25. Deutscher EDV-Gerichtstag

Neue Ermittlungsinstrumente bei der Bekämpfung von Cybercrime

- Erweiterung der gesetzlichen Handlungsoptionen

22.09.2016, 15:00-17:00 Uhr

Moderation: **Dieter Kesper**, Oberstaatsanwalt; Staatsanwaltschaft Köln

Referenten: **Dr. iur. Dominik Brodowski, LL.M. (UPenn)**, wissenschaftlicher Mitarbeiter am Lehrstuhl Prof. Dr. Christoph Burchard, Goethe Universität Frankfurt am Main

Markus Hartmann, Oberstaatsanwalt; Staatsanwaltschaft Köln

Carsten Rosengarten, Oberstaatsanwalt; Generalstaatsanwaltschaft Celle

Protokoll: Marie-Luies Rubel, LL.M., wissenschaftliche Mitarbeiterin am Lehrstuhl Prof. Dr. Georg Borges, Universität des Saarlandes

Der Moderator **Dieter Kesper** begrüßt die Referenten und die Teilnehmer. Herr Kesper stellt sich selbst vor. Er führt aus, dass alles mit einem sog. Hacker-Camp im Jahre 2012 begann. Das Interesse an diesem Thema ist so gestiegen, dass nun bereits zum fünften Mal über dieses Themengebiet referiert wird. Was vor einem Jahr beim Workshop zu Cybercrime ausgeführt wurde, soll heute fortgeführt werden.

In den Medien wurde bereits viel berichtet über Angriffe auf Computersysteme, etwa der Angriff auf ein Krankenhaus oder der Amoklauf in München, bei welchem der Täter eine Waffe aus dem sog. Darknet benutzte.

Dieses Jahr wird der Workshop noch mehr in die Tiefe gehen in Bezug auf tatsächliche und rechtliche Fragen. Stichworte wie NSA, Bundestrojaner, etc. um nur einige Beispiele zu nennen.

Herr Kesper stellt seine Gäste vor: Herrn Rosengarten, Oberstaatsanwalt in der Generalstaatsanwaltschaft Celle, welcher ins Thema einführen soll; dann Herrn Dr. Brodowski, wissenschaftlicher Mitarbeiter am Lehrstuhl von Prof. Dr. Christoph Burchard an der Goethe Universität Frankfurt. Er wird die Stellschrauben, die dem Gesetzgeber gegeben werden, beleuchten. Zuletzt Herr Hartmann,

Leiter der Cybercrime Abteilung und Oberstaatsanwalt in der Staatsanwaltschaft Köln. Er wird einige Fallgestaltungen betrachten und abschließende Fragen erörtern.

Herr Kesper freut sich auf drei interessante Themen. Er führt aus, dass zwar Zwischenfragen erlaubt sind, die Diskussion jedoch am Schluss stattfinden wird.

Herr Rosengarten übernimmt das Mikrofon und begrüßt seinerseits die Teilnehmer. Er möchte nicht näher auf politische Diskussionen eingehen, sondern stellt die Bekämpfung von Schwerstkriminalität im Internet in den Blickwinkel. Denn dort sind am ehesten Unzulänglichkeiten im Ermittlungsinstrumentarium zu erkennen.

Er zeigt auf der Folie die Visualisierung des Datenverkehrs eines Netzknotens. Netzwerkkommunikation ist wie ein Schaltplan: die Kommunikation verläuft nie nur in einer Richtung. Hier sieht man zugleich ein Problem beim Auffinden und Verfolgen von strafrechtlichen Strömen. Es ist wie die Verfolgung von Wassertropfen in einem Fluss – man hat eine unendliche Zahl an Angriffspunkten. Dies stellt die Ermittler vor allem vor technische Herausforderungen.

Jeder kennt das sog. Eisbergbild – es gibt nicht nur das klassische WWW, dessen Eisbergspitze aus dem Wasser ragt, sondern auch noch eine Vielzahl anderer krimineller Plattformen (Pedoplanet, Darknet usw.). Deshalb muss man das Internet differenziert betrachten. Eine Unterteilung von legalen Diensten, welche ebenfalls von Kriminellen genutzt werden, und illegalen bzw. ausschließlich kriminellen Zwecken dienenden Diensten, ist notwendig.

Mit den zur Verfügung stehenden Mitteln ist es äußerst schwierig, gerade die illegalen Dienste zu verfolgen. Allerdings würde eine leichtere Zugänglichkeit zu Missbräuchen führen.

Als Gegenpole kennen wir das Dreieck von Grundrechten, diese müssen immer abgeprüft werden, bevor man eingreifen kann. Das erste ist das Recht auf informationelle Selbstbestimmung mit den bekannten von der Rechtsprechung festgelegten Begrenzungen. Das zweite Problem ist das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Hierbei stellt sich eine Gewichtungsfrage: inwieweit sollen Zugriffe erlaubt sein, ohne das Grundrecht auszuhöhlen. Das BVerfG hat verschiedene Richtungen eingeschlagen. Das dritte Grundrecht, welches es zu beachten gilt, ist Art. 10 GG – der Schutz der Fernkommunikation, welcher sich auch auf die IT-Kommunikation

bezieht. Dieser wirft vor allem bei verdeckten Ermittlern im Internet Probleme auf.

Wir müssen uns die Frage stellen, was wir haben wollen, welche Zugriffsrechte sollen zur Aufklärung von Straftaten den Ermittlern zur Verfügung stehen? Dabei muss man vier Arten unterscheiden: die Nutzungsdaten, deren Eingriffsgrundlagen in den §§ 161, 163 StPO iVm § 15 TMG liegen. Den Verkehrsdaten (§ 100g StPO), den Bestandsdaten (§§ 161, 163 StPO iVm § 14 TMG und 100j StPO) sowie die Inhaltsdaten mit Eingriffsgrundlage aus § 100a StPO.

Den Ermittlern begegnen dabei nicht nur alltägliche Begriffe, die Sprache der Cyberkriminalität entwickelt sich ständig weiter. Begriffe wie Geolokalisation, IP-Daten, Log-Daten oder Zeitstempel tauchen vermehr auf, gerade weil die Täter anonym im Netz sind. Die Identifizierung des Täters ist vorrangig, erst danach setzt die „klassische“ Täterverfolgung an. Bei diesem „Vorschritt“ fallen Unmengen an Daten an. Probleme ergeben sich zwangsläufig in Bezug auf Datenschutz, Verschlüsselung, Grundrechtsrelevante Eingriffe und Anonymisierungsdienste.

Herr Rosenberg führt aus, dass sie nur mit mittelbaren Daten arbeiten können (Log- und IP-Daten), um überhaupt erstmal zu identifizieren. Bei diesem Schritt entstehen noch keine Inhaltsdaten. Eine Dekryptierung dieser Daten ist jedoch utopisch in diesem Bereich, da zeitlich nicht zu bewältigen.

Ein weiteres Problem gerade im Bereich DDoS-Angriffe und Ransomware ist, dass wir es häufig nicht mit Einzeltätern oder Banden zu tun haben, sondern sich eine ganze Wirtschaft entwickelt hat, die dauerhaft gegen Geld eine Infrastruktur zur Verfügung stellt. Dazu kommt, dass die Angriffe quasi live sind. Es dauert mitunter Jahre und schafft Unmengen von Daten, um sich durch einzelne Serverschichten hochzuarbeiten, um die einzelnen Panels zu identifizieren und dann eine konkrete Person dahinter zu finden. Die tägliche Arbeit besteht dabei daraus, Verbindungen zu überprüfen und Datenquellen auszuwerten.

Den Ermittlern drängt sich zudem die Frage auf, wenn eine Lokalisierung geschafft wurde, wie vorzugehen ist. Entweder fährt ein Einsatzkommando hin und schaltet den Server ab (so sieht der Alltag bisher aus) oder ob man bereit ist, einen neuen Weg zu gehen, indem man direkt auf den Server zugreift. Bei letzterem stellt sich die Abwägungsfrage, wo die Grenze sein soll – man will einerseits den Grundrechtsschutz wahren (und die Verhältnismäßigkeit), andererseits Ermittlungserfolge erzielen, welche man mitunter nur erreichen kann, wenn man die Systeme infiltriert. Diese Frage wird uns wohl noch Jahre beschäftigen. Zum Abschluss zeigt Herr Rosenberg den BVerfG-Beschluss vom 14.09.1998 (BvR 1062/87).

Damit übergibt er an **Herrn Dr. Brodowski**, welcher sich bedankt und die Teilnehmer begrüßt. Er führt aus, dass es einer Erweiterung bzw. Konkretisierung des Themas bedarf: Was sind die wesentlichen Regelungen und Leitfragen? Was bedeutet dies für die Praxis? Was für Regelungsmodelle bieten sich dem Gesetzgeber an? Was für Handlungsbedarf folgt daraus?

Die §§ 100 j ff. StPO sind unübersichtlich genug – wir brauchen ein Mehr an Ermittlungsverfahren, aber ein organisatorisches Weniger. Dabei zeigt Herr Dr. Brodowski das Bild einer Fahrbahn: er führt aus, dass wir Rahmenvorgaben bräuchten, die man nicht überfahren sollte ähnlich wie die Fahrbahnstreifen auf einer Autobahn. Die andere Frage ist eher politisch und lässt sich nicht allein rechtlich beantworten.

Wenn man wie gewohnt die formelle und materielle Vereinbarkeit prüft, herrscht keine Streitigkeit, dass ein Grundrechts-Eingriff vorliegt. Aus Sicht des Verfassungsrechts und der Verfassungsrechtsprechung, welche sich stark in diesem Bereich entwickelt hat (exemplarisch: Kernbereich privater Lebensgestaltung), muss man alle Stellschrauben berücksichtigen.

Wenn man dies heute diskutiert, gibt es keine binäre Antwort, es gibt eine Vielzahl von Variationen, die man diskutieren sollte.

Herr Brodowski hat 12 zentrale Leitfragen entwickelt. Aus Zeitgründen kann er jedoch nicht auf alle 12 Leitfragen eingehen. Die ersten beiden Fragen (das Ob und das Wie der Maßnahme) sind zunächst politischer Natur. Die konkrete Ausgestaltung muss der Verhältnismäßigkeit entsprechen. Die Verfassung selbst enthält kaum Maßnahmen. Herbert Landau hat dies zwar immer wieder hervorgehoben (und dies hat sich in der Rechtsprechung des zweiten Senats widergespiegelt), dennoch existiert ein Spannungsfeld.

Als Beispiel: Welche Daten will man abgreifen und auf welchen Weg soll der Bundestrojaner auf ein System aufgespielt werden? Wie detailliert?

Nach Meinung von Herrn Dr. Brodowski muss das Parlament dies regeln (Wesentlichkeitstheorie). Untermauert wird dies durch die zweite verfassungsrechtliche Vorgabe: normenklare Formulierung (bereichsspezifisch). Der Bürger braucht die Gewissheit, dass er nicht eingeschränkt wird. Problem ist dabei das „hinreichend bestimmte“ Gesetz. Was heißt das?

Auf dem 69. Juristentag in München ging Herr Armin Nack noch weiter und fordert die StPO in diesem Bereich radikal auszudünnen und auf drei General-

klauseln zu beschränken (Unterscheidung von Kommunikationsinhalten und –umständen).

Problem ist, dass die Rechtsprechung viel zu selten mit diesen Themen konfrontiert wird. Es besteht ein ständiger Nachbesserungsbedarf zu diesen diffizilen Abgrenzungsfragen. Zum Beispiel stellt sich die Frage, ob es zulässig ist, dass man ein Zielsystem so beeinflusst, dass es einen unsicheren Schlüssel verwendet. Bisheriger Rechtsstand dazu: nur dann, wenn es unersetzlich ist, ist es zulässig. Als die §§ 100 a und b StPO im Jahre 1960 erschaffen wurde, war noch nicht die Rede von solchen Problemen. Daher sollte eine umfassende Strafrechtsreform gemacht werden, insbesondere eine technikneutrale, um der Normenklarheit zu genügen.

Dauerbrenner ist ebenfalls das Quellen-TKÜ (Quellen-Telekommunikationsüberwachung) bezüglich des Zugriffs auf verschlüsselte Daten insbesondere auf Smartphones. Hierbei stellt sich die Frage, in welchem Umfang die deutschen Behörden darauf zugreifen dürfen, insbesondere wenn die Server (Datenspeicher) im Ausland stehen, insb. bei US-Anbietern.

Eine weitere Frage, die sich Ermittlern stellt, ist, ob sich ein Polizeibeamter als private Person in sozialen Netzen ausgeben darf oder ob Data Mining zur Strafverfolgung zur Verfügung steht.

Herr Dr. Brodowski wirft die Frage in den Raum, wie man mit der Operationalisierung des Ermittlungsverfahrens umgehen soll, d.h. Kriminalität nicht nur allein in der Vergangenheit, sondern in der Zukunft (Grenze zur Gefahrenabwehr verschwimmt). Dies ist eine gesellschaftliche, politische und rechtliche Fragestellung!

Er empfiehlt: Schaffung eines § 100x StPO, der beantworten soll, ob der Zugriff auf die Täter-IT notwendig, sinnvoll und angemessen ist; ob dies technisch möglich ist und unter welchen sachlichen Voraussetzungen. Denn nur eine verfassungskonforme und verhältnismäßige Eingriffsgrundlage kann einen solchen weitreichenden Eingriff deckeln. Die §§ 100c bis e StPO sind so wie sie jetzt sind noch keine mögliche Eingriffsgrundlage, man müsste diese verschärfen, damit diese verfassungskonform sind, allerdings sind sie dann wohl kaum mehr anwendbar, da die Straftat aktuell vom System ausgehen muss.

Der Moderator übergibt an **Herrn Hartmann**, welcher ebenfalls die Teilnehmer begrüßt. Dabei sagt er, dass er nicht allen Antworten seiner Vorredner zustimmen kann. Sodann gibt er keinen Überblick über seine Dienststelle: ZAC NRW.

Er leitet die zentrale Ansprechstelle für ganz NRW für herausragende Cybercrime-Angriffe. Er sagt, die ZAC ist ähnlich wie eine Quick Reaction Force (QRF) – schnell und rund um die Uhr (24/7) erreichbar. Dabei setzt sich die ZAC aus drei Aufgabenfeldern zusammen: die Ermittlung in herausragenden Verfahren, die Beantwortung von Grundsatzfragen und die Aus- und Fortbildung mit Kontakt zur Wissenschaft.

Ein brisantes Beispiel war das Krankenhaus in Neuss: durch Ransomware wurden wesentliche Teile der Krankenhausakten verschlüsselt, über eine Woche lang konnte das Krankenhaus keine Operationen und Behandlungen führen, was gerade bei Langzeittherapien, wie z.B. die Krebsbehandlung, schwere oder sogar lebensbedrohliche Folgen haben kann. Bei diesem Angriff war es so, dass wir (die ZAC) wissen, wo der Server steht, von dem die Ransomware verschickt wurde. Wir wissen auch, wer kommuniziert. Fakt ist aber, dass wir keine Eingriffsbefugnis haben, um aktiv dagegen vorzugehen, also um aktiv die Software zu kompromittieren.

Die StPO stammt aus einer Zeit, wo es noch Telegraphen gab. Der historische Gesetzgeber hat die Beschlagnahme von Telegraphen-Dokumenten erlaubt. Die Frage ist, ob sich das fortspielen auf die heutige Diskussion lohnt.

In den USA gibt es eine aktive Diskussion über den Umgang mit verschlüsselten Daten, wir kennen aus den Medien die Auseinandersetzungen zwischen FBI und Apple (Muss Apple das iPhone entschlüsseln, um dem FBI Zugriff auf den verschlüsselten Datenspeicher zu ermöglichen).

Ein großes Problem stellt das Darknet als krimineller Umschlagplatz für kriminelle Güter (Waffen bequem online bestellen). Uns (der ZAC) gelingt es, die Täter zu individualisieren und zu identifizieren. Problem ist aber, dass die IT-Geräte, auf die man zugreifen muss, verschlüsselt sind. Theoretisch müsste man also die Polizei losschicken, bevor der Täter es schafft, das Gerät zu verschlüsseln – dies ist in der Realität kaum möglich (Verschlüsselung oft in wenigen Sekunden möglich).

Für diese Problematik (der Verschlüsselung von IT-Geräten) gibt es zwei Modelle: Modell 1 – man lässt Hintertüren bei der Implementierung bereits von Anfang an ins Programm einbauen für die Strafverfolgungsbehörden, dies ist aber ein ungünstiger Weg, da die Angreifer diese Hintertüren ebenfalls nutzen können. Modell 2 – die Benutzung von Verschlüsselung ist erlaubt, aber im Einzelfall (mit Richtervorbehalt) soll die Dechiffrierung in der Dienststelle erlaubt sein („licence to hack“ für die Ermittlungsbehörden). Dafür muss die Dienststelle aber mit notwendigen Mitteln ausgestattet werden.

Ein Fallbeispiel dazu (realer Fall): ein Anbieter einer Kinderpornoseite stellt online TV zur Verfügung. Dort sieht man (live) ein Kind in einem Käfig. Der Besteller kann nun, gegen vorherige Bezahlung, auswählen, welche Art von Missbrauch an dem Kind durchgeführt werden soll. Das ganze wird dann live gestreamt.

Den Ermittlungsbehörden gelingt es, mit den IT-technischem Mitteln, eine Lokalisierung durchzuführen. Die Behörde sieht dann: Pseudonym A bestellt Missbrauch XYZ. Aber wir sehen nicht: Wie wird bezahlt, wann startet der Stream, da diese Daten verschlüsselt sind. Wenn die Behörde das sehen will, müsste sie die IT kompromittieren, in etwa durch Quellen-TKÜ. Worauf kann sich aber ein solcher Eingriff stützen? Laut dem Gutachten der GBA reicht § 100a StPO nicht als Ermächtigungsgrundlage. Laut BMI darf das Quellen-TKÜ repressiv angewendet werden. Wir müssen also auf Beendigung des Streams warten. Das BMI führt weiterhin aus, dass die Aussage vom GBA nicht verbindlich ist und der einzelne Richter im Einzelfall entscheiden muss.

Herr Hartmann geht kurz auf die Entscheidung des 1. Senats vom 20.04.2016 ein (1 BvR 966/09 und 1 BvR 1140/09) und sagt, dass der Bundestag dazu berufen ist, dies zu klären.

Ein anderes Thema ist, wenn die Behörden einen Täter festnehmen und dessen Smartphone mittels Fingerabdruck verschlüsselt ist. Darf die Behörde den Fingerabdruck verwenden, den sie bei der erkennungsdienstlichen Maßnahme genommen hat, um das Smartphone zu entsperren oder darf sie sogar polizeiliche Gewalt anwenden und den Finger auf das Handy zum Entsperren drücken? Dies muss der Gesetzgeber beantworten!

Herr Hartmann führt weiterhin aus, so wünschenswert eine generelle Überarbeitung der StPO wäre, würde er eine schnellere Methode vorziehen. Er endet mit den Worten: wir brauchen einen § 100x StPO so schnell wie möglich!

Der Moderator bedankte sich bei den Referenten und wünschte den Teilnehmern einen schönen Rest-EDV-Gerichtstag und eine gute Heimreise.