TAGUNGSBERICHTE

Erlanger Cybercrime Tag 2019: Cyber-Finanzkriminalität und Virtuelle Geldwäsche

von Akad. Rat a.Z. Dr. Christian Rückert
und Wiss. Mit. Marlene Wüst

Der Tagungsbericht enthält sprachlich bereinigte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten. Dementsprechend wurde auch auf Fußnoten verzichtet. Der Erlanger Cybercrime Tag 2019 wurde vom Bundesministerium des Innern, für Bau und Heimat gefördert.

Am 13. März 2019 fand die Veranstaltungsreihe „Erlanger Cybercrime Tag" (ECCT) zum dritten Mal statt. Nach den erfolgreichen Tagungen zu virtuellen Kryptowährungen sowie zur Underground Economy des Darknet in den letzten Jahren, widmete sich der ECCT dieses Jahr der Cyber-Finanzkriminalität und der Virtuellen Geldwäsche. Annähernd 100 Besucher versammelten sich im Wassersaal der Erlanger Orangerie, um die Vorträge zu hören und sich über die Tagungsthemen auszutauschen. Wie in den letzten Jahren, fand sich ein breit gefächertes Publikum bestehend aus Vertreterinnen und Vertretern der Polizei- und Finanzbehörden, der Anwaltschaft, der Informatik und der Rechtswissenschaft sowie aus Wirtschaft und Industrie, insbesondere aus dem Bankenwesen, ein. Außerdem hatten erfreulicherweise auch zahlreiche Studierende den Weg zur Tagung gefunden.

Mit den Themen „Cyber-Finanzkriminalität und Virtuelle Geldwäsche" griff der ECCT erneut brandaktuelle Problemfelder auf. Finanzielle Transaktionen werden heute fast ausschließlich online vorgenommen, Bankgeschäfte werden nahezu vollständig im virtuellen Raum des Internets abgewickelt. Die Digitalisierung des Geldkreislaufs hat eine zunehmende Verlagerung der Finanzkriminalität in den virtuellen Raum zur Folge. Parallel ist in den letzten Jahren ein Anstieg der Verwendung von modernen IT-Technologien zur Geldwäsche zu beobachten. Bereits in den Begrüßungsworten der Vizepräsidentin Education der FAU, *Professor Dr. Bärbel Kopp*, und des Sprechers des Fachbereichs Rechtswissenschaft der FAU, *Professor Dr. Jan-Reinhard Sieckmann*, sowie in der Einführungsrede des Veranstalters, *Professor Dr. Christoph Safferling, LL.M. (LSE)*, wurden die gesellschaftlichen und rechtsdogmatischen Fragestellungen aufgeworfen, die diese Entwicklung mit sich bringt: Auf welche neuen Formen der Finanzkriminalität müssen sich Strafverfolger, Unternehmer und Bürger[1] einstellen? Sind die bestehenden Strafgesetze ausreichend oder bedarf es einer Anpassung an die neuen Phänomene? Welche neuen Ermittlungsmaßnahmen und -werkzeuge müssen den Strafverfolgungsbehörden zur Verfügung gestellt werden, um eine wirksame Strafverfolgung von Finanzdelikten auch im virtuellen Raum zu ermöglichen? Und welche neuen Anforderungen ergeben sich durch die Virtualisierung der Finanzkriminalität und der Geldwäsche für die anwaltliche Beratung und die Compliance von Unternehmen?

Zur Beantwortung dieser und weiterer Fragen, hatte die International Criminal Law Research Unit (ICLU) von *Professor Dr. Christoph Safferling, LL.M. (LSE)* mit *Dr. Boris Hemkemeier* (Commerzbank AG), *Professor Dr. Philipp Maume*, *S.J.D. (La Trobe)* (TU München), *Andrea Link* (BayLKA) und *RA Dr. Alexander Cappel* (Norton Rose Fulbright) herausragende Experten aus unterschiedlichen Bereichen eingeladen.

I. Cyber-Finanzkriminalität: Online-Betrug gegen Firmenkunden (*Dr. Boris Hemkemeier,* Commerzbank AG)

Die Tagung wurde durch einen Vortrag von *Dr. Boris Hemkemeier*, Direktor für Information Security Consulting & Research bei der Commerzbank in Frankfurt, eingeläutet. *Dr. Hemkemeier* führte das interessierte Publikum in das Thema der Cyber-Finanzkriminalität aus der Sicht von Banken und Unternehmen ein.

1. Vom beleghaften Betrug zum Cybercrime

Online-Banking wurde in Deutschland erstmals in dem Jahr 1983 mit BTX durchgeführt, im Internet erst seit Mitte der 90er Jahre; die Commerzbank betreibt es seit 1996. Mit Cybercrime, womit im Folgenden Angriffe auf die Kunden und ihre Geräte gemeint sind, sieht sich die deutsche Kreditwirtschaft erst seit den Jahren 2004-2005 konfrontiert. Bis heute sind die Schadenszahlen in klassischen, „analogen" Betrugsformen wesentlich höher als im Online-Banking, obgleich die subjektive Risikowahrnehmung der Kunden eine andere ist. Als Reaktion auf den Cybercrime hat man verstärkt in die Sicherheit der Technik beim Online-Banking sowie im Freigabeverfahren in-

[1] Aus Gründen der besseren Lesbarkeit wurde an gegebenen Stellen das generische Maskulinum verwendet. Diese Formulierung umfasst gleichermaßen weibliche und männliche Personen.

vestiert. Dies hat zur Folge, dass die Täter nicht mehr primär die Technik angreifen, sondern vermehrt auch deren Nutzer. Aus diesem Grund reichen sichere Netzwerke und Apps nicht mehr aus, sondern präventive Ansätze müssen die Nutzer erreichen.

a) Die Sicherheitsstrategie im Cybercrime

Zum strategischen Plan der Cybercrime-Bekämpfung der Commerzbank gehören vier Säulen: Prävention, Detektion, Reaktion und Strafverfolgung. In einem ersten Schritt müssen präventiv ein sicheres Online-Banking sowie sichere Onboarding-Prozesse geschaffen werden. Kommt es dennoch zu Cybercrime-Vorfällen, ist eine frühzeitige Detektion dieser notwendig. Ziel ist es, einen Angriff in Echtzeit sehen und erkennen zu können. Wird ein Angriff entdeckt, muss hierauf reagiert werden. Diese Reaktion kann verschiedene Facetten haben, z.B. das Stoppen einer verdächtigen Zahlung oder die Änderung interner Prozesse. Die vierte Säule der engen Zusammenarbeit mit den Strafverfolgungsbehörden ist ausgesprochen wichtig. Wie *Darwin* sagte: „Bessere Mausefallen enden mit schlaueren Mäusen". Eine gute Prävention bewirkt zum einen eine Verdrängung der Täter zum Wettbewerber, zum anderen die Entwicklung neuer, intelligenterer Angriffe. Gegen dieses Wettrüsten ist es nachhaltig allein wirksam, die Täter aus dem Verkehr zu ziehen. Die Bedeutsamkeit der engen Zusammenarbeit von Banken und Strafverfolgungsbehörden wird durch das föderale Prinzip Deutschlands verstärkt. Hiernach werden Cybercrime-Fälle nach dem Tatortprinzip lokal ermittelt, was das Erkennen eines etwaig bestehenden Zusammenhangs zwischen einzelnen Fällen erschwert. Banken können dahingegen einfacher einen Überblick gewinnen, welche Fälle zu einer gemeinsamen Serie gehören.

b) Wandel durch Digitalisierung

Im digitalen Zahlungsverkehr hat sich die Art des Betruges im Vergleich zum analogen Zahlungsverkehr verändert. Beim SEPA-Überweisungsträger dient die Unterschrift des Kunden, die aber durchaus fälschbar ist, als Autorisierung für den Zahlungsvorgang. Die digitalen Signaturen im Electronic-Banking können dahingegen nicht mehr einfach gefälscht werden. Sie sind an den Zahlungsauftrag gebunden und können nur durch den Kunden erzeugt werden. Aus diesem Grund ist im Zuge der Digitalisierung der Kunde in den Fokus der Cyberkriminellen gerückt. Im Folgenden sollen ein paar – primär aus dem Privatkundengeschäft stammende – Beispiele für industrialisierten Cybercrime dargestellt werden.

2. Beispiele für industrialisierten Cybercrime

Schadsoftwares werden per E-Mail, z.B. durch fiktive Telekom-Rechnungen, verbreitet. Ist der PC infiziert, bleibt die Schadsoftware solange inaktiv, bis der Kunde eine Zahlung per Online-Banking, PayPal oder ähnlichem beginnt. In diesem Moment greift die Schadsoftware ein und greift Benutzernamen und das Passwort ab. Die zur Freigabe von Transaktionen noch fehlenden TANs werden von den Betrügern oftmals durch simples Nachfragen erlangt. Auch wenn nur wenige auf solch eine Anfrage reagieren, ist dies bei Millionen betroffenen Kunden eine beachtliche Anzahl. Teilweise wird die Anfrage auch unter einem Vorwand gestellt, z.B. dass die Bank ein neues Freigabeverfahren einführt und zur „Qualifizierung für das neue Verfahren" eine Entwertung aller alten TANs notwendig ist.

Eine der tückischsten Methoden ist der sog. Rücküberweisungs-Trojaner. Die Schadsoftware blendet eine Nachricht an den Nutzer ein, dass er irrtümlich einen Geldeingang erhalten habe, der ihm nicht zusteht und nun zurücküberwiesen werden müsse. Dies sei einerseits in der Filiale möglich, zusätzlich wird jedoch ein Link mit einer vorausgefüllten Überweisungsmaske eingefügt. Um den Druck zu erhöhen, erfolgt außerdem ein Hinweis, dass das Konto bis zur Rücküberweisung gesperrt werde. Bei einer Prüfung des Kontostandes durch den Nutzer erscheint tatsächlich ein höherer Saldo. Das trojanische Pferd hat in den Umsatzlisten einfach eine weitere Zeile hinzugefügt und den Saldo entsprechend manipuliert. Dem Kunden ist durchaus bewusst, dass er jetzt Geld überweist, aber der Kontext des vermeintlichen Geldeingangs ist eine Täuschung.

Die Commerzbank betreibt eigene Detektionssysteme, um diese Angriffe auf Kunden in Echtzeit zu erkennen und Zahlungen zu überprüfen. Eine Sicherheitsgarantie für Privatkunden sichert einen möglichen Schadensfall ab, wenn der Kunde eine Anzeige stellt und bei der Aufklärung unterstützt.

3. Social Engineering: Cybercrime im Firmenkundengeschäft

Das Firmenkundengeschäft unterscheidet sich vom Privatkundengeschäft dahingehend, dass Banking deutlich weniger standardisiert ist. Im Gegensatz zum Online-Banking durch Privatkunden wird hier in der Regel nicht die Online-Seite der Bank oder deren App genutzt, sondern eigene Systeme oder Clients. Die Heterogenität der verwendeten Systeme erschwert den Tätern einen Angriff und macht diesen weniger lukrativ. Aus diesem Grund versuchen die Täter ihre kriminellen Absichten über eine Manipulation des Kunden zu verwirklichen (sog. Social Engineering). Technische Angriffe bilden im Firmenkundengeschäft eine Ausnahme. Im Folgenden werden verschiedenste Szenarien des Social Engineering skizziert:

a) Ein Betrugsszenario ist das „Remote Access Tool". In diesem Fall wird ein Mitarbeiter vermeintlich von der Bank angerufen und darauf hingewiesen, dass ein Update ihres Zahlungssystems durchgeführt werden muss. Unter diesem Vorwand wird der Mitarbeiter gebeten, alle Legitimationsmedien anzuschließen, die Zugangsdaten zu offenbaren, sowie eine Fernwartungssoftware zu starten. Hierdurch erhalten die Täter freien Zugriff auf die Banking-Systeme der Firma.

b) Einen Klassiker des Social Engineering bilden gefälschte Zahlungsbestätigungen. Hier weist der vermeintliche Käufer nach Abschluss eines Geschäfts gefälschte Zahlungsbestätigungen oder Formulare nach, bis der Verkäufer die Ware versendet. Verbreitet sind in diesem Zusammenhang auch gefälschte Bankgarantien. Um die Glaubhaftigkeit zu stärken sind diese oftmals mit komplexen Texten sowie Unterschriften von Vorständen der Bank versehen. Für Rückfragen sind zum Teil E-Mail-Adressen oder Links zu einer Webseite angegeben, die jedoch zu einer gefälschten Domain führen.

c) Weit verbreitet sind ferner Rechnungen für nicht erbrachte Leistungen. Diese gehen häufig mit einer vermeintlichen E-Mail des Vorgesetzten einher, der um eine Bezahlung der Rechnung mit dem Hinweis bittet, dass eine Rückmeldung nicht notwendig sei. Auffällig ist, dass sich die Höhe der Rechnungen oftmals an Grenzwerten wie 10.000 € oder 50.000 € orientieren, deren Überschreitung eine strengere Prüfung zur Folge hat.

d) Ein weiteres sehr bekanntes Betrugsszenario ist die Schecküberzahlung. Bei diesem Szenario stellt der Kunde „versehentlich" einen zu hohen (gefälschten) Scheck aus, um dann eine Rücküberweisung des überschüssigen Geldes zu verlangen. Eine Neuheit stellt hier das Vorgehen der Betrüger dar, den Scheck nicht dem Kunden zu übergeben, sondern diesen im Namen des Kunden direkt bei der Bank einzureichen. Die Firma erreicht dann lediglich der für sie nicht zuordenbare überschüssige Betrag. Aus diesem Grund fragt die Commerzbank bei Unsicherheiten direkt beim Kunden nach, ob er den Scheck eingereicht hat.

e) Das meiste Betrugsvolumen macht der Mandatsbetrug aus. In diesem Fall teilt der Betrüger im Namen eines echten Lieferanten dem Kunden mit, dass sich seine Kontoverbindung geändert habe und das Geld zukünftig auf ein anderes Konto überwiesen werden solle. Dieser Betrug fällt leider häufig erst auf, wenn der wirkliche Lieferant nach einer Weile nach seinem Geld fragt. Deswegen wird empfohlen, Stammdatenveränderungen nur bei klarer Legitimation oder nach Rückfrage beim Lieferanten vorzunehmen.

f) Neben diesem „klassischen" Betrug innerhalb einer Kunden-Lieferanten-Beziehung ist das Betrugsszenario des „Man in the Middle" seltener und raffinierter. Hier mischen sich die Täter in das Geschäft ein indem sie Domains registrieren, die fast so aussehen wie die Domains der beteiligten Geschäftspartner. Der „Man in the Middle" macht zunächst nichts anderes, als die Dokumente jeweils an die Geschäftspartner weiterzuleiten. Die Geschäftspartner kommunizieren also über eine dritte Person miteinander, ohne dies zu merken. Sobald die Bankverbindung übermittelt wird, ändert der Täter diese.

g) Als „Königsdisziplin" wird der sog. CEO Fraud oder „Fake President" angesehen. Hier erhält ein zur Freigabe von Transaktionen befugter Mitarbeiter eine vermeintliche E-Mail von seinem Chef, durch die er mit einer streng geheimen Finanztransaktion betraut wird. Zudem meldet sich ein angeblich mit der Vorbereitung der Transaktion beauftragter Anwalt bei dem Mitarbeiter und erklärt dessen Zustimmung. Insgesamt handelt es sich um ein lukratives Geschäft für die Täter, für das sie viel Aufwand betreiben. Eine Rückfrage durch die Bank, ob es sich um einen Betrug handeln könnte, wird in diesen Fällen meist abgelehnt und auf die strenge Vertraulichkeit des Geschäfts verwiesen. Der CEO-Fraud endet auf zwei Weisen: entweder wird er entdeckt oder der Firma gehen die liquiden Mittel aus.

h) Ein weiteres Betrugsszenario ist die Ransome Ware. Dieser Trojaner wird z.B. mittels eines E-Mail-Anhangs verschickt. Wird der Anhang geöffnet, erhält die Schadsoftware Zugang auf den Rechner und verschlüsselt die Laufwerke. Nach der Verschlüsselung wird ein Lösegeld (meist in Bitcoin) gefordert. Dieses Betrugsmittel hat sich dahingehend verändert, dass nicht mehr nur Konsumenten angegriffen werden. Mittlerweile werden Firmen vorher ausspioniert und Back-Ups beseitigt, bevor diese mit einer Ransom Ware attackiert und sehr hohe Lösegelder gefordert werden.

4. Schutzmöglichkeiten und Maßnahmen im Betrugsfall

Der wichtigste Punkt beim Schutz vor Betrügereien im Firmenkundengeschäft ist die Firmenkultur. Unter den Mitarbeitern muss ein Bewusstsein für die Betrugsrisiken herrschen und Rückfragen zu Kontonummeränderungen oder ungewöhnlichen Zahlungen müssen – insbesondere, wenn es um große Geldsummen geht – erlaubt sein. Wurde man dennoch Opfer eines Betrugs ist es wichtig, sofort die Bank zu kontaktieren. Je weniger Zeit vergangen ist, desto höher sind deren Chancen, das Geld verfolgen zu können. Die Bank kann unmittelbare Überweisungsrückrufe tätigen, die weitaus erfolgreicher sind als ein alleiniger Swift Recall bei der Zielbank. Zudem verfügt die Commerzbank über ein weltweites Netzwerk mit internationalen Banken und kann je nach Modus Operandi hohe Recovery Rates erzielen. Darüber hinaus kann sie Kontakte zu Ermittlungsbehörden, die auf Cybercrime bzw. Wirtschaftskriminalität spezialisiert sind, vermitteln. Eine enge Zusammenarbeit der Banken mit den Strafverfolgungsbehörden ist – wie eingangs erörtert – der ausschlaggebende Punkt im Umgang mit Cyber-Finanzkriminalität.

5. Diskussion

In der Diskussion wurde näher auf die genauen Vorgehensweisen der Bank und der von ihr verwendeten Mechanismen bei der Detektion und Prävention von Betrugsfällen eingegangen. Insbesondere wurde thematisiert, wie detailliert das Kundenverhalten von der Bank beobachtet wird und welche Daten diese erhebt. Um die Transaktionen nachvollziehen und regulatorische Anforderungen erfüllen zu können, werden klassische Webserverlogs eingesetzt, die sowohl die IP-Adresse als auch den verwendeten Browser bzw. die verwendete App speichern. Darüber hinaus wurde die angesprochene Rückkehr zum klassischen Betrug diskutiert und festgehalten, dass sich die

moderne Cyber-Finanzkriminalität sowohl durch klassischen Betrug als auch durch ein Ausnutzen der Technik auszeichnet.

II. Cyber- Finanzermittlungen – Herausforderungen und Chancen durch moderne IT-Technologie (*Andrea Link,* BayLKA)

Nach der Betrachtung der Cyber-Finanzkriminalität aus dem Blickwinkel der Banken erfolgte ein Perspektivenwechsel. *Andrea Link*, die als Wirtschaftskriminalistin beim Bayerischen Landeskriminalamt (BayLKA) tätig ist, thematisierte in ihrem Vortrag die Besonderheiten von Finanzermittlungen.

Von einer Veröffentlichung dieses Vortrags wird aus ermittlungstaktischen Gründen abgesehen.

III. Virtuelle Kryptowährungen und Geldwäscheregulierung *(Professor Dr. Philipp Maume, S.J.D [La Trobe]*, Technische Universität München)

Im Anschluss an die Darlegung der Möglichkeiten bei Cyber-Finanzermittlungen beleuchtet der Vortrag von *Professor Maume* vor allem dogmatische Fragen der Geldwäscheregulierung im Bereich der Kryptowährungen.

1. Geldwäsche und Regulierung von Kryptowährungen

Geldwäscheregulierung ist technologieneutral, das heißt, es werden Akteure und nicht Technologien reguliert. Das hat den Vorteil, dass auch für neue Technologien bereits ein Regulierungskorsett vorhanden ist, das nur noch angepasst werden muss. Deshalb ist auch die Aussage falsch, Kryptowährungen und ICOs seien nicht reguliert. Es fehlt jedoch bislang an einer spezifischen, auf die Geldwäschegefahren der Kryptowährungen zugeschnittene, Regulierung.

2. Technischer Hintergrund von Tokensystemen

Die Blockchain ist eine „kontinuierlich erweiterbare Liste von Datensätzen, die durch kryptografische Verfahren miteinander verbunden sind und deren Speicherung dezentral auf den Rechnern der Teilnehmer erfolgt". Grundlage ist die Distributed Ledger Technology. Ledger bedeutet Speichereinheiten. Es handelt sich also um eine Datenbank. Diese Datenbank wird ständig fortgeschrieben und die Datensätze werden in sog. Blöcken gespeichert und aneinandergereiht. Daher kommt der Begriff Blockchain. Auf dieser Blockchain können Transaktionen durchgeführt werden. Die Transaktionen in der Datenbank funktionieren durch die sog. Tokenisierung. Der Begriff Token meint in diesem Zusammenhang schlicht „Werteinheit". Durch Tokenisierung schafft man eine Form von virtueller Umlauffähigkeit auf der Blockchain. Die Teilnehmer einer Blockchain verfügen über gewisse Rechte. Auf der Blockchain hat jeder User einen sog. Public-Key. Das ist eine Ziffernfolge, mit der er identifiziert werden kann. Man kann beliebig viele Public Keys generieren, d.h. ein bestimmter User kann unter verschiedenen Identitäten auf einer Blockchain gespeichert sein. Zu jedem Public Key hat der User auch einen Private Key, mit dem er Transaktionen ausführen kann und den der User geheim halten sollte. Die Schlüsselpaare werden von den Nutzern in einer sog. Wallet verwaltet.

Zur Durchführung einer Transaktion genügt das Absenden der Nachricht in das System, dass ein Token von einem Public Key auf einen anderen Public Key übertragen werden soll. Der Token ist dann dem anderen Public Key zugewiesen. In der Rechtswissenschaft wird dies bisweilen unscharf als Übertragung oder Übereignung bezeichnet. Es wird bei der Übertragung z.B. eines Bitcoins aber nichts verschickt, sondern nur eine Zuordnung geändert. Was die Blockchain-Technologie so interessant macht, ist, dass es durch die dezentrale Speicherung zwar nicht unmöglich, aber zumindest extrem schwierig ist, Transaktionen zu fälschen oder nachträglich zu verändern. Außerdem sind Transaktionen von überall auf der Welt möglich. Die Blockchain ist auch nicht an ein bestimmtes Bankensystem oder an ein Transaktionsformat gebunden, es gibt also keine Schnittstellenproblematik. Die Blockchain ist auch sehr flexibel: Je nach verwendeter Programmierung kann sie offen einsehbar sein oder eben nicht.

In der Praxis haben sich drei verschiedene Tokenarten herausgebildet. Zunächst gibt es die sog. Investment oder Security Token. Diese sind wertpapierähnlich, das bedeutet, dem Inhaber dieses Tokens stehen Rechte an einem Unternehmen zu, i.d.R. eine Beteiligung am Gewinn oder eine fixierte Rückzahlung im Sinne einer Anleihe. Daneben gibt es die sog. Currency Token, auch virtuelle Währung genannt. Currency Token zeichnen sich dadurch aus, dass sie im Regelfall keine besonderen Rechte repräsentieren. Sie basieren nur darauf, dass andere ihnen einen Wert zumessen. Drittens gibt es sog. Utility Token, welche mit einem digitalen Gutschein vergleichbar sind. Der Inhaber dieses Token hat ein Recht gegen ein Unternehmen, z.B. Zugriff auf Rechenleistung oder Speicherplatz in einer Cloud. Geldwäscherechtlich sind alle Tokenarten relevant. Sie werden alle auf die gleiche Art und Weise technisch übertragen und können alle zur Zahlung oder zum Tausch genutzt werden.

Aus Regulierungsperspektive ist interessant, dass Blockchains im Grundsatz pseudonym sind, weil die Transaktionshistorie einsehbar ist und jeder User durch mindestens einen Public-Key repräsentiert wird. Man kann eine Transaktion einem Public-Key und damit einer Person zuordnen. Das bedeutet, dass die Aktivitäten einer Person über die Blockchain verfolgbar sind, wenn man die Person identifiziert hat. Allerdings sind einige Token sogar anonym, d.h. man kann keinen Zusammenhang zwischen Public-Key und den Transaktionen herstellen. Das sind die sog. Privacy Token, z.B. Monero. Außerdem existieren Services, wie Mixer oder Tumbler, die durch eine Abfolge von Transaktion, Teilung von Token, Zirkulartransaktion usw. den Rückschluss auf den Inhaber erschweren.

Es gibt drei Möglichkeiten, Token zu erhalten:
(1) Ein Ersterwerb von Token erfolgt durch ein Initial Coin Offering, bei dem ein Emittent neue Token an Investoren oder Käufer ausgibt.

(2) Ein Zweiterwerb findet beispielsweise statt über Kryptowechselstellen, die Fiat-Geld in Token tauschen oder andersherum. Viele Geschäftsmodelle sind hier sehr intransparent. Es ist oft unklar, ob der Kunde bei solchen Wechselstellen tatsächlich selbst Token erhält (sog. On-Chain-Transaktion) oder, ob der Dienstleister die Token behält und man nur einen Herausgabeanspruch oder sogar nur einen Anspruch auf Bilanzausgleich erwirbt (sog. Off-Chain-Transaktion). Die konkrete Geschäftsart hat wegen der Erlaubnispflicht von Einlagengeschäften eine große Bedeutung im Bereich der Finanzmarktregulierung und im Insolvenzrecht.

(3) Schließlich können an sog. Kryptobörsen im Wege des Zweiterwerbs verschiedene Tokenarten gegeneinander getauscht werden, z.B. Bitcoin gegen Ethereum.

3. Token im System der Geldwäscheregulierung in Deutschland

Rechtsquelle der Geldwäscheregulierung in Deutschland ist vor allem das Gesetz über das Aufspüren von Gewinn aus schweren Straftaten oder Geldwäschegesetz (GWG). In seiner jetzigen Fassung basiert es auf der 4. Geldwäscherichtlinie und wird gerade an die 5. Geldwäscherichtlinie angepasst.

Geldwäscheprävention betrifft, anders als die Straftat der Geldwäsche, nur die sog. Verpflichteten. Verpflichtete sind Kreditinstitute, Banken, Finanzdienstleistungsinstitute, Zahlungsinstitute etc. Ferner gibt es nach § 2 GWG bestimmte Dienstleister, die ebenfalls geldwäscherelevant sind, z.B. Wirtschaftsprüfer, Rechtsanwälte, Immobilienmakler etc. Gleiches gilt für sog. Güterhändler. Der Güterhändler reicht dabei vom kleinen Onlineshop bis hin zu großen Industriekonzern.

Die Verpflichteten müssen nach dem GWG gewisse Pflichten im Rahmen der Geldwäscheprävention erfüllen, z.B. eine Identitäts- und Legitimationsprüfung ihrer Kunden durchführen (sog. KYC-System) und Geldwäscheverdachtsmeldungen abgeben. In diese Regulierung könnten Kryptowährungen über zwei Stellschrauben eingepasst werden:
(1) Erfassung der Dienstleister im Kryptowährungssektor als Verpflichtete und (2) Auslösung von Pflichten durch Kryptowährungstransaktionen.

Damit Kryptowährungstransaktionen vom GWG erfasst wären, müsste es sich um Transaktionen i.S.v. § 1 Abs. 5 GWG handeln. Hiernach ist eine Geldbewegung oder sonstige Vermögensverschiebung erforderlich. Es ist unklar, ob eine Tokentransaktion eine Vermögensverschiebung ist. Grund hierfür ist, dass die Verwaltung eines Tokens auf seinem Public Key nach bislang herrschender Meinung kein absolutes Recht, sondern nur eine faktische Zugriffsmöglichkeit darstellt. Dennoch kann die Tokentransaktion unter den Transaktionsbegriff des GWG subsumiert werden. Nach h.M. genügt für die Vermögensverschiebung der Erwerb eines Gegenstands, dem tatsächlich ein Wert beigemessen wird. Dies ist aufgrund der oben geschilderten Erwerbs- und Verkaufsmöglichkeiten für Token offensichtlich der Fall.

Was die Art der Regulierung angeht, so kann man einen Blick auf die unterschiedlich scharfe Regulierung von Bargeld und Giralgeld werfen. Bargeld ist anonym, aber seine Umlauffähigkeit ist aufgrund seiner Körperlichkeit stark eingeschränkt. Giralgeld lässt sich leicht und schnell in großen Mengen weltweit übertragen, die Transaktionen sind jedoch durch das Bankensystem überwacht. Token dagegen sind pseudonym (ggf. sogar anonym) übertragbar und weisen eine hohe Umlauffähigkeit auf. Sie besitzen daher ein noch über dem Bargeld liegendes Gefährdungspotential für die Geldwäsche. Allerdings sind Token mangels Körperlichkeit offensichtlich kein Bargeld, sodass eine direkte Anwendung der Vorschriften über Bargeld ausscheidet.

Eine weitere Möglichkeit bestünde darin Token als E-Geld zu erfassen. E-Geld ist jeder elektronisch gespeicherte monetäre Wert in Form einer Forderung an den Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge durchzuführen und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird. Wären Token E-Geld, wären die Geschäfte von Token-Emittenten erlaubnispflichtig nach dem ZAG. Die allermeisten Token sind jedoch kein E-Geld. Bei Currency Token fehlt es schon am zentralen Emittenten, die anderen Tokenarten werden nicht allgemein als Zahlungsmittel entgegengenommen.

4. Erfassung von Token durch die 5. Geldwäscherichtlinie

Abhilfe soll auf europäischer Ebene durch Ergänzung der 5. Geldwäscherichtlinie geschaffen werden. Dort wird eine virtuelle Währung definiert als „die digitale Darstellung eines Werts“, der „von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann“. Currency Token werden von dieser Definition erfasst, wohl auch die anderen Tokenarten.

Die 5. Geldwäscherichtlinie führt auch neue Arten von Geldwäschepräventionsverpflichteten ein. Allen voran sind dies die Wechselstuben, die definiert werden als Dienstleister, die virtuelle Währung in Fiatgeld oder umgekehrt, tauschen. Weiterhin gibt es sog. Walletanbieter. Hierunter sind die Anbieter elektronischer Geldbörsen zu verstehen, in denen virtuelle Währungen gespeichert oder auch übertragen werden können.

Die fehlerhafte Annahme, eine Kryptotokentransaktion entspreche einer Zahlung im Bankensystem und die hierauf beruhende Übertragung der bisherigen Geldwäschepräventionsregeln auf Tokensysteme, führt zu Inkonsistenzen. Ein Beispiel hierfür sind Güterhändler. Güterhändler haben nach § 10 Abs. 6 GWG Sorgfaltspflichten, insbesondere die Durchführung eines KYC-Checks in den Fällen des § 10 Abs. 3 S. 1 Nr. 3 (Geldwäscheverdacht) und bei Transaktion, bei welchen sie Barzahlungen über mindestens 10.000 Euro tätigen oder entgegennehmen, zu erfüllen.

Das heißt Bargeld wird schärfer reguliert, was mit Blick auf die geldwäscherechtliche Systematik auch überzeugend ist. Allerdings ist die Zahlung mit Kryptowährungen der Transaktion gleichgestellt und nicht derjenigen mit Bargeld. Das bedeutet, ein Güterhändler muss hier einen KYC-Check nur bei einem Geldwäscheverdacht vornehmen. Angesichts der guten Eignung von Kryptowährungen zur Geldwäsche ist dies ein Wertungswiderspruch. Hieran ändert sich auch nichts durch die 5. Geldwäscherichtlinie. Möglich bliebe somit nur, bei jeder Zahlung mit Kryptowährungen einen Geldwäscheverdachtsfall zu bejahen. Dies erscheint jedoch unwahrscheinlich, weil die Rechtsprechung hierfür bislang konkrete Anhaltspunkte verlangt. Das kann bei einer Kryptowährungstransaktion durchaus der Fall sein, wenn z.B. eine besonders hohe Summe transferiert wird oder eine Stückelung von Transaktionen vorgenommen wird. Weiterhin könnte man erwägen, die Regeln über Bargeld analog anzuwenden. Hiergegen spricht jedoch das Analogieverbot. Das Problem ist also bislang – auch durch die 5. Geldwäscherichtlinie – nicht gelöst.

Ein weiteres Regulierungsproblem besteht darin, dass die Geldwäscherichtlinie nur innerhalb der EU gilt. Man sollte daher erwägen, neue Wege zu gehen. Im Projekt BITCRIME wurde z.B. vorgeschlagen, die Vorteile wie Transparenz und Fälschungssicherheit für die Geldwäscheprävention fruchtbar zu machen. Durch die Verfolgbarkeit der Transaktionen können Transaktionen (und deren Nachfolger in gewissen Teilen) „geblacklisted" werden. Hierin liegt freilich ein starker Grundrechtseingriff, weil die Token hierdurch (teilweise) entwertet werden. Ferner könnte man auch mit einem Whitelisting-Verfahren arbeiten, bei dem „saubere" Transaktionen oder Adressen gelistet werden. Für beides bräuchte man ein zentrales Register, das von einer (halb-)staatlichen Stelle verwaltet wird.

5. Abschließende Thesen

Da Kryptowährungen die besonderen Risikopotentiale von Bargeld und Giralgeld vereinen, wäre eine gesonderte Regulierung geboten. Im derzeitigen GWG und auch nach der 5. Geldwäscherichtlinie wird diesen Besonderheiten nicht ausreichend Rechnung getragen. Die Reform und Erweiterungen der 5. Geldwäscherichtlinie sind sinnvoll, basieren aber auf dem Fehlschluss, das Banksystem und oder die Zahlung im Banksystem wäre mit der Zahlung in Kryptowährungen vergleichbar. Daher sollte eine spezielle Kategorie in das GWG aufgenommen werden, was auch unter Geltung der 5. Geldwäscherichtlinie möglich ist, da diese nur eine Teilharmonisierung erfordert. Vorzugswürdig, aber wohl schwer realisierbar, wäre dagegen ein komplett neuer transaktionsbezogener Ansatz.

Im Diskussionsteil wurde u.a. der regulatorische Umgang mit „anonymeren" Token wie z.B. Monero diskutiert und festgestellt, dass hier noch größere Probleme bestehen, als bei Bitcoin. Weiterhin wurden praktische Fragen zum Umgang mit einer potenziell zu erwartenden großen Menge an Verdachtsmeldungen gestellt. Es wurde empfohlen, nach „Gebräuchlichkeit" der jeweiligen Token für geldwäscherelevante Straftaten zu priorisieren. Schließlich wurde auch eine Regulierung der Kryptotokendienstleister nach KWG (und nicht „nur" nach dem GWG erwogen).

IV. Beratung, Compliance und Verteidigung in (virtuellen) Geldwäscheverfahren (*RA Dr. Alexander Cappel,* Norton Rose Fulbright)

Nachdem die dogmatischen Fragen der Geldwäscheregulierung im Bereich der Kryptowährungen im Vorfeld geklärt wurden, greift der Vortrag von *RA Dr. Alexander Cappel* (Norton Rose Fulbright) Themenkomplexe der Beratung, Compliance und Verteidigung in (virtuellen) Geldwäscheverfahren auf.

1. Beratung, Compliance und Verteidigung in (virtuellen) Geldwäscheverfahren

In der Beratung zum Thema Geldwäscheprävention besteht in der Praxis das große Problem darin, dass es oft allenfalls Anhaltspunkte, selten aber klare Beweise dafür gibt, dass in bestimmten Sachverhalten ein Fall von Geldwäsche vorliegt. Unternehmen können dann nur entweder bestimmte Geschäftsmodelle ablehnen oder diese trotz Unsicherheit durchführen. Denn ex post betrachtet ist es oftmals leicht zu sagen, das Risiko wäre im Voraus abzusehen gewesen.

Die Probleme des § 261 StGB sollen in diesem Vortrag anhand eines Praxisbeispiels aufgezeigt werden. Dieser ist ein häufiges Einfallstor in der Praxis, weil Mandanten des Öfteren der Meinung sind, das GWG beträfe nur Banken und § 261 StGB nur „den" Geldwäscher. Wie falsch eine solche These sein kann und welches Risiko mit dieser Fehleinschätzung für die Mitarbeiter der Unternehmen sowie für das Unternehmen selbst einhergeht, wird im Folgenden näher erörtert. Darauf aufbauend wird erläutert, wie man in der Praxis risikobasiert an das Thema Kryptowährungen herangeht und mit welchen Stellschrauben sich ein Unternehmen auf der Compliance-Seite gut aufstellen kann, um geldwäscherechtliche Risiken weitestgehend zu minimieren. Dabei lässt gerade die Ungenauigkeit des Gesetzgebers den Unternehmen einen großen Spielraum.

2. Der Ausgangsfall

Der Ausgangsfall des Vortrages stellt sich wie folgt dar: Ein Start-up „X", welches im Internet b2b-Software für mittelständische Unternehmen vertreibt, akzeptiert alle Arten von Zahlungsmittel, darunter auch Kryptowährungen. Das Unternehmen hat Geschäftsbeziehungen zu einer Vielzahl an im Internet agierender Unternehmen, darunter das Unternehmen „D", welches als Haupteinnahmequelle im Darknet Waffen vertreibt. D möchte Software von X kaufen und diese mit einer Kryptowährung bezahlen. X ist ein klassischer Güterhändler und hat bisher keine Compliance-Maßnahmen getroffen. Auch die Kunden des X werden nicht vorher überprüft, insbesondere wird die Herkunft der Gelder, die zur Zahlung dienen, nicht erforscht. Dem Mitarbeiter „M" des X kommt die Zahlung des D

komisch vor und er äußert seine Bedenken gegenüber seinem Chef, dem CEO „C“. Letzterer sieht keinen Handlungsbedarf und weist den M an, die Zahlung anzunehmen. Der Fall kann dahingehend variieren, dass das Geld in jedem Fall aus der inkriminierten Quelle stammt oder dass das Geld aus einer anderen Quelle kommt und man nur die entsprechenden Informationen über das Unternehmen D findet. Vorliegend wird von trennbaren Quellen ausgegangen.

Es wird deutlich, dass das weitsichtigere Compliance-Handeln auf wirtschaftliche Interessen trifft. Der unternehmerische Wille, ein Geschäft machen zu wollen, bevor der Konkurrent zuvorkommt, ist sicherlich nachvollziehbar. Dabei entstehen jedoch Risiken sowohl für X und M als auch C. Zunächst muss festgestellt werden, was Geldwäsche eigentlich ist. Dies ist jeder Vorgang, der darauf gerichtet ist, Spuren unrechtmäßiger Herkunft von Erlösen aus Straftaten zu verschleiern, um so die unerlaubt erlangten Vermögenswerte als scheinbar legales Vermögen in den regulären Wirtschaftskreislauf einzuschleusen. Als Beispiel lässt sich der illegale Waffenhändler anführen, der Ware von einem Güterhändler kauft, die er wiederrum schnell weiterveräußern kann und somit das Geld „gewaschen“ wird.

3. Der Rechtsrahmen

Fraglich ist weiterhin, ob ein Geldwäscheverdacht vorliegt. Gesetzlich ist dazu wenig geregelt, so dass Unternehmen oftmals auf Auslegungshinweise von Behörden angewiesen sind oder Literatur konsultieren müssen. Letztlich kommt es aber auf das Geschäft an. Dabei gibt es klassische sog. „Red-Flags“ im Rahmen der Geldwäsche, wie etwa brachen-untypische oder wirtschaftlich unsinnige Geschäfte. Jedoch könnte man hier aufgrund der Neuheit von Kryptowährungen allein die Zahlung mit ihnen als branchen-untypisch charakterisieren. Dies wird wohl in wenigen Jahren schon anders zu sehen sein. Dann wird dies branchen-typisch sein. Zudem könnte die mit Kryptowährungen einhergehende Anonymität bzw. Pseudonymität ein Verdachtsmoment begründen. Diese liegen jedoch in der Natur der Sache, was gegen ein solches Verdachtsmoment spricht. Aus Compliance-Gesichtspunkten heißt dies, dass man feststellen muss, ob gewisse Handlungen überhaupt etwas mit einem konkreten Geschäft zu tun haben und, ob es für sie überhaupt einen plausiblen Grund gibt.

Der Rechtsrahmen ist (neben den EU-Geldwäscherichtlinien) in § 261 StGB, im GWG, aber auch für Finanzunternehmen wie Banken im KWG geregelt. Daneben gibt es in verschiedenen Aufsichtsbehörden vielfältige Veröffentlichungen zum Thema Geldwäsche wie Rundschreiben, Anwendungs- und Auslegungshinweise der BaFin. Es gibt aber auch von verschiedenen Regierungspräsidien hilfreiche Handreichungen zum Thema Geldwäsche, die eine Auslegungshilfe darstellen.

4. Der Straftatbestand der Geldwäsche nach § 261 StGB

Der Straftatbestand der Geldwäsche ist ein klassisches Anschlussdelikt. Es ist also vorher eine Straftat begangen worden und der Geldwäscher versucht die Herkunft von inkriminierten Gegenständen zu verschleiern. Es geht nicht nur um Geld, sondern dies kann jeden Gegenstand betreffen, so dass auch Kryptowährungen darunterfallen und allgemein bewegliche und unbewegliche Sachen, die in irgendeiner Form vermögenswerten Charakter haben. Daneben bedarf es einer tauglichen Vortat, entweder eines Verbrechens oder eines Vergehens aus dem Katalog des § 261 StGB. Da dieser sehr weit ist, muss der Berater seinen Mandanten stets fragen, woher das Geld seiner Kunden stammt bzw. womit diese ihr Geld verdienen. Der § 261 StGB kennt sodann drei Handlungsvarianten: Den Verschleierungstatbestand, den Vereitelungs- und Gefährdungstatbestand und den Isolierungstatbestand. Diese sind denkbar weit formuliert.

Im Vorsatzbereich besteht für die Mandanten ein großes Risiko dahingehend, dass bereits Eventualvorsatz ausreichen kann. Aus Sicht von *Dr. Cappel* stellt die größte Gefahr in der Beratung zur Geldwäsche aber die Leichtfertigkeit dar. Diese liegt bereits dann vor, wenn – wie im vorliegenden Fall – leicht durch eine schnelle Recherche herausgefunden werden kann, dass der Kunde mit Waffen handelt.

Aus Sicht der Unternehmen ist dabei gar nicht eine einige Jahre später ergehende Entscheidung des *BGH* darüber interessant, ob tatsächlich Geldwäsche vorlag. Kritisch ist bereits die Einleitung eines Ermittlungsverfahrens und die (öffentlichkeitswirksame) Durchführung von Ermittlungsmaßnahmen wie Durchsuchungen. Gerade beim Leichtfertigkeitstatbestand fällt es leicht, einen Anfangsverdacht der Geldwäsche zu begründen.

5. Verpflichtungen für Güterhändler nach dem GWG

Neben dem StGB können den Güterhändler aber auch Pflichten nach dem GWG treffen. Das GWG richtet sich an einen Kreis bestimmter Verpflichteter, in erster Linie Banken. Ein Güterhändler ist jede Person, die gewerblich Güter veräußert, unabhängig davon, in wessen Namen und auf wessen Rechnung. Als Güterhändler ist man wie alle anderen verpflichtet, jedoch mit gewissen Erleichterungen. Die Kernpflichten des GWG sind das Risikomanagement, die Kundensorgfaltspflichten und die Pflicht zur Meldung von Verdachtsfällen. Der Güterhändler hat nur in zwei dieser drei Fälle einen „Emergency Exit“, denn in Hinblick auf die Meldung von Verdachtsfällen hat er ihn gerade nicht.

Tatsächlich gab es im Jahr 2017 jedoch nur eine verschwindend geringe Anzahl von Verdachtsmeldungen durch Güterhändler. Daraus könnte man nun schließen, dass bei Güterhändlern solche Verdachtsmomente nicht auftauchen und somit kein Meldebedarf besteht. Die Erfahrung zeigt aber vielmehr, dass Start-Ups, Hidden Champions und der klassische Mittelständler das Thema gar nicht auf dem Schirm haben und diese sich über ihr Risiko und ihre Verpflichtungen gar nicht bewusst sind. Die Frage ist nun, ab wann man ein Risikomanagement implementieren muss. Grundsätzlich sind alle nach dem GWG Verpflichteten davon betroffen. Somit muss ein System erstellt werden, das sicherstellt, dass man nicht zur

Geldwäsche missbraucht werden kann. Es muss dann eine Person benannt werden, die für die Implementierung zuständig ist. Erfahrungsgemäß lassen sich selten Personen dafür bereiterklären, diese Aufgabe zu übernehmen. Der Güterhändler muss aber nur dann über ein wirksames System zum Risikomanagement verfügen, wenn er im Rahmen einer Transaktion Barzahlungen über mindestens 10.000 € vor- oder entgegennimmt. Erfolgen die Zahlungen bei einem Güterhändler nur über Kryptowährungen, so sind diese nicht als Barzahlung anzusehen, so dass sich diese nicht unter eben Genanntes subsumieren lassen. Muss er allerdings ein Risikomanagement einrichten, muss seine Risikoanalyse auf die Kundenstruktur, das Kundenrisiko, das Produkt- oder Dienstleistungsrisiko sowie das geographische Risiko eingehen. Dabei ist fraglich, ob die Zahlung mit Kryptowährungen per se schon auffällig ist. Je nach Ergebnis der Risikoanalyse gilt es dann, die richtigen Maßnahmen zu treffen. Dabei wird häufig pauschal auf online verfügbare Policys zurückgegriffen, unabhängig davon, ob diese auf den konkreten Einzelfall passen oder nicht. Eine solche „Feigenblatt-Compliance" fällt den Behörden allerdings im Regelfall sehr schnell auf und wird nicht als ordnungsgemäße Aufsicht akzeptiert.

Im Bereich der Kundensorgfaltspflichten ist auch Sorgfalt im Hinblick auf Kryptowährungen geboten, etwa dann, wenn eine Verbindung zu Geldwäsche oder Terrorismus nicht auszuschließen ist. Es stellt sich dann die Frage, ob jeder Fall einer Zahlung mit Kryptowährungen schon die Gefahr von Geldwäsche indiziert. Zwar sind Kryptowährungen recht neu, allerdings stellen sie eine „normale" Art der Zahlung dar und sind somit nicht per se verdächtig. Eine KYC-Prüfung ist somit nicht schon aufgrund der Zahlung mit Kryptowährungen notwendig. Das entbindet allerdings nicht von der Pflicht, sich mit dem Geschäft seines Kunden auseinanderzusetzen, je nach Geschäftsgröße durch eine Google-Recherche oder eine Kundenanfrage, und ggf. ein Geschäft abzulehnen. Im Rahmen der verstärkten Sorgfaltspflichten ist insbesondere auf sog. PEPs (politisch exponierte Personen) oder besonders ungewöhnliche Transaktionen hinzuweisen. Hier ist ein besonderes Monitoring vonnöten. Das Gesetz lässt den Anwender letztlich im Unklaren, welche Maßnahmen genau getroffen werden müssen. Auch hier stellt sich die Frage, ob Zahlungen mit Kryptowährung als ungewöhnlich einzustufen sind und somit das Anwendungsfeld der verstärkten Sorgfaltspflichten eröffnet ist. Auch hier plädiert *Dr. Cappel* aber dafür, dass der neuartige Charakter der Kryptowährungen eine Zahlung mit ebendiesen nicht per se ungewöhnlich macht. Die Verpflichtung, Verdachtsfälle zu melden, besteht jedoch weiterhin und ist davon unberührt.

6. Drohende Konsequenzen bei Nichteinhaltung der notwendigen Compliance

Wann werden nun Compliance-Maßnahmen im Bereich der Geldwäsche notwendig? Zum einen also beim Vorliegen eines Verpflichtetenstatus und zum anderen im Rahmen des für den Güterhändler relevanteren Fall des § 261 Abs. 5 StGB (leichtfertige Geldwäsche). Für die Unternehmensleitung gilt § 130 OWiG, der von den Behörden im Geldwäschebereich schnell bejaht wird und Bußgelder bis zu 10 Millionen Euro nach sich ziehen kann. Der Bußgeldkatalog für etwaige Verstöße gegen das GWG ist in § 56 GWG geregelt, welcher Geldbußen bis 1 Million Euro, für Banken bis zu 5 Millionen oder 10 Prozent des Gesamtumsatzes festlegt.

Die Tatsache, dass die notwendigen Compliance-Maßnahmen nicht detailliert feststehen, ist einerseits schlecht für die Vorhersehbarkeit von Sanktionen, bietet aber anderseits den Unternehmen einen hohen Grad an Flexibilität. Hier sind individuelle Lösungen notwendig und möglich. Kleine und mittelständische Unternehmen können nicht die gleichen Pflichten haben wie große Banken. Individualisiert werden können Maßnahmen zur Transaktionsüberprüfung und Recherchen bezüglich der Geschäftspartner. Unternehmensintern können sog. Red Flags bestimmt werden, z.B. Zahlungen mit Kryptowährungen. Auch die Verwendung von speziellen präventiven Softwarelösungen ist möglich, aber eine Kostenfrage. Dabei ist auch im Blickfeld zu behalten, dass das Unternehmen die von ihm selbst gesetzten Maßstäbe effektiv einhalten können muss. Hier muss also mit Augenmaß gearbeitet werden und es darf nur in schwierigen Fällen vom Standardprogramm abgewichen wird.

7. Question & Answers-Session

In der Q&A-Session wurden das Verhältnis von Dokumentationspflichten und Datenschutz thematisiert und festgehalten, dass die KYC-Pflichten des GWG einen datenschutzrechtlichen Erlaubnistatbestand enthalten. Außerdem müssen im Rahmen der Pflichten gesammelte Informationen bei Vorhandensein entsprechender Eingriffsbefugnisse auch an die Strafverfolgungsbehörden herausgegeben werden. Nach Auffassung von *Dr. Cappel* gibt es kaum rechtssichere Möglichkeiten, verbindliche Auskünfte hinsichtlich der notwendigen Compliance-Maßnahmen von Behörden zu erlangen. Schließlich wurde darauf eingegangen, dass der Begriff des „Güterhändlers" auch solche Unternehmer erfasst, die ausschließlich im Endkundenvertrieb tätig sind. Besonders im Fokus der Behörden stehen dort Waren, die leicht zu Geld zu machen sind wie Autos, Schmuck, Gutscheine etc. Allerdings plädiert *Dr. Cappel* für eine maßvolle Anwendung der GWG-Bestimmungen, um nicht jeden Bereich des alltäglichen Lebens geldwäschetechnisch zu „überregulieren"

V. Resümee

Die sich an die Vorträge anschließenden interessierten Nachfragen sowie die rege Diskussion, die beim Stehempfang in lockerer Atmosphäre fortgesetzt wurde, verdeutlichen die aktuelle Brisanz und Relevanz des Tagungsthemas. Mit dem Erlanger Cybercrime Tag wurde eine Plattform für Expertinnen und Experten verschiedener Fachrichtungen sowie Interessierte geschaffen, auf der diese sich jährlich über aktuelle Entwicklungen im Bereich des Cybercrime austauschen können. *Professor Safferling* und sein Team der International Criminal Law Research Unit freuen sich, die interdisziplinäre Veranstaltungsreihe „Erlanger Cybercrime Tag" im nächsten Jahr fortzusetzen.