erwirkten Beschlüsse gemäß § 100g StPO konnten die Anschlüsse, von denen die Drohanrufe erfolgten, und die Täterin ermittelt werden.
- Im Zuge einer telefonischen Bombendrohung gegen die Ulmer Justiz musste das Justizhochhaus abgesperrt werden. Tausende Bürger und Mitarbeiter wären betroffen. Es wurde ein Zielsuchlauf zur Ermittlung des zur Tatzeit bei der Telefonzentrale eingehenden Anrufes durchgeführt. Die Ermittlungen ruhen zurzeit aufgrund der vom Bundesverfassungsgericht erlassenen einstweiligen Anordnung.

Beispiel: Wettbetrugsfall

Der aktuelle Wettskandal im Profifußball mit Tatverdächtigen bzw. Tatorten in etwa 20 vorwiegend europäischen Staaten und illegalen Wettgewinnen in Höhe von mehreren Millionen Euro konnte durch ca. 50 Beschlüsse gemäß § 100 g StPO aufgeklärt werden. Für die Aufklärung von Strukturen der organisierten Begehungsweise ist das sog. „**Quick-Freeze-Verfahren**“ keine geeignete Alternative. Bei Taten, die länger

zurück liegen, fehlen die bereits gelöschten Verkehrsdaten. Tatplanungszeiträume, insbesondere bei organisierten Tätergruppierungen, betragen in der Regel deutlich mehr als drei Monate. Nur durch retrograden Zugriff auf Verkehrsdaten kann die Vorbereitungs- und Tatplanungsphase aufgestellt werden.

Dies hat sich auch beim **Meliani-Verfahren** (versuchter Anschlag auf den Straßburger Weihnachtsmarkt 2000) gezeigt: Das Netzwerk der Gruppe konnte nicht weiter aufgeklärt werden, da die Verbindungs- bzw. Verkehrsdaten nach 3 Monaten gelöscht waren.

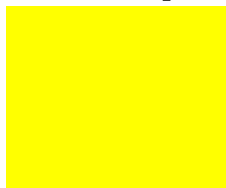
3. Kategorie: Funkzellenabfrage/Standortdaten

Beispiel: Ausspähen von Zahlungskarten

Für den Zeitraum 2007 bis 2008 konnten im Zusammenhang mit dem Ausspähen von Zahlungskartendaten durch retrograd erhobene Funkzellendaten entscheidende Ermittlungsansätze gewonnen werden. Im Ergebnis waren die von der Täterseite genutzten Mobiltelefone zu tatkritischen Zeiten an verschiedenen Tatorten in der Nähe von Banken eingebucht.

Es gelang mittels dieser Daten die Identifizierung einer Vielzahl von Beschuldigten - sowohl in Deutschland als auch im Ausland - mit einer Zuordnung von insgesamt 37 Straftaten.

Im Auftrag



[gez. 24.03.10]

[gez. 24.03.10]