Strafverfolgung im Internet - juristische, technische und praktische Herausforderungen

Zeit: Donnerstag, 24.09.2015, 15.00 Uhr

Ort: Hörsaal 0.19

Moderation: DIETER KESPER, Oberstaatsanwalt; Staatsanwaltschaft Köln

Referenten: EVA BARTHOLOMY, Oberstaatsanwältin; Staatsanwaltschaft Köln

MARKUS HARTMANN, Staatsanwalt; Staatsanwaltschaft Köln

ANDREAS BRÜCK, Staatsanwalt; Staatsanwaltschaft Köln

Die „ZAC“ (Zentralstelle und Ansprechpartner Cybercrime) ist eine vor knapp zwei Jahren gegründete Abteilung der Staatsanwaltschaft Köln. Bereits im Herbst 2013 erkannte das Justizministerium des Landes Nordrhein-Westfalen, dass eine effektive Strafverfolgung bei Online-Kriminalität besondere rechtliche und technische Kompetenzen erfordert. Es verfügte die Einrichtung einer Zentralstelle im Zuständigkeitsbereich der Generalstaatsanwaltschaft Köln, wo entsprechende Kompetenzen bereits vorhanden waren. Die neue Abteilung nahm am 15.01.2014 ihre Arbeit auf; mittlerweile werden dort vier Dezernenten eingesetzt.

Zu ihren Aufgaben gehört außer der Verfahrensführung in herausgehobenen Ermittlungsverfahren (etwa Angriffe auf kritische Infrastrukturen - beispielsweise Krankenhäuser oder Energieversorger - oder die organisierte, grenzüberschreitende Kriminalität) im Bereich Cybercrime auch, als Ansprechpartner für Grundsatzfragen zu fungieren und im Bereich der Aus- und Fortbildung tätig zu sein.

Um neue Ermittlungsansätze und wissenschaftliche Erkenntnisse in diesem Bereich rechtlich und technisch umsetzen zu können, ist die Zusammenarbeit mit Institutionen sowohl der öffentlichen Hand (z. B. LKA) als auch Privaten von besonderer Bedeutung. Denn einerseits ist externer Sachverstand notwendig, etwa wenn es um den Einsatz von Ermittlungssoftware geht, andererseits müssen die so getroffenen Maßnahmen mit dem Grundgesetz und der Strafprozessordnung vereinbar sein. Technik und Recht sind insoweit verzahnt.

Für Schwierigkeiten bei der Strafverfolgung sorgt der Einsatz von Kryptographie-Tools und Anonymisierungsmöglichkeiten (etwa Jondonym, Tor). Verschleiert der Täter seine IP-Adresse, können Strafverfolger ihre Überwachungsmaßnahmen an keinem Punkt technisch ansetzen. Zur Diskussion um „Cryptowars“ wird festgestellt, dass häufig anlasslose Eingriffe in die Daten von Bürgern in der öffentlichen Diskussion stehen, obwohl die Ermittlungsbehörden auf strafprozessuale Maßnahmen für den Zugriff auf Daten erst bei bestehendem Anfangsverdacht angewiesen sind.

Eine bundesweit einmalige Besonderheit ist ein telefonischer Bereitschaftsdienst, der rund um die Uhr erreichbar ist. Dort steht ein Ansprechpartner zur Verfügung, dem zu jeder Zeit etwa Angriffe auf Infrastrukturen gemeldet werden können. Dieser kann bei Bedarf auch Rechtshilfemaßnahmen mit dem Ausland koordinieren.

Zu den Delikten, mit denen die Abteilung hauptsächlich befasst ist, zählen etwa das Ausspähen von Daten oder Computersabotage. Diese sind häufig nur „Mittel zum Zweck“, um weitere Straftaten begehen zu können, etwa (Computer)-Betrug, Fälschung beweiserheblicher Daten, Erpressung oder Verrat von Geschäfts- und Betriebsgeheimnissen gemäß § 17 UWG. Aber auch Verstöße gegen das Datenschutzrecht (§§ 43, 44 BDSG) oder die Verbreitung ehrverletzender Äußerungen oder von Kinderpornographie gehören zum Alltag der Behörde. Es wird eine Tendenz beobachtet, dass klassische „Offline-Delikte“ wie Beleidigung oder Erpressung immer häufiger über das Internet begangen werden.

Die Täter, gegen die häufig wegen mehrerer Delikte ermittelt wird, verfolgen meist finanzielle Interessen. Um die Tat möglichst kostengünstig und effektiv zu begehen, kommt es sehr oft zum Zukauf krimineller Dienstleistungen über Online-Foren (Crime-as-a-Service). Das gilt nicht nur für „angehende“ Cybercrime-Täter, denen das Wissen und die Angriffsinstrumente fehlen, zumal Straftaten durch Einzeltäter kaum vorkommen. Stattdessen arbeiten die „Banden“ arbeitsteilig, sodass sich jedes Mitglied auf seine Fähigkeiten (beispielsweise die Herstellung von Angriffswerkzeugen oder das Weiterleiten von erbeuteten Beträgen) konzentrieren kann. Teilweise wird auch gegen staatliche Akteure, soweit dann nicht die Zuständigkeit des Generalbundesanwalts gegeben ist, ermittelt.

Fallbeispiele

1) Häufig sind Geräte, die an das Internet angeschlossen sind (Internet der Dinge) das Ziel von Hacker-Angriffen. Im Jahr 2014 kam es vermehrt zu Angriffen auf Router in Privathaushalten. Über eine Schwachstelle konnte die VoIP-Funktion aktiviert und genutzt oder die Zugangsdaten ausgelesen werden. Anschließend verursachten die Täter bei mehreren tausend Betroffenen hohe Schäden durch unerlaubte Telefonate über deren Anschluss. Die ZAC arbeitete mit betroffenen Providern zusammen, es kam auch zur Überwachung von Telekommunikation und Servern. Schwierigkeiten ergaben sich einerseits aus der hohen Zahl der Geschädigten und damit zu führenden Verfahren, andererseits aus der großen Menge an Daten (ca. 400 Terabyte), die bei den Überwachungsmaßnahmen erzeugt wurden. Eine Herausforderung stellt dies aber nicht nur für die Ermittlungsbehörde, sondern auch für das Gericht, das eine Hauptverhandlung durchzuführen hat, sowie für die Verteidigung etwa bei der Akteneinsicht dar.

2) Bei „DDos deluxe“-Attacken kommt es zu massenhaften Zugriffen auf einen Server durch ein Bot-Netz (hohe Anzahl von infizierten Rechnern). Der betroffene Server ist nach dem Angriff nicht mehr erreichbar. Schon mehrfach stand diese Vorgehensweise im Zusammenhang mit Schutzgelderpressungen von Unternehmen, die auf ihre Online-Präsenz angewiesen sind. Als Beweismittel kommen Protokolldaten in Frage, aus denen sich die IP-Adressen der infizierten Rechner ergeben. Daraus kann man unter Umständen schließen, wer am Angriff beteiligt war, welche Computer oder Geräte für eine Infektion anfällig waren, etc. Bei der Datenspeicherung handelt es sich aber nach der Rechtsprechung des Bundesverfassungsgerichts um einen Grundrechtseingriff. Derzeit besteht dafür keine Rechtsgrundlage, aber es existiert ein Gesetzesentwurf der Bundesregierung zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten.

Um die Verantwortlichen feststellen zu können, ist eine schnelle Einleitung der Ermittlungen notwendig und in diesem Fall auch erfolgt: Es kam zu einer Vielzahl von DDos-Angriffen mit

Schutzgelderpressungen; täglich gingen neue Strafanzeigen von Unternehmen ein, die die Protokolldaten ihrer IT-Abteilungen zur Verfügung stellten. Bei Stichproben der infizierten Rechner konnte die Schadsoftware identifiziert und letztlich das Bot-Netz übernommen und auf einen Rechner der Staatsanwaltschaft umgeleitet werden („Behörden-Bot“). Weitere Angriffe konnten so vermieden werden. Ein Problem lag aber darin, dass es sich bei dem Abschalten eines Bot-Netzes nach seiner Übernahme nicht um Strafverfolgung, sondern Gefahrenabwehr handelt.

3) Auch Phishing-Angriffe beim Online-Banking finden nach wie vor statt: Dabei werden die Bankzugangsdaten von Kunden ausgespäht, dann erfolgt eine Überweisung aus dem Online-Banking des Kunden zu sogenannten Finanzagenten und von dort aus auf weiteres Konto. Früher gab es wenig Ermittlungsansätze. Die Finanzagenten sind häufig gutgläubig und werden unter einer Legende angeworben. Sie haben selbst keine Daten des „Hintermanns“. Es muss also untersucht werden, wer das Geld bekommen hat, wie die Finanzagenten angeworben werden und wie die Kommunikationswege sind. Dies führte die Ermittler in einem Fall zur Telefonnummer eines „Hintermanns“. Mit einer groß angelegten Telefonüberwachung wurde später die Struktur der Bande aufgedeckt.

4) Die Banden sind häufig so organisiert, dass in Deutschland unzählige Finanzagenten aktiv sind, die durch Finanzagentenführer angeleitet werden. Diese sind Regionalverantwortlichen unterstellt, welche einem Hauptkoordinator für Deutschland untergeordnet sind. Diesem wiederum übergeordnet sind Kriminelle aus dem Ausland. In einem Fall konnte ein Regionalverantwortlicher identifiziert werden. Durch eine Telefonüberwachung wurde dann bekannt, dass ein ausländischer Verantwortlicher vorhatte, anlässlich einer Hochzeit in die Bundesrepublik einzureisen. Auch dieser konnte festgenommen werden; es kam zu mehreren Verurteilungen.

5) Außerdem konnte die ZAC Erfolge gegen Foren (u. a. boerse.bz) verzeichnen, in denen ein rechtswidriger Austausch von urheberrechtlich geschützten Filmen, Musik und Software stattfand.

Nach 20 Monaten „ZAC“ zieht die Behörde eine positive Bilanz. Die Fallzahlen sind nach wie vor hoch, allerdings ist die Aufklärungsquote im Jahr 2014 gestiegen und liegt bei ca. 20%. Hilfreich für die Staatsanwälte ist die neue Meldepflicht für Unternehmen bei Angriffen nach dem IT-Sicherheitsgesetz. Das Fehlen einer Vorratsdatenspeicherung ist kein großes Defizit, stattdessen muss ein zielgerichteter und anlassbezogener Zugriff auf Daten möglich sein.

Protokoll: Dipl. jur. Alexander Gratz, Universität des Saarlandes