Internetkriminalität

Berichte aus der Anwaltspraxis

Vortrag 16. Fachtagung Arbeitskreis Drogen und Justiz
vom 17.05.2017

Rechtsanwalt Frank Palkovits, Marl

Internetkriminalität

I. Begrifflichkeiten (IuK-Kriminalität / Cybercrime)

II. Cybercrime zum Nachteil der Mandanten

III. Cybercrime durch Mandanten

I. Begrifflichkeiten

IuK-Kriminalität = Informations- und Kommunikations-Kriminalität, heute bezeichnet als Cybercrime.

Cybercrime im engeren Sinne = Straftaten, bei denen Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind (der Hacker, der in fremde Systeme eindringt, unbe-rechtigt Daten erhebt und destruktiv Daten verändert).

Cybercrime im weiteren Sinne = alle konventionellen Straftaten, bei denen der Computer nur der effizienteren Durchführung dient.

II. Cybercrime zum Nachteil der Mandanten

Fall 1 (Warenbetrug)

II. Cybercrime zum Nachteil der Mandanten

Fall 1 (Warenbetrug):

Der fotografiebegeisterte Mandant kauft bei eBay eine tolle, sonst über 1.000 € teure digitale Spiegelreflexkamera, nahezu neuwertig, mit Restgarantie zum Festpreis für 450 €. Er zahlt, erhält aber keine Kamera. Im Rahmen seiner Strafanzeige wegen Betruges erfährt er, dass der polizeibekannte, drogenabhängige Täter an dem Tag diese Kamera, die er gar nicht besitzt, 40 x verkauft hat (Schaden 18.000 €).

Warenbetrug (§ 263 Strafgesetzbuch, nachfolgend = StGB):
Der Täter verkauft etwas übers Internet, z.B. über eBay, was er gar nicht besitzt und damit nach Geldeingang auch nicht liefern kann.

II. Cybercrime zum Nachteil der Mandanten

Fall 2 (Onlineshops)

Fall 2 (Onlineshops):

Die Mandantin stellte fest, dass ihrer Kreditkarte Einkäufe in einem Online-Shop von 800 € belastet wurden, den sie gar nicht kannte. Sie musste ihre Kreditkarte sperren lassen und (kostenpflichtig) eine neue bestellen. Sie erstattete Strafanzeige. Es stellte sich heraus, dass sie in einem anderen Online-Shop Ware bestellt hatte. Laut BSI (Bundesamt für Sicherheit in der Informationstechnik) vom April 2017 sollen mindestens 1000 deutsche Online-Shops von Online-Skimming betroffen sein. Dabei nutzten Cyber-Kriminelle Sicherheitslücken in veralteten Versionen der Shopsoftware, um einen schädlichen Programm-code einzuschleusen. Dieser späht (engl.: to skimm) dann beim Bestellvorgang die Zahlungsinformationen der Kunden aus und übermittelt sie an die Täter.

Betroffen waren Online-Shops mit der weit verbreiteten Software Magento. Nach § 13 VII TMG (Telemediengesetz) sind Betreiber von Online-Shops zu aktueller Sicherheitssoftware verpflichtet, die sogar auf aktuellen Stand mit dem kostenfreien Dienst MageReport überprüft werden kann.
Die Mandantin erhielt ihr Geld zurück, die Bank nahm Regress beim Online-Shop.

II. Cybercrime zum Nachteil der Mandanten

Fall 3 (Nachstellung, Cybermobbing, § 238 StGB,
Beleidigung, Verleumdung §§ 185, 187 StGB)

Fall 3 (Nachstellung, Cybermobbing, § 238 StGB, Beleidigung, Verleumdung §§ 185, 187 StGB):

Die 19-jährige Mandantin hatte sich nach massiven verbalen Attacken von ihrem Freund (20) getrennt. Tagelang bedrängte er sie per Handy, SMS, WhatsApp, facebook etc. Er machte sie im sozialen (?) Netzwerk schlecht. Mehrfach stündlich klingelte ihr Smartphone. Er drohte ihr, das alles zu verschärfen, wenn sie nicht zu ihm zurück käme.

Die Empfehlung, für mindestens zwei (!) Tage ihr Handy komplett ab zu schalten und aus zu lassen, führte überraschend zum Erfolg, er ließ sie in Ruhe.

Für die Mandantin waren allerdings die zwei (!) Tage ohne Handy eine grenzwertige Erfahrung (O-Ton: „Das war Höchststrafe!“)

Fall 4 (Kurzberichte: Navigation / Wetter / websites):

Geburtstagswetter-Anfrage der Mandantin wird teuer.
Tippfehler-Domains
Ge-Sucht / Ge-Funden: Navigation zum Urlaubsort kostenpflichtig
Fake-Shops

- Hilfen im Netz gegen Cyber-Mobbing:
  http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing

- Prävention und Ansprechpartner:

„Sicher im Netz“, aktuelle Päventionsbroschüre im Verlag Deutsche Polizeiliteratur = av@vdpolizei.de.

Nähere Infos auch unter www.PolizeiDeinPartner.de .

ZAC Köln (Zentral- und Ansprechstelle Cybercrime Köln),
Gesamt-E-Mail-Adresse = zac@sta-koeln.nrw.de

III. Cybercrime durch Mandanten

Fall 5 (Der Märklin-Fan, Warenkreditbetrug, § 263 StGB)

III. Cybercrime durch Mandanten

Fall 5 (Der Märklin-Fan, Warenkreditbetrug, § 263 StGB):

Der Mandant ist Märklin - H0 – Fan. Geld hat er nicht. Er bestellt übers Internet in einer Märklin-Börse ein seltenes Diesellok-Modell bei einem privaten Verkäufer, der keine Vorkasse wünscht. Die Lok kommt bei ihm an, er zahlt nicht. Dem Verkäufer gibt er auf Mahnungen an, er habe die Lok nie erhalten.

Warenkreditbetrug (§ 263 StGB: der Käufer erhält die von ihm bestellte Ware, zahlt nicht und behauptet, sie nie erhalten zu haben).

Betrüger sind oftmals Wiederholungstäter, es ging trotz engagierter Verteidigung für den Mandanten nicht gut aus.

III. Cybercrime durch Mandanten

Fall 6 (H. und die Pille)

Fall 6 (H. und die Pille):

Die 13-jährige H., zum Leid ihrer Eltern sehr früh sehr weit sexuell entwickelt, wollte für den Sex mit ihrem Freund die „Pille“ haben. Die Eltern lehnten das ab, es gab diverse Gespräche. H. scannte ohne Kenntnis ihrer Mutter deren Personalausweis ein und bestellte im Internet die Anti-Baby-Pille ohne Rezept, dieses nach zu reichen versprechend, Eilbedürftigkeit, fruchtbare Tage etc. mit dem Altersnachweis über den Personalausweis ihrer Mutter auf deren Namen. H. bekam die „Pille“.....

Strafbarkeit nach § 281 StGB (Missbrauch von Ausweispapieren) und Verstoß gegen das ArznMiG (Arzneimittelgesetz) kamen in Betracht. Aber H. war unter 14 Jahre alt und damit nach § 19 StGB straflos. Kommentar des Vaters. „Ich sperr die im Schrank ein, bis sie 18 ist!“ Der Rechtsanwalt: „ das ist ein Verbrechenstatbestand, Freiheitsberaubung, § 239 III Nr. 1 StGB.“ Der Vater blieb straflos.

III. Cybercrime durch Mandanten

Fall 7 (Heroin und bitcoins)

Fall 7 (Heroin und bitcoins):

Der 15-jährige Mandant bestellte zum Eigenkonsum übers Darknet wochenlang sporadisch Heroin, das über Packstationen geliefert wurde (§§ 29, 29 a BtMG = Betäubungsmittelgesetz).

Als die international agierende Bande, die mit den Drogen handelte, aufflog, wurde auch der Ankauf des Mandanten bekannt.

Gezahlt hatte er mit der Internetwährung bitcoins. Besonders pikant: beschafft hatte er sich diese dadurch, dass er seinerseits gefakte, angeblich gestohlene PINs und TANs von Bankkonten übers Darknet an andere im Internet agierende Täter verkaufte (also selbst Betrüger betrog, § 263 StGB).

Seine monatlichen Einnahmen hieraus waren stets im vierstelligen Euro-Bereich.

Bitcoin

Bitcoin ist das virtuelle Internetzahlungsmittel. Es gibt andere Zahlungseinheiten wie „Ukash“ (seit 2015 = „paysafecard“), aber bitcoin hat sich seit 2008 durchgesetzt.

Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet abgewickelt. Die kryptografische Technik schützt dabei vor Missbrauch Dritter. Zahlungen erfolgen an pseudonyme Adressen, die permanent neu erzeugt werden können.

Zum Empfangen und Überweisen wird eine lokale Bitcoin-Software oder eine Online-Plattform genutzt.

Der Kurs schwankt, derzeit kostet ein bitcoin ca. 1.400 €.

III. Cybercrime durch Mandanten

Fall 8 (Nord-Süd-Gefälle, § 29 a BtMG)

Fall 8 (Nord-Süd-Gefälle, § 29 a BtMG):

Der Mandant, Student (20 Jahre alt), hatte einen Freund in Bayern, der Ecstasy konsumierte. Von diesem kannte der Mandant die bayerischen Preise, die fast doppelt so hoch wie in NRW waren. Er kam auf die Idee, das gewinnbringend zu nutzen und kaufte hier 500 XTC-Pillen.

Über seinen Freund bekam er Kontakt zu dessen Dealer in Bayern. Die gesamte Korrespondenz lief über E-Mails. Genutzt wurde dafür das Programm privatenotes. Danach vernichten sich E-Mails direkt selbst, nachdem sie gelesen wurden. Das Programm ist frei über Chip.de oder Computerbild etc. downloadbar.

Als der Dealer in Bayern nach gezielter Observation aufflog, wurden seine Bankkonten überprüft. Dabei fand sich auch die Überweisung auf das private Girokonto des Mandanten, der so ermittelt wurde.

III. Cybercrime durch Mandanten

Fall 9 (Großdealen über Packstationen, §§ 29 a, 30, 30 a BtMG)

Fall 9 (Großdealen über Packstationen, §§ 29 a, 30, 30 a BtMG):

Der Mandant war Mitglied einer deutschlandweit agierenden Bande, die mit Drogen, insbesondere Marihuana und Amphetaminen jeweils im Kilogrammbereich handelte. Er konsumierte zunehmende Mengen Marihuana, Amphetamine und Kokain selbst. Der Bandenchef hatte diverse Kontakte, insbesondere über das Darknet. Er teilte dem Mandanten und weiteren Bandenmitgliedern regelmäßig per E-Mail über privatnotes mit, an wen sie wohin welche Mengen zu verpacken und zu verschicken hatten.

Die Paketsendungen wurden dann regelmäßig bei Postschaltern aufgegeben und an Packstationen zur Abholung versandt.

Die zu verschickenden Drogen besorgte ein örtlicher Großdealer. Es war ein äußerst lukrativer An- und Verkaufshandel entstanden, der über einen Zeitraum von 1,5 Jahren betrieben wurde.

Die eingehenden Geldbeträge aus dem Verkauf gingen an den Bandenchef, der Gelder in bar dem Mandanten für den Ankauf der Drogen vom örtlichen Großdealer übergab. Der Mandant war damit quasi der Buchhalter.

Die Korrespondenz zwischen dem Bandenchef und den Abnehmern erfolgte ebenfalls über E-Mails. Nach seiner Festnahme konnte sein total gesicherter PC trotz des Einsatzes von Spezialisten der Polizei nicht „geknackt“ werden.

Fall 9, S. 3

Ins Visier der Fahnder war die Bande geraten, weil einer Mitarbeiterin einer Poststation auffiel, dass meistens derselbe Kunde an Privatadressen wöchentlich bis zu mehrere Dutzend Pakete aufgab. Sie meldete das der internen Sicherheitsabteilung, die die Kripo einschaltete. Bereits das daraufhin von der Polizei am Bestimmungsort in Süddeutschland untersuchte erste Paket enthielt 1 kg Marihuana. Daraufhin begann die gezielte Observation mit TKÜ (Telekommunikationsüberwachung) etc. Dennoch konnte die E-Mail-Korrespondenz nicht gehackt werden.

Die Täter erhielten Haftstrafen je nach Tatbeteiligung zwischen 3 und 10,5 Jahren.

Fazit

Im Internet wird inzwischen nahezu alles gesucht, verkauft oder zum Gegenstand von Straftaten im Drogen- und allen anderen Kriminalitätsbereichen gemacht.

Das Tatgeschehen erfolgt oftmals wesentlich schneller und beim Cybermobbing durch die erreichte Menge von Usern wesentlich einschneidender für die Tatopfer.

Das Tagungsthema „Ge-Sucht im Netz Gefahren und Hilfen im Internet“ erfasst damit in erheblichem Umfang auch den strafrechtlichen Bereich.

Wir werden uns in (baldiger) Zukunft sicherlich erneut mit dem Thema befassen müssen.

Quellen

Reiter, Martin (StA), Cybercrime – was ist das?, JM (Juris – Die Monatszeitschrift) 2/2016, S. 83 ff.

BSI (Bundesamt für Sicherheit in der Informationstechnik), Skimming-Attacken gegen Online-Shops, NJW-aktuell 4/2017, S. 28

www.klicksafe.de

Deutsche Polizei, Heft Mai 2017, S. 8 (Prävention)

Wikipedia, Bitcoin

www.heise.de/thema/Bitcoin

Vielen Dank

für Ihre Aufmerksamkeit!