TAGUNGSBERICHT

Symposium Cybercrime – Herausforderungen der Ermittlungspraxis

Bericht zum Symposium am 25.10.2016 an der Hochschule der Polizei Rheinland-Pfalz

von Polizeirat Christian Kirchner *

Auf die steigende Bedeutung des Kriminalitätsbereiches Cybercrime muss innerhalb der Strafverfolgungsbehörden nicht weiter hingewiesen werden. In fast allen Ermittlungsbereichen hat das Thema Einzug gehalten. Nachdem die Hochschule der Polizei Rheinland-Pfalz (HdP) bereits 2015 ein Symposium Cybercrime mit dem Schwerpunkt Kinderpornografie durchgeführt hat, fand am 25. Oktober 2016 nun erneut eine Veranstaltung statt – dieses Mal zu den Herausforderungen für die Ermittlungspraxis. Über 220 Teilnehmer aus Polizei und Justiz von Bund und Ländern folgten der Einladung auf den Campus Hahn der HdP in den Hunsrück. In diesem Tagungsbericht werden die wesentlichen Erkenntnisse zusammengefasst.

I. Einführung

Begrüßt wurden die Teilnehmer der Veranstaltung von *Dr. Axel Henrichs*, dem Leiter der Abteilung Ausbildung an der HdP. Anhand verschiedener aktueller Vorkommnisse wie der zeitweisen Lahmlegung des Lukaskrankenhauses in Neuss mit Hilfe einer Krypto-Schadsoftware, dem Verkauf der Tatwaffe für den Amoklauf in München über das Darknet oder einer großen Anzahl von Betrugsfällen an Unternehmen mittels Social-Hacking (CEO-Fraud) wurden die steigende Bedeutung, die hohe Dynamik und die Schwierigkeit der Anpassung an das Phänomen für die Strafverfolgungsbehörden dargestellt. Zwar seien erste Schritte getan, aber sowohl das Recht als auch die Organisation würden der Entwicklung hinterherhinken.

Auch der Schirmherr der Veranstaltung, Staatssekretär im Ministerium des Innern, Herr *Günter Kern,* stellte heraus, dass zwar erste Schritte zur Anpassung der Organisation erfolgt seien, trotzdem aber weitere Anpassungen für eine wirksame Kriminalitätsbekämpfung folgen müssten.

II. Vorträge

1. Aktuelle Rechtsfragen zu IT-Ermittlungen

Im ersten Vortrag gab *Dr. Wolfgang Bär* (Richter am BGH) einen Überblick über aktuelle rechtliche Problemstellungen im materiellen und formellen Strafrecht. Anhand eines Strafverfahrens der StA Kempten zur Schadsoftware Skynet und dem Beschluss des BGH vom 21.7.2015 (BGH 1 StR 16/15 – *LG Kempten)* wurden Lücken in den aktuellen gesetzlichen Vorschriften erörtert. Hierbei hatte ein Täter Schadsoftware, welche zum Beispiel als zum Download bereitgestellte Video-Dateien getarnt war, auf mindestens 327.000 Rechnern verbreitet. Diese Schadsoftware konnte Daten mittels Keylogger abgreifen und nutzte weiterhin die Rechenleistung des Computers, um Bitcoins zu generieren (Bitcoin-mining). Die Befassung des BGHs mit dem Sachverhalt machte deutlich, dass bei Fällen des Ausspähens von Daten nach § 202a StGB dem Nachweis einer bestehenden Zugangssicherung auf den betroffenen Geräten der Geschädigten eine erhöhte Bedeutung zukommt. Dies stellt jedoch bei retrograden Ermittlungen eine besondere Herausforderung für die Strafverfolgungsbehörden dar, da oftmals gerade bei festgestelltem Befall mit Schadsoftware betroffene Systeme neu aufgesetzt werden. Ebenso seien der Verfall nach § 73 StGB hier für die durch Bitcoin-mining erlangten Werte zwar angeordnet worden, allerdings bleibe fraglich, ob diese Bitcoins unmittelbar aus der Tat heraus erlangt wurden.

Neben diesem Fall gab *Dr. Bär* auch kursorisch einen Überblick über die Strafnormen der Cybercrime im engeren Sinne. Im Ergebnis würden diese Normen zwar eine Strafbarkeit für viele Phänomene eröffnen, allerdings seien einer angemessenen Bestrafung durch fehlende Qualifikationstatbestände, beispielsweise bei bandenmäßiger oder gewerbsmäßiger Begehung, Grenzen gesetzt. Ebenso fehlten Versuchsstrafbarkeiten.

Für den Bereich des Strafverfahrensrechts stellte der Referent zunächst die Schwierigkeiten in der Abgrenzung zwischen Telemedien und Telekommunikation dar. Diese sei letztlich bedeutsam, denn sowohl für die Anbieter der Dienste als auch für die Verfolgungsbehörden greifen je nach Einordnung sehr unterschiedliche Vorschriften bei Anfragen und Datenübermittlungen. Neben verschiedenen Datenabfragen in diesen Bereichen wurde insbesondere die Neuregelung der Verkehrsdatenabfrage dargestellt. Ob diese Vorschrift, welche auf Grund von Übergangsvorschriften erst ab 1.7.2017 wirksam in Kraft tritt, tatsächlich so Bestand haben wird, hänge allerdings auch vom Ausgang verschiedener Verfahren ab, die beim BVerfG wie auch beim EuGH anhängig sind.

Zuletzt wurden kurz die Fragestellungen zur Beschlagnahme von E-Mails, zur Rechtsgrundlage der Quellen-TKÜ sowie Ermittlungen im Cloud Computing erörtert.

* Der Verfasser ist Dozent an der Hochschule der Polizei Rheinland-Pfalz.

2. Strategie – Erwartungen und Realität

Der zweite Vortrag des Tages widmete sich den Herausforderungen an die Ermittlungsbehörden in komplexen Strafverfahren. *Dr. Eric Samel* (Landeszentralstelle Cybercrime, GenStA Koblenz) und *Thorsten Runkel* (Kriminalinspektion Mayen) stellten ein Ermittlungsverfahren gegen den Programmierer und Anbieter für Schadsoftware dar. Dieser hatte neben verschiedenen Anwendungen wie Keyloggern, Exploit-Kits, DDoS-Tools auch eine Testplattform für Schadsoftware betrieben, auf welcher getestet werden konnte, ob die Anwendung von gängigen Virenscannern erkannt wird. Herr Runkel stellte zunächst dar, dass auf Grund der hohen Dynamik und Bandbreite der Delikte eine „klassische" Herangehensweise an ein Kriminalitätsphänomen nicht erfolgversprechend sei.

Es erweise sich als Vorteil, dass sowohl in der Polizei als auch in der Justiz mit der Schaffung von Zentralstellen kompetente Ansprechpartner vorhanden waren, die für die Abwicklung eines solchen Verfahrens zwingend erforderlich seien. Der Vortrag zeigte deutlich, dass vergleichbare Sachverhalte für örtliche Ermittlungsbehörden eine große Belastung darstellen, insbesondere, da eine große Menge von Daten zu sichern und auszuwerten ist. Das breite Ermittlungsspektrum und die anfallenden Daten erforderten – gerade für kleine und mittelgroße Dienststellen wie die KI Mayen – einen sehr flexiblen Personaleinsatz. Als sehr positiv beschrieb Herr Runkel die hervorragende und unkomplizierte Zusammenarbeit mit anderen Behörden und Institutionen.

Von den Rednern wurde auch dargestellt, dass das Verfahren am Ende gegen den Täter aufgrund des Tatbestandes des „Vorbereiten des Ausspähens und Abfangens von Daten" nach § 202c StGB sowie wegen Beihilfe zu Betrugsdelikten betrieben wurde. Der Täter selbst habe demnach gar nicht Angriffe auf andere Systeme durchgeführt, vielmehr habe er das Handwerkszeug für solche Taten zur Verfügung gestellt. Prägnant für die Ermittler war in diesem Zusammenhang die Feststellung, dass im Internet professionell „Crime as a Service" angeboten wurde. Das Fazit zeigte auch deutlich, dass durch diese Serviceleistungen mittlerweile keine besonderen Kenntnisse mehr benötigt werden, um Angriffe auf fremde Systeme durchführen zu können. Vielmehr könne man diese Fachkenntnisse einfach im Internet einkaufen.

3. CEO-Fraud – Soziales Hacken

Streng genommen sei das Phänomen eigentlich kein Cybercrime, stellten *Andreas Brück* und *Janina Menzel* von der Zentral- und Ansprechstelle Cybercrime der Staatsanwaltschaft Köln zu Beginn ihres Vortrages heraus. An sich sei es eine eher klassische – an den Enkeltrick angelehnte – Betrugsbegehungsweise, bei der zahlungsbevollmächtigte Mitarbeiter von Firmen durch Täuschung zur Begleichung nicht unerheblicher Rechnungen veranlasst werden. Die Begehungsweise sei hierbei immer sehr ähnlich:

Die Täter verschaffen sich zunächst ein sehr genaues Bild von dem Unternehmen. Sie kennen Zuständigkeiten, Abläufe, Struktur, die Sprachkultur und vor allem die Abwesenheit des CEO (geschäftsführender Vorstand eines Unternehmens). Dabei greifen Täter zur Vorbereitung oftmals auf offene Informationen im Internet zu. Viele Unternehmen würden sich so transparent im Internet präsentieren, dass zahlreiche der für den Betrug notwendigen Informationen frei im Netz zugänglich seien. Gleichwohl gebe es auch Indizien, dass teilweise mittels Schadsoftware auf technischem Weg Informationen abgegriffen werden.

Im weiteren Verlauf werde dann von den Tätern Kontakt zu einem Mitarbeiter im Unternehmen aufgenommen, der für den Finanzhaushalt oder für Zahlungsanweisungen zuständig ist. Dabei gäben sich die Täter als Firmenchef (CEO) aus, stellten eine wichtige Unternehmensveränderung in Aussicht und pochten dabei ausdrücklich auf Diskretion und das Einhalten bestimmter Kommunikationswege. Mittels Einbindung, Nachweisen und Kontakt zu vermeintlich externen Organisationen wie beispielsweise der BaFin oder KPMG, die ebenso von den Tätern vorgetäuscht werden, erlange der Vorgang zusätzlich Seriosität. Am Ende stehe die Aufforderung zu einer Zahlung von hohen Geldbeträgen, häufig größer als 1 Mio. Euro, welche in vielen Fällen auch gezahlt würden. Allein bei den von der StA Köln betriebenen Vorgängen sei hierdurch schon ein tatsächlicher Schaden von 39 Mio. Euro entstanden.

Die Referenten wiesen darauf hin, dass diese Taten leicht vermeidbar seien, vielfach wären die Richtlinien der Unternehmen für die IT sowie den Zahlungsverkehr sehr lasch, sodass am Ende durch Einwirkung auf eine einzelne Person dem Unternehmen erheblicher Schaden zugefügt werden könne.

III. Workshops

Innerhalb des Symposiums hatten die Teilnehmer die Möglichkeit, aus verschiedenen angebotenen Workshops zwei auszuwählen.

1. Workshop „Polizei-Hacking"

Im ersten Workshop wurden durch *Tobias Hofmann* (LKA Hessen), orientiert an den Bedürfnissen der Praxis, unterschiedliche Ermittlungs- und Recherchemöglichkeiten im Bereich von Cybercrime vorgestellt.

Ein schnell und effektiv anzuwendendes Tool, um zu überprüfen, ob beispielsweise eine Datei oder eine Webseite mit einem Virus infiziert wurde, sei VirusTotal. Dabei handelt es sich um einen vom Unternehmen Google betriebenen, kostenlosen Online-Dienst.

Als Recherchetool wurden die Nutzungsmöglichkeiten der erweiterten Suchoperatoren von beispielsweise Google – in IT-Kreisen auch gerne als Google-Hacks bezeichnet – dargestellt. Hiermit könne zielgerichtet nach Informationen im Internet gesucht werden, auch

dann, wenn die normale Suche in Google nicht erfolgversprechend war. So ist es mittels spezieller Suchfunktionen möglich, beispielsweise auch ältere oder gelöschte Informationen abzurufen.

Neben anderen Tools wurden auch die Sicherung von Webseiten mittels „WGET“ sowie die Netzwerkdiagnose mit „NMap“ als nützliche Anwendung für die Praxis dargestellt.

2. Workshop Waffen- und Drogenhandel im „Darknet“

In einem weiteren Workshop gab *Dr. Benjamin Krause* (Zentralstelle für Internetkriminalität GenSta Frankfurt) einen Überblick über das Phänomen des Waffen- und Drogenhandels im Darknet. Hierbei stellte er zunächst die Zugangsmöglichkeiten mittels TOR-Browser sowie die weitgehend anonymen Bezahl- und Versendemöglichkeiten vor.

Anhand von Fallbeispielen beschrieb *Dr. Krause*, welche Ermittlungen im Darknet möglich und welche Ermittlungsmethoden in diesem Bereich nicht zielführend seien. Im Ergebnis stelle sich dar, dass klassische technische Ermittlungen wie Bestands- und Nutzungsdatenabfrage, große Bereiche der Finanzermittlungen, Telekommunikationsüberwachung oder Serverbeschlagnahme meist nicht zum Ziel führen. Allerdings gebe es trotzdem Möglichkeiten der Ermittlung; denn auch, wenn der Informationsaustausch mittels TOR kaum zurückzuverfolgen sei, ergäben sich insbesondere durch die Kommunikation mit dem Täter Identifizierungs- und Ermittlungsmöglichkeiten.

Der Vortrag endete mit der Fallvorstellung des Amoklaufs aus München und den damit einhergehenden erfolgreichen Ermittlungen im Darknet bezüglich der dort erworbenen Tatwaffe.

3. Workshop „EG Pornplayer“

Michael Prior und *Carsten Ehlert* (PD Hannover) stellten in ihrem Vortrag das Ermittlungsverfahren „Pornplayer“ vor. Hierbei wurden Computer und Android-Smartphones mittels Schadsoftware gesperrt. Die Täter stellten die Entsperrung gegen eine Zahlung von 100,- Euro mittels PaysafeCard oder ITunes-Gutscheinen in Aussicht. Die Infizierung erfolgte durch Werbebanner. Im Rahmen der Ermittlungen stellte sich heraus, dass allein in Deutschland mindestens 5000 Personen auf die Erpressung eingegangen sind und die geforderte Summe bezahlt hatten. Dabei werde die Dunkelziffer erheblich höher eingeschätzt.

Die Referenten stellten dar, dass es im Rahmen ihrer Ermittlungen gelungen sei, die Server der Täter ausfindig zu machen und diese automatisiert zu überwachen. So konnten unter anderem PINs von PaySafe Karten gesperrt und Gelder abgeschöpft werden. Die Ermittler lobten insbesondere die hervorragende Zusammenarbeit mit PaySafeCard, die erlaube, neu festgestellte PINs zum Teil innerhalb eines Tages zu sperren.
Dadurch seien die PINs für die Täter unbrauchbar und diese kämen nicht mehr an das Geld heran. Durch den intensiven Ermittlungsdruck sei es mittlerweile gelungen zu verhindern, dass die Täter neue Server in Betrieb nehmen. Ein Umstand, der wahrscheinlich ursächlich dafür sei, dass derzeit keine neuen Anzeigen zu verzeichnen seien.

4. Workshop Cybergrooming

Andreas Pößel (LKA Rheinland-Pfalz) stellte die Initiativermittlungen zum Phänomen des Cybergrooming dar. Hierbei würden Täter auf Chat-Plattformen gezielt Kinder ansprechen, um dann im weiteren Verlauf in einem Videochat vor diesen sexuelle Handlungen vorzunehmen. Die Ermittlungsgruppe sei mit der Zielrichtung gebildet worden, weitere Erkenntnisse zu dem nicht ganz neuen Phänomen zu erhalten, Tatverdächtige zu identifizieren und Ermittlungsverfahren einzuleiten sowie Täterkreise zu verunsichern. Als Plattform wurde die Webseite knuddels.de gewählt, die Zusammenarbeit mit dem Betreiber sei hierbei unproblematisch gewesen. Mittels einer nicht offen ermittelnden Polizeibeamtin, welche sich im Chat als Kind ausgab, konnten dabei zahlreiche Täter identifiziert werden. *Herr Pößel* beschreibt dabei, dass es stellenweise kaum möglich gewesen wäre, den Anfragen potentieller Täter hinterherzukommen, da man noch im Chat mit einem anderen Täter gewesen sei.

In den folgenden Videochats sei es dann in vielen Fällen zu sexuellen Handlungen wie Masturbation der Täter gekommen. In insgesamt 27 Fällen wurden Strafanzeigen wegen §§ 176 Abs. 4 Nr. 1 und 2 i.V.m. 22, 23 StGB eingeleitet. Die Zahl der bedenklichen Chats sei zwar deutlich höher gewesen, allerdings habe man sehr genau darauf geachtet, dass die Beamtin nicht als agent provocateur aufgetreten sei.

IV. Fazit

Dr. Jörg Angerer (Leiter Landeszentralstelle Cybercrime, GenStA Koblenz) und *Johannes Kunz* (Präsident des LKA Rheinland-Pfalz) fassten zum Abschluss der Veranstaltung zusammen, dass man den verschiedenen Aspekten der Cybercrime begegnen könne. Notwendig seien innovative Ermittlungsansätze und vor allem der Mut und die Bereitschaft, auch einmal ein komplexeres Ermittlungsverfahren zu betreiben.

Beide betonten die gute Zusammenarbeit zwischen Justiz und Polizei in Rheinland-Pfalz. Als entscheidend und erfolgversprechend stuften beide die Bildung von Schwerpunktdienststellen bei Polizei und Justiz ein. Im Ergebnis sei man im Thema Cybercrime gut aufgestellt.