Landgericht Essen, 32 KLs 11/16

Datum:	03.02.2017
Gericht:	Landgericht Essen
Spruchkörper:	XII. Große Strafkammer -Wirtschaftsstrafkammer-
Entscheidungsart:	Urteil
Aktenzeichen:	32 KLs 11/16
ECLI:	ECLI:DE:LGE:2017:0203.32KLS11.16.00

Schlagworte:	Computerbetrug, Fälschung beweiserheblicher Daten, Phishing
Normen:	StGB § 263 Abs. 2, Abs. 3; § 263a Abs. 1, Abs. 2; § 267 Abs. 3;; § 269 Abs. 1, Abs. 3; § 25 Abs. 2
Sachgebiet:	Strafrecht

Tenor:

Der Angeklagte wird wegen Computerbetruges in 29 tateinheitlich zusammentreffenden Fällen, wobei es in drei Fällen beim Versuch verblieb, und wegen Fälschung beweiserheblicher Daten in 13 Fällen zu einer Gesamtfreiheitsstrafe von **4 Jahren und 6 Monaten** verurteilt.

Die in den Niederlanden erlittene Auslieferungshaft wird in einem Verhältnis von 1:1 auf die verhängte Freiheitsstrafe angerechnet.

Der Angeklagte trägt die Kosten des Verfahrens.

Angewendete Vorschriften: §§ 263 Abs. 2, Abs. 3 Nr. 1 Alt. 1, 263a Abs. 1, Abs. 2, 267 Abs. 3 Nr. 1 Alt. 1, 269 Abs. 1, Abs. 3, 22, 23 Abs. 1, 25 Abs. 2, 51 Abs. 4 S. 2, 52, 53 StGB

Gründe: 1

Vorspann: 2

Der Angeklagte war im Tatzeitraum Mitglied einer internationalen Tätergruppe, deren Ziel es war, durch Verwendung sogenannter „Phishingmails“ Zugangsdaten von Bankkunden aus verschiedenen europäischen Ländern zu erlangen und sodann unter Verwendung dieser 3

Zugangsdaten – täuschungsgleich – Überweisungen von den Kundenkonten auf Drittkonten zu veranlassen. Diese Drittkonten waren durch sogenannte „Finanzagenten“ und teilweise unter Verwendung falscher Personalien eröffnet worden und erlaubten den Tätern so den Zugriff auf die transferierten Gelder. Zu der Tätergruppierung gehörten neben dem Angeklagten u.a. die gesondert Verfolgten V und H sowie weitere namentlich nicht bekannte Telefonisten /-innen. Das Vorgehen der Gruppe erfolgte arbeitsteilig, organisiert und – schon mit Blick auf die notwendige technische Ausstattung und das erforderlich Fachwissen – professionell.

Die Aufgabe des Angeklagten bestand – entsprechend dem gemeinsamen Tatplan – darin, von ihm oder durch Dritte erstellte Phishingmails, die den Eindruck erweckten, von „echten“ Banken zu stammen, massenhaft an potentielle Bankkunden, deren Emailadressen er sich zuvor beschafft hatte, zu versenden. Durch einen in den Emails enthaltenen Link wurden die Kunden auf durch die Tätergruppe erstellte Internetseiten geleitet, auf denen diese Kunden zur Eingabe persönlicher Daten aufgefordert wurden. Diese Seiten wurden auf verschiedenen Servern platziert („gehostet“), auf welche sich die Täter unberechtigten Zugriff verschafft hatten. Wie von dem Angeklagten und seinen Mittätern geplant, wurden die Daten der Bankkunden sodann über auf den Seiten hinterlegte, sogenannte „php-Skripte“ zu verschiedenen Email-Postfächern geleitet, auf welche der Angeklagte Zugriff nehmen konnte. Seine weitere Aufgabe bestand darin, die auf diese Art und Weise „abgephishten“ Daten auszuwerten und durch einen ersten Zugriff auf das Onlinebanking des Kunden weitere Informationen – etwa hinsichtlich des verfügbaren Guthabens oder des verwendeten Sicherungsverfahrens – zu erlangen. 4

Um nunmehr an für Transaktionsnummer(TAN)-pflichtige Vorgänge – wie etwa Überweisungen oder die Änderung der hinterlegten Rufnummer im Rahmen des sogenannten SMS-TAN-Verfahrens – erforderliche TANs zu gelangen, bediente sich der Angeklagte der Hilfe der gesondert Verfolgten H und weiterer Telefonisten /-innen. Zumindest an die gesondert Verfolgte H leitete der Angeklagte Kundendaten und Informationen zu Kontoständen und TAN-Verfahren weiter, wobei nicht aufgeklärt werden konnte, ob die Weiterleitung in einem Vorgang als „Datenpaket“ oder in – und wenn in wie vielen – einzelnen Datensätzen erfolgte. Die Aufgabe der Telefonisten /-innen bestand darin, die Kunden anzurufen und diese unter Vorspiegelung falscher Tatsachen zur Herausgabe einer TAN zu veranlassen. Mit dieser TAN wurden durch die Täter sodann unautorisierte Überweisungen entweder direkt vorgenommen oder durch Änderung der Rufnummer im SMS-TAN-Verfahren eine eigene Empfangsberechtigung für TANs geschaffen. Sämtliche verfahrensgegenständlichen Überweisungen wurden durch ein Mitglied der Tätergruppe mit Wissen und Billigung auch des Angeklagten durchgeführt. 5

Im Einzelnen gelang es der Tätergruppe auf die zuvor dargelegte Weise in den angeklagten Fällen zu Tatkomplex A – nach Teileinstellungen verblieben insoweit noch 29 verfahrensgegenständliche Taten – Überweisungen in einer Höhe von insgesamt ca. 160.000,00 € auszuführen. Eine Rückbuchung des Geldes war nur in drei Fällen – namentlich Fällen 3, 23 und 25 (Fälle A3, A21 und A28 der Anklageschrift vom 31.08.2016) – möglich. Wo ansonsten erfolgreich überwiesene Gelder letztlich verblieben sind und in welcher Höhe der Angeklagte hinsichtlich der festgestellten Taten konkret partizipiert hat, konnte nicht aufgeklärt werden. Sicher festzustellen war jedoch, dass der Angeklagte beabsichtigte, aus der wiederholten Begehung der Taten eine fortdauernde Einnahmequelle zu erzielen, und dass seine Mitwirkung für ihn mit finanziellen Vorteilen verbunden war. 6

7

Im Tatkomplex B verblieben nach Teileinstellungen betreffend die Versendung weiterer Phishingmails an potentielle Kunden der portugiesischen Q sowie der Schweizer Q1 13 Taten, in denen auf die vorgenannte Art und Weise durch den Angeklagten massenhaft Phishingmails an potentielle Kunden der niederländischen S sowie der J Bank und an Kunden der Q1 versendet wurden.

Der Angeklagte hat die Begehung der Taten pauschal in Abrede gestellt, ohne Fragen der Kammer zur Sache zu beantworten. Er konnte der Beteiligung an den festgestellten Taten – hinsichtlich des Tatkomplexes A im Sinne der Mittäterschaft (§ 25 Abs. 2 StGB) – jedoch infolge der durchgeführten Beweisaufnahme – insbesondere der Aussagen der betroffenen Bankkunden und ermittelnden Polizeibeamten sowie der umfassenden Auswertung von TKÜ-Maßnahmen und bei ihm sichergestellten Asservaten – überführt werden. Einzelne Erkenntnisse ergänzten und verstärkten sich bei der gebotenen Gesamtschau dabei zu einem Gesamtbild, welches an den festgestellten Taten und der Beteiligung des Angeklagten keine begründeten Zweifel ließ. 8

I. Feststellungen zur Person 9

Der am … nach eigenen Angaben in O im Südsudan geborene Angeklagte wuchs als Einzelkind bei seinen Eltern – von denen nicht geklärt werden konnte, ob sie aus dem Sudan stammen – auf und besuchte den Schulunterricht, der in einer Kirche des Dorfes erteilt wurde. Nebenbei wurde er von seinen Eltern, die gebildet waren, unterrichtet. Nach dem Tod seiner Eltern reiste er im Alter von 15 oder 16 Jahren allein und ohne Ausweisdokumente über Libyen in die Niederlande ein, beantragte dort Asyl und besuchte die Schule. Sodann arbeitete er für zweieinhalb bis drei Jahre bei einem Verpackungsunternehmen namens „J1“. Im Jahr 2013 besuchte er eine „Taxischule“, um eine Taxilizenz zu erhalten. Nach Erhalt der Lizenz genügten seine finanziellen Mittel zunächst nicht, um sich ein Taxi zu kaufen. Nachdem er zu Geld gekommen war, kaufte er sich noch im Jahr 2013 ein eigenes Taxi und arbeitete mit diesem, bis es im Jahr 2014 defekt war und er aufgrund dessen sein Taxiunternehmen aufgab. Seither bezog der Angeklagte bis zu seiner Festnahme am 09.04.2016 Sozialleistungen in Höhe von 400,00 € monatlich zuzüglich der ebenfalls durch den niederländischen Staat übernommenen Miete in Höhe von 600,00 €. Vor seiner Verhaftung hatte der Angeklagte sich bei dem Taxiunternehmen V1 als Fahrer angemeldet, jedoch diese Tätigkeit bis zu jenem Zeitpunkt noch nicht aufgenommen. Neben seinem amtlichen Vornamen N wird der Angeklagte auch mit dem Namen „N1“ angeredet; auch tritt er im Freundes- und Bekanntenkreis selbst unter diesem Namen auf. 10

In den Niederlanden lebte der Angeklagte zunächst allein in F und zuletzt für etwa 12 bis 13 Jahre in einer Zweizimmerwohnung in der W-Straat … in S1. Seinen Aufenthaltstitel für die Niederlande musste er alle 5 Jahre erneuern lassen. Er verfügt über einen niederländischen Reisepass. 2015 erhielt der Angeklagte ein Formular zu Beantragung der niederländischen Staatsbürgerschaft, welches er jedoch nicht einreichte. Der Angeklagte spricht und schreibt neben Englisch auch Pidgin-Englisch, eine u.a. in Nigeria gebräuchliche Abwandlung der englischen Sprache. 11

Etwa 2010 oder 2011 lernte der Angeklagte J2, die die nigerianische Staatsbürgerschaft hat, auf einer Geburtstagsfeier in den Niederlanden kennen. Sie lebte zu dieser Zeit in T und zog zum 01.12.2014 gemeinsam mit ihren drei Kindern – D, die derzeit 7 oder 8 Jahre alt ist, N2, derzeit 4 Jahre, und X, derzeit 3 Jahre – in eine Wohnung in der A-Straße … in F1. Dort besuchte der Angeklagte jeweils für Zeiträume von 4 bis 5 Tagen sowohl Frau J2 als auch ihre beiden gemeinsamen Kinder N2 und X. Seine Kinder N2 und X besuchten ihn auch gelegentlich in seiner Wohnung in S1. 12

Der Angeklagte ist strafrechtlich bereits in Erscheinung getreten: Unter dem 14.06.2012 – rechtskräftig seit dem 14.07.2012 – erließ das Amtsgericht F1 gegen ihn im Verfahren … wegen Beleidigung einen Strafbefehl über eine Geldstrafe von 20 Tagessätzen zu je 10,00 €. 13

In der vorliegenden Sache wurde der Angeklagte aufgrund des Haftbefehls des Amtsgerichts C vom 08.03.2016 (…) in Verbindung mit dem Europäischen Haftbefehl der Staatsanwaltschaft C1 vom 21.03.2016 (…) am 09.04.2016 in S1 in den Niederlanden festgenommen und befand sich vom 09.04.2016 bis zum 30.06.2016 in Auslieferungshaft in den Niederlanden. Sodann befand er sich bis zum Beginn der Hauptverhandlung in Untersuchungshaft in der JVA C2 und zwischen dem 30.09.2016 und dem 25.11.2016 im Justizvollzugskrankenhaus G sowie in Krankenhäusern in V2 und E. Mitte Oktober 2016 unterzog sich der Angeklagte einer Bypass-Operation. 14

Die Kammer ist zudem von Folgendem ausgegangen: Zum Zwecke der Wahrnehmung von insgesamt 13 Sitzungstagen des hiesigen Hauptverfahrens in der Zeit zwischen dem 30.11.2016 und dem 03.02.2017 wurde er regelmäßig zur JVA F3 verbracht. In dem vorbenannten Zeitraum befand sich der Angeklagte daher nahezu durchgehend auf Transportabteilungen und nicht in einem ihm ordnungsgemäß zugewiesenen Haftraum. Zudem war es infolge der ständigen Verschubungen in diesem gesamten Zeitraum nicht möglich, ihm Besuch von Privatpersonen zu gewähren. Auf Nachfrage bei der Staatsanwaltschaft C1 wurde zwischenzeitlich unzutreffend mitgeteilt, dass der Angeklagte sich in der JVA in E befände. Infolge des Umstands, dass der Angeklagte der deutschen Sprache nicht mächtig ist, war und ist es für ihn besonders erschwert, innerhalb des Vollzugs mit Mitgefangenen oder auch Bediensteten der JVA in Kontakt zu treten. 15

II. Feststellungen zur Sache 16

1. Arbeitsweise der Tätergruppierung 17

Der Angeklagte war Mitglied einer europaweit agierenden Tätergruppierung, die sich auf unbestimmte Zeit zusammengeschlossen hatte, um einer Vielzahl von Bankkunden u. a. in Deutschland, der Schweiz und den Niederlanden im Wege des sog. „Phishings“ die erforderlichen Daten zur Ausführung von Online-Überweisungen – insbesondere Kontoverbindungen, Online-Banking-Account-Zugangsdaten und Transaktionsnummern (TAN) – abzulisten. Unter Verwendung der derart erlangten Daten wurden sodann ohne Wissen und Willen der Bankkunden von deren Bankkonten Geldbeträge auf Bankkonten sog. „Finanzagenten“ im In- und Ausland bzw. auf zu diesem Zweck unter falscher Identität eröffnete Konten überwiesen oder Geldbeträge auf andere Weise zugunsten der Tätergruppe – etwa an die X1 GmbH – transferiert. Ziel der Täter – insbesondere auch des Angeklagten – war es, so Zugriff auf die Geldbeträge zu erlangen und sich hierdurch eine nicht nur vorübergehende, erhebliche Einnahmequelle zu verschaffen. Neben dem Angeklagten waren zumindest die gesondert Verfolgte H, namentlich nicht bekannte Telefonisten /-innen und der gesondert Verfolgte V Teil der Tätergruppierung. Die Kommunikation innerhalb der Tätergruppe erfolgte häufig über Z-Chats, bei denen der Angeklagte als „L“, die gesondert Verfolgte H als „Q2“ und der gesondert Verfolgte V als „X2“ auftraten. 18

Zur Umsetzung des gemeinsamen Tatplans ging die Tätergruppe arbeitsteilig wie folgt vor: 19

Zunächst durchsuchte der Angeklagte mittels spezieller Computerprogramme das Internet nach Emailadressen möglicher Empfänger von Phishingmails. Sodann bestand seine Aufgabe darin, von ihm oder durch Dritte erstellte Phishingmails massenhaft an die zuvor erlangten Emailadressen zu versenden. Die Emails sollten – wozu sie ihrer Aufmachung und 20

ihrem Inhalt nach zumindest hinsichtlich der hier in Rede stehenden T1-, Q1-, S- und J-Emails auch geeignet waren – bei den Empfängern den Eindruck erwecken, von ihrem Bankinstitut zu stammen. In den Emails wurden die Empfänger stets unter einem Vorwand – etwa, dass der Online-Banking-Zugang aktualisiert und/oder ein Sicherheitsupdate durchgeführt werden müsse – aufgefordert, einem in der Email enthaltenen Link zu folgen.

Auf der durch den jeweiligen Link erreichten Seite wurden die Emailempfänger aufgefordert, persönliche Daten, wie Namen, Anschrift, Geburtsdatum, Telefon- und Mobilfunknummer und Emailadressen, aber auch Online-Banking-Zugangsdaten, E-Finance-Nummern, Benutzeridentifikationen und Passwörter einzugeben. Diese Seiten, die von der Tätergruppe, hauptsächlich von dem gesondert Verfolgten V, erstellt und von diesem in Zusammenarbeit mit dem Angeklagten auf fremden Servern platziert worden waren, waren von der Tätergruppe mit sog. „php-Skripten“ hinterlegt, wodurch die dort eingegebenen Daten in Emailpostfächer der Tätergruppe, auf die der Angeklagte Zugriff nehmen konnte, geleitet wurden. Der Angeklagte wertete die Daten aus und beschaffte teilweise durch Zugriffe auf die entsprechenden Konten weitere Daten etwa zum Guthaben oder dem TAN-Verfahren. Hieraus erstellte er Datensätze, die er – wobei nicht festgestellt werden konnte, in wie vielen einzelnen Vorgängen – auch an die gesondert Verfolgte H weiterleitete. Wenn auch nicht festgestellt werden konnte, dass der Angeklagte hiernach eigenhändig unbefugte Überweisungen vornahm, steuerte er gleichwohl maßgeblich das weitere Geschehen, zumal er derjenige war, der den gesondert Verfolgten V und der Telefonistin Anweisungen erteilte. So gab er dem gesondert Verfolgten V konkrete Arbeitsaufträge unter Mitteilung von Internetseiten, auf welche gefälschte Bankseiten hochgeladen werden sollten, und hielt ihn dazu an, seiner Aufgabe nachzukommen. Dieser wiederum teilte dem Angeklagten die Ergebnisse seiner Arbeit mit und bat ihn um Überprüfung. Gegenüber der gesondert Verfolgten H erteilte er Anweisungen, Anrufe durchzuführen und teilte ihr hierzu Bankdaten nebst Online-Banking-Zugangsdaten mit. Auch war er derjenige, mit dem die gesondert Verfolgte H über ihren finanziellen Anteil diskutierte. Dieser wurde letztlich vom Angeklagten bestimmt. 21

Die Aufgabe der zur Tätergruppe gehörenden Telefonisten /-innen – insbesondere auch der gesondert Verfolgten H – bestand darin, die Personen, deren Daten von dem Angeklagten übersandt worden waren, anzurufen und unter Vorspiegelung falscher Tatsachen zur Herausgabe einer TAN zu veranlassen. Weiterhin sollten sie die Angerufenen dazu zu bringen, für einen gewissen Zeitraum nicht auf ihr Online-Banking-Account zuzugreifen, um so zu verhindern, dass von der Tätergruppe veranlasste Überweisungen rechtzeitig von dem Konteninhaber zurückgerufen würden. Die Telefongespräche wurden nahezu formalisiert anhand von Gesprächsleitfäden der Tätergruppe geführt. Nachdem die jeweilige Telefonistin bzw. der jeweilige Telefonist sich als Bankmitarbeiter – die gesondert Verfolgte H regelmäßig unter dem Namen „E1“ – oder als von einem Callcenter der Bank anrufend vorgestellt hatte, wurde zunächst der vermeintliche Grund des Anrufs – in der Regel die Durchführung einer Aktualisierung und/oder eines Sicherheitsupdates – benannt. Sodann wurde ein Datenabgleich durchgeführt, um den angerufenen Konteninhabern zu suggerieren, dass es sich tatsächlich um einen Anruf der Bank handele. Ebenfalls zu diesem Zweck nutzte die Tätergruppe die Dienste der Firma W1. Diese vermietet lokale Rufnummern, die mit dem eigentlichen Telefonanschluss derart verbunden werden, dass nicht die tatsächliche Rufnummer bei Anrufen angezeigt wird, sondern die gemietete, über die der Anruf durchgeleitet wird. Hierdurch war es möglich, dass anstelle der tatsächlichen Anrufernummer der Tätergruppe bei dem Angerufenen die bei der Firma W1 für diese als anzuzeigende Nummer gemietete Nummer – für Anrufe der Tätergruppe bei Konteninhabern in Deutschland zumeist eine mit „0800“ beginnende und hierdurch den Anschein einer Service-Nummer 22

erweckende Nummer – angezeigt wurde.

Der weitere Verlauf des Telefonats und der Handlungen der Telefonisten /-innen war sodann – jeweils mit Wissen und Billigung der übrigen Mitglieder der Tätergruppe – abhängig davon, ob der jeweilige Anrufer das sog. „Chip-TAN-Verfahren“ oder das sog. „SMS-TAN-Verfahren“ nutzte. Bei Verwendung des „Chip-TAN-Verfahrens“ wird mittels eines Generators mit eingesteckter Kontokarte durch Halten vor ein Flackerbild am Computerbildschirm innerhalb des Online-Banking-Accounts oder durch manuelle Eingabe eines Sicherheitscodes und weiterer Angaben, die sich nach dem beabsichtigten TAN-pflichtigen Vorgang richten, eine TAN generiert und auf dem Generator angezeigt. Bei Verwendung des SMS-TAN-Verfahrens wird im Falle der Anforderung einer TAN für einen TAN-pflichtigen Vorgang diese per SMS an eine im Online-Banking-Account hierfür hinterlegte Mobilfunknummer gesendet. 23

Im erstgenannten Fall („Chip-TAN-Verfahren“) hatte der jeweilige Telefonist bzw. die jeweilige Telefonistin bis zu diesem Zeitpunkt bereits mit den erlisteten Daten Zugriff auf das Online-Banking-Account des Angerufenen genommen und dort eine Überweisung vorbereitet. Weiterhin hatte er/sie dort angegeben, dass manuell eine TAN mit dem Generator erzeugt werden solle, woraufhin ihm/ihr ein in den Generator einzugebender achtstelliger Sicherheitscode angezeigt wurde. Im Telefonat wurde der jeweilige Konteninhaber aufgefordert, den TAN-Generator zur Hand zu nehmen, die Kontokarte hinein zu stecken und auf die TAN-Taste zu drücken. Sodann sollten der von dem Telefonisten/der Telefonistin vorgegebene achtstellige „Code“, die ebenfalls vorgegebenen letzten 10 Ziffern der Empfänger-IBAN der vorbereiteten Überweisung sowie der durchgegebene Überweisungsbetrag – wobei jeweils nicht angegeben wurde, was sich tatsächlich hinter den Ziffernfolgen verbarg – eingegeben und jeweils bestätigt werden. Die hierdurch manuell generierte TAN – die die Konteninhaber unwissentlich erzeugt hatten und zumeist nicht als solche erkannten – wurde dem Kontoinhaber auf dem Generator angezeigt und auf Aufforderung des Telefonisten/der Telefonistin durchgegeben. Hierdurch konnte diese/r die Überweisung unter Vorspiegelung einer tatsächlich nicht gegebenen Legitimation gegenüber der datenverarbeitenden Stelle freigeben. Der Konteninhaber wurde sodann regelmäßig darauf hingewiesen, dass er sein Online-Banking zunächst, in der Regel für 24 Stunden, nicht nutzen könne, um hierdurch das Entdecken und einen möglichen rechtzeitigen Rückruf der unautorisierten Überweisung zu verhindern. 24

Im zweitgenannten Fall („SMS-TAN-Verfahren“) hatte der jeweilige Telefonist bzw. die jeweilige Telefonistin bis zu diesem Zeitpunkt bereits mit den erlisteten Daten Zugriff auf den Online-Banking-Account des Angerufenen genommen. Dort wurde entweder eine Überweisung nach o.g. Muster oder eine Änderung der Mobilfunknummer für den Empfang von TANs per SMS auf eine eigene Rufnummer vorbereitet, was ebenso wie eine Überweisung ein TAN-pflichtiger Vorgang ist. Im Telefonat gab er/sie gegenüber dem Konteninhaber sodann an, dass diesem eine SMS mit einem „Code“ zugeleitet würde, der durchgegeben werden müsse. In diesem Moment forderte der Telefonist/die Telefonistin für die Überweisung oder Nummernänderung im Online-Banking des Angerufenen eine TAN an, die auf das Handy des Angerufenen per SMS versendet wurde. Nach Durchgabe der – als solche regelmäßig nicht von den Angerufenen erkannten – TAN gab der Telefonist/die Telefonistin diese im Online-Banking-Account des Angerufenen unter Vorspiegelung einer tatsächlich nicht gegebenen Legitimation gegenüber der datenverarbeitenden Stelle ein und gab die Überweisung hiermit frei bzw. änderte hiermit die hinterlegte Mobilfunknummer. In letzterem Fall wurden seitens der Tätergruppe sodann weitere nicht autorisierte Überweisungen von dem Konto des Bankkunden getätigt, wobei die hierfür erforderlichen TANs jeweils auf die zuvor geänderte eigene Mobilfunknummer per SMS gesendet wurden. 25

Ob solche Überweisungen auch durch den Angeklagten selbst ausgeführt wurden, konnte nicht sicher festgestellt werden. Auch in diesen Fällen endeten die Telefonate zumeist mit dem Hinweis, dass der Online-Banking-Account zunächst nicht genutzt werden könne, um eine Entdeckung und einen rechtzeitigen Rückruf der unautorisierten Überweisungen zu verhindern.

2. Die einzelnen Taten 26

Nachdem das Verfahren hinsichtlich der Fälle A4, A13, A27, B8, B10, B11, B12 und B18 der Anklageschrift vom 31.08.2016 eingestellt wurde, beruht der Schuldspruch auf den Feststellungen zu folgenden einzelnen Vorgängen: 27

a) 28

Tatkomplex A: Nutzung der durch Phishing erlangten Daten für Überweisungen zu Lasten von getäuschten T1-Kunden 29

Es gelang der Tätergruppe in der vorbeschriebenen Art und Weise bundesweit Daten von Kunden verschiedener T1 zu erlangen und Überweisungen von Konten der Kunden in einer Höhe von insgesamt ca. 160.000,00 € auszuführen. 30

Hierzu versandte die Tätergruppe eine Email folgenden oder ähnlichen Inhalts, wobei als Absender der Email etwa „T1 Online-Banking <…>“ oder „T1 Online-Banking <…>“ ausgewiesen wurden: 31

„Sehr geehrter T1 Kunde, 32

Bitte beachten Sie, dass Ihr online-Banking-Zugang bald ablaeuft. Um diesen Dienst weiterhin nutzen zu koennen, klicken Sie bitte auf den untenstehenden Link um Ihren Zugang manuell mit unserem Sicherheits-Update zu aktualisieren. 33

Zur Aktualisierung 34

Online Banking ist mit einem umfassenden Sicherheitssystem ausgestattet, das gewaehrleistet, dass Ihre persoenlichen Daten von Unbefugten nicht entschluesselt oder verändert werden können. 35

Nach Vervollstaendigung dieser Schritte werden Sie von einem Mitarbeiter unseres Kundendienstes zum Status Ihres Kontos telefonisch kontaktiert um den Updatevorgang abzuschliessen. 36

Bankgeschäfte immer dort, wo Sie sind! 37

Verwalten Sie Ihre Konten/Depots online und erledigen Sie Ihre Bankgeschäfte einfach, schnell und sicher vom Buero oder von Zuhause aus. Unabhaengig von Öffnungszeiten - 24 Stungen am Tag, an 365 Tagen im Jahr. Alles, was Sie benoetigen, ist ein Internetzugang und die Freischaltung Ihres Kontos oder Wertpapierdepots für Ihr Online Banking der T1. 38

Mit freundlichen Grüssen 39

Ihre T1 40

Sicherheitsabteilung.“ 41

42

Der Angeklagte war hinsichtlich sämtlicher Taten in der vorbezeichneten Art und Weise – namentlich durch vorherige Versendung der Phishingmail, Auswertung und Weitergabe der erlisteten Daten der betroffenen T1-Kunden an die jeweilige Telefonistin sowie Benennung des jeweiligen Empfängerkontos – konkret beteiligt.

Wo die transferierten Gelder letztlich verblieben und ob und in welcher Höhe der Angeklagte hinsichtlich der festgestellten Taten konkret finanziell partizipiert hat, konnte nicht aufgeklärt werden. Sicher festzustellen war jedoch, dass er beabsichtigte, sich aus der wiederholten Begehung der Taten eine nicht nur vorübergehende Einnahmequelle zu verschaffen und dass seine Mitwirkung für ihn mit finanziellen Vorteilen verbunden war. 43

Im Einzelnen kam es so zu folgenden Taten: 44

Fall 1 – G1 (Fall A1 der Anklageschrift) 45

Am 02.09.2014 rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe den Zeugen G1 gegen 09:00 Uhr von der Nummer … aus an. Unter der Vorspiegelung, es müsse ein Aktualisierungs-Update für sein Onlinekonto, welches er bei der T2 im Chip-TAN-Verfahren führte, durchgeführt werden, brachte sie den Zeugen – entsprechend dem Tatplan der Tätergruppe – dazu, seine EC-Karte in seinen Chip-TAN Generator einzustecken, einen achtstelligen „Code“ – nämlich einen Sicherheitscode zur manuellen Generierung einer TAN – sowie weitere Zahlenfolgen einzugeben und ihr die hierdurch generierte TAN – … – durchzugeben. Bei den weiteren Zahlenfolgen handelte es sich zum Einen um die letzten zehn Ziffern der Empfänger-IBAN einer Überweisung an einen L1 in Großbritannien, IBAN …, die sie im Online-Banking-Account des Zeugen vorbereitet hatte, nachdem sie sich hierzu mittels der in der eingangs dargelegten Weise abgephishten Daten des Zeugen Zugang verschafft hatte. Zum anderen handelte es sich um den eingegebenen Überweisungsbetrag in Höhe von **2.000,00 €**. Die gesondert Verfolgte H bzw. die Telefonistin gab die TAN – da eine Überweisung ein TAN-pflichtiger Vorgang ist – ein und sandte die vorbereitete Überweisung ab. Die Überweisung wurde ausgeführt und das Konto in Höhe des genannten Betrages belastet. Das Telefonat endete mit dem Hinweis, dass der Zeuge für 24 Stunden nicht auf sein Online-Banking-Account zugreifen könne. 46

Eine Rückbuchung des transferierten Geldes konnte nicht veranlasst werden; der Überweisungsbetrag wurde dem Zeugen jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 47

Am 20.11.2014 rief die gesondert Verfolgte H den Zeugen G1 (erneut) an und stellte sich als Mitarbeiterin des „T1 Online Banking“ namens „E1“ vor. Unter Bezugnahme auf ein zuvor geführtes Telefonat des Zeugen mit ihrer Kollegin gab sie an, dass es um die Aktualisierung des Online-Bankings gehe, woraufhin der Zeuge das Gespräch abbrach. 48

Fall 2 – I (Fall A2 der Anklageschrift) 49

Am 10.09.2014 gegen 12:00 Uhr rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe die Zeugin I an und stellte sich ihr als Mitarbeiterin der C3, bei der die Zeugin ein Geschäftskonto und ihr privates Konto hatte, vor. Bereits zuvor hatte die Zeugin, welche das SMS-TAN-Verfahren nutzte, von der Nummer … aus am 03.09.2014 einen Anruf erhalten. Unter dem Vorwand, dass es um eine Aktualisierung des Online-Bankings gehe, brachte sie die Zeugin im Telefonat am 10.09.2014 – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten – dazu, ihr die auf ihr Handy gesandte Nummer anzugeben. Hierbei handelte es sich um eine TAN, die der Zeugin 50

im Rahmen des SMS-TAN-Verfahrens auf ihr Handy geleitet wurde, nachdem die Telefonistin sich mit den abgephishten Daten der Zeugin Zugang zu deren Online-Banking-Account verschafft und dort eine Änderung der Empfängernummer für TANs vorbereitet und während des Telefonats für diese Änderung – die ein TAN-pflichtiger Vorgang ist – eine TAN angefordert hatte. Sodann gab die Anruferin die von der Zeugin herausgegebene TAN in deren Online-Banking-Account ein und änderte hiermit die SMS-Empfängernummer für TANs auf die von der Tätergruppe hierfür genutzte Nummer …. Das Telefonat endete mit dem Hinweis, dass die Zeugin die erhaltene SMS sofort löschen solle, was sie tat. Unmittelbar nach dem Gespräch bereitete die Anruferin im Online-Banking-Account der Zeugin eine Überweisung in Höhe von **4.000,00 €** an einen I1 in Polen, IBAN …, vor, forderte eine TAN an, die auf die zuvor geänderte Empfängernummer geleitet wurde, und führte die Überweisung um 12:12:14 Uhr aus. Eine weitere Überweisung wurde mittels einer weiteren angeforderten TAN am selben Tag um 14:45:52 in Höhe von **1.479,00 €** an einen P in Spanien, IBAN …, ausgeführt.

Eine Rückbuchung des transferierten Geldes konnte nicht veranlasst werden; der Überweisungsbetrag wurde der Zeugin jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 51

Fall 3 – I2 (Fall A3 der Anklageschrift) 52

Am 29.09.2014 gegen 15:38 Uhr rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe die Zeugin I2 von der Nummer … aus an und stellte sich ihr als Mitarbeiterin der T3 vor. Die Zeugin verwaltete ihr Konto bei der T3 online im SMS-TAN-Verfahren. Unter dem Vorwand, dass es um ein Sicherheitsupdate und einen Datenabgleich gehe, brachte sie die Zeugin – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten – dazu, ihr die auf ihr Handy gesandte Nummer - … - anzugeben. Tatsächlich handelte es sich um eine TAN, die der Zeugin im Rahmen des SMS-TAN-Verfahrens auf ihr Handy geleitet wurde, nachdem die Anruferin sich mit den zuvor entsprechend der eingangs dargelegten Vorgehensweise der Tätergruppe abgephishten Daten der Zeugin Zugang zu deren Online-Banking-Account verschafft und dort eine Überweisung über einen Betrag in Höhe von **2.312,00 €** an einen G2 in Italien, IBAN …, vorbereitet und während des Telefonats für diese Überweisung eine TAN angefordert hatte. Um 15:41 Uhr gab die Anruferin die Überweisung unter Verwendung der von der Zeugin erlisteten TAN in deren Online-Banking-Account frei. Das Telefonat endete mit dem Hinweis der Anruferin, dass die Zeugin 24 Stunden lang nicht auf ihr Online-Banking zugreifen könne. 53

Als sich die Zeugin unmittelbar nach dem Telefonat in ihr Online-Banking einloggte, war die Überweisung bereits ausgeführt und das Konto in gleicher Höhe belastet. Aufgrund der schnellen Aufdeckung der Tat konnte das Geld jedoch im weiteren Verlauf zurückgebucht werden. 54

Fall 4 – T4 (Fall A5 der Anklageschrift) 55

Am 29.09.2014 um 16:40 Uhr rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe die Zeugin T4 von der Nummer … aus an und stellte sich ihr als Mitarbeiterin der T1 vor. Die Zeugin verwaltete ihr Konto bei der M online im SMS-TAN-Verfahren. Die Anruferin gab vor, dass es um eine Aktualisierung des Online-Bankings gehe. Da die Zeugin am 29.09.2014 keine Zeit für ein Telefonat hatte, verabredete man sich zu einem Telefonat am 30.09.2014 um 14:00 Uhr. Nachdem die Zeugin einen weiteren Anruf nicht entgegen genommen hatte, wurde sie am 01.10.2014 um 15:45 Uhr – nunmehr von der Nummer … – zum Zweck des „Datenabgleichs“ von der Telefonistin 56

angerufen. Diese brachte die Zeugin – entsprechend dem gemeinsamen Tatplan – dazu, ihr die auf ihr Handy gesandte sechsstellige Nummer anzugeben. Hierbei handelte es sich tatsächlich um eine TAN, die der Zeugin im Rahmen des SMS-TAN-Verfahrens auf ihr Handy geleitet wurde, nachdem die Anruferin sich mit den zuvor abgephishten Daten Zugang zu dem Online-Banking-Account verschafft, dort eine Änderung der Empfängernummer für TANs vorbereitet und während des Telefonats für diese Änderung eine TAN angefordert hatte. Mit der so abgelisteten TAN wurde die Empfängernummer auf eine von der Tätergruppe hierfür verwendete Rufnummer geändert. Das Telefonat endete mit den Hinweisen, dass die Zeugin ihr Online-Banking-Account einen Tag nicht nutzen und die erhaltene SMS löschen solle, was sie tat.

Am 02.10.2014 wurden von einem Mitglied der Tätergruppe sodann zur Ausführung von Überweisungen zwei TANs – … und … – generiert, mit denen Überweisungen an N3 in Portugal, IBAN …, in Höhe von **4.887,00 €** und an eine K in Spanien, IBAN …, in Höhe von **3.555,00 €** ausgeführt wurden. 57

Eine Rückbuchung der transferierten Gelder konnte nicht veranlasst werden; der jeweilige Überweisungsbetrag wurde der Zeugin jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 58

Fälle 5 und 6 – X3 (Fälle A6 und A7 der Anklageschrift) 59

Am 29.10.2014 um 12:50:24 Uhr rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin den Zeugen X3 von der Nummer … aus an und stellte sich ihm als Mitarbeiterin der C3 vor. Der Zeuge verwaltete sein Konto bei der C3 online im SMS-TAN-Verfahren. Unter dem Vorwand, dass es um eine Wartung des Online-Bankings gehe, brachte sie den Zeugen – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten – dazu, ihr die auf sein Handy gesandte Nummer anzugeben. Hierbei handelte es sich tatsächlich um eine TAN, die dem Zeugen im Rahmen des SMS-TAN-Verfahrens auf sein Handy geleitet wurde, nachdem die Anruferin sich mit den zuvor entsprechend der eingangs dargelegten Vorgehensweise der Tätergruppe abgephishten Daten des Zeugen Zugang zu dessen Online-Banking-Account verschafft, dort eine Änderung der Empfängernummer für TANs vorbereitet und während des Telefonats für diese Änderung eine TAN angefordert hatte. Sodann gab die Anruferin die von dem Zeugen herausgegebene TAN in dessen Online-Banking-Account ein und änderte hiermit um 12:53:10 Uhr die SMS-Empfängernummer für TANs auf die von der Tätergruppe hierfür genutzte Nummer … . 60

Unmittelbar nach dem Gespräch am 29.10.2014 **(Fall 5)** gab sie im Online-Banking-Account des Zeugen zunächst eine Überweisung in Höhe von **5.000,00 €** an einen D1 in Italien, IBAN …, ein, forderte eine TAN an, die auf die zuvor geänderte Rufnummer geleitet wurde, und führte die Überweisung um 13:03:10 Uhr unter Verwendung der TAN und Vorspiegelung ihrer in Wahrheit nicht gegebenen Berechtigung aus. Noch am selben Tag folgte in vorbeschriebener Art und Weise eine weitere Überweisung in Höhe von **5.000,00 €** an „E2“ in Polen, IBAN … . 61

Am 30.10.2014 **(Fall 6)** folgte in entsprechender Vorgehensweise eine weitere Überweisung an „N4“ in Polen, IBAN …, in Höhe von **9.950,00 €**. Zwischenzeitlich teilte die Telefonistin dem Zeugen zweimal telefonisch mit, dass die Wartungsarbeiten andauerten, um weitere unautorisierte Überweisungen durchführen zu können. 62

Das Konto des Zeugen wurde jeweils in der zuvor genannten Höhe belastet. Eine Rückbuchung des transferierten Geldes konnte nicht veranlasst werden; der 63

Überweisungsbetrag wurde dem Zeugen jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt.

Eine weitere Überweisung am 31.10.2014 in Höhe von 9.950,00 € an einen B konnte durch die Bank gestoppt werden, so dass es in diesem Fall nicht zu einer Abbuchung kam. 64

Fall 7 – N5 (Fall A8 der Anklageschrift) 65

Am 05.11.2014 rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe den Zeugen N5 um 15:04:38 Uhr von der Nummer … aus an. Sie gab vor, es müsse eine Umstellung erfolgen, damit der Zeuge sein Online-Banking, welches er bei der T5 führte, weiter nutzen könne. So veranlasste sie den Zeugen – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten – seine EC-Karte in seinen Chip-TAN Generator einzustecken, einen achtstelligen „Code“, sodann einen zehnstelligen „Code“ und schließlich die Zahlenkombination … einzugeben sowie jeweils zu bestätigen und ihr sodann die auf dem Display angezeigte Zahlenfolge – … – zu benennen. Tatsächlich handelte es sich bei dieser Zahlenfolge um eine von dem Zeugen unwissentlich generierte TAN, die die Anruferin, die sich zuvor mittels der abgephishten Daten des Zeugen Zugang zu dessen Online-Banking-Account verschafft und dort eine Überweisung an einen T6 in Höhe von 9.687,00 € vorbereitet hatte, zur Durchführung dieser Überweisung benötigte. Der zunächst eingegebene achtstellige „Code“ war ein Sicherheitscode, der der gesondert Verfolgten H oder der Telefonistin nach der Eingabe der Überweisungsdaten für den Fall der manuellen Bedienung des Chip-TAN-Generators zur Generierung einer für die Überweisung erforderlichen TAN angegeben wurde und der hierzu in den TAN-Generator eingegeben werden musste. Bei dem weiteren, von dem Zeugen eingegebenen zehnstelligen „Code“ handelte es sich tatsächlich um die letzten zehn Ziffern der Empfänger-IBAN, die ebenfalls zur Generierung einer TAN eingegeben werden mussten. Die Zahlenfolge … schließlich stellte den Überweisungsbetrag, und damit die letzte erforderliche Angabe zur manuellen Generierung einer TAN, dar. Während des insgesamt über sieben Minuten dauernden Telefonats gab die Anruferin die von dem Zeugen N5 durchgegebene TAN in dessen Online-Banking-Account ein und gab die Überweisung über **9.687,00 €** um 15:09 Uhr frei. Das Konto des Zeugen wurde in der Folge in entsprechender Höhe belastet. 66

Eine Rückbuchung des transferierten Geldes konnte nicht veranlasst werden; der Überweisungsbetrag wurde dem Zeugen jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 67

Auf dieselbe Weise hatte die Anruferin bereits im Rahmen zweier vorheriger Telefonate mit dem Zeugen am 04.11.2014, bei denen die Anrufernummer … angezeigt wurde, TANs abgelistet, deren Verwendung letztlich jedoch nicht zu einer Belastung des Kontos des Zeugen geführt hatten. 68

Fälle 8 und 9 – S2 (Fälle A9 und A10 der Anklageschrift) 69

Der Zeuge S2 verwendete im Rahmen seines Online-Bankings bei der L2 das SMS-TAN-Verfahren. Am 06.11.2014 **(Fall 8)** rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe den Zeugen nachmittags an und stellte sich als T1-Angestellte vor. Unter dem Vorwand, das Online-Banking müsse aktualisiert werden und dass ihm hierzu eine Nummer in einer SMS auf sein Handy geleitet würde, die er ihr durchgeben müsse, brachte sie den Zeugen – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten – dazu, ihr die auf sein Handy gesandte Nummer … anzugeben. Tatsächlich handelte es sich um eine TAN, die dem Zeugen im 70

Rahmen des SMS-TAN-Verfahrens auf sein Handy geleitet wurde, nachdem die Anruferin sich mit den abgephishten Daten des Zeugen Zugang zu dessen Online-Banking-Account verschafft, dort eine Überweisung in Höhe von **9.976,00 €** an einen B1 in Polen, IBAN …, vorbereitet und während des Telefonats hierfür eine TAN angefordert hatte. Um 16:36 Uhr gab die Anruferin die von dem Zeugen herausgegebene TAN in dessen Online-Banking-Account ein und sandte die vorbereitete Überweisung ab, wodurch das Konto in gleicher Höhe belastet wurde.

Am 07.11.2014 **(Fall 9)** vormittags rief sie den Zeugen erneut an und erlistete sich unter dem Vorwand, das Update vom Vortag sei fehlgeschlagen, auf dieselbe Weise wie am Vortag eine weitere TAN. Mit dieser gab sie um 10:36 Uhr eine bereits vorbereitete Überweisung in Höhe von **9.987,00 €** an einen B2 frei, wodurch das Konto in gleicher Höhe belastet wurde. Das Telefonat endete mit dem Hinweis der angeblichen T1-Angestellten, dass der Zeuge sein Online-Banking-Account bis zum darauffolgenden Sonntag nicht nutzen könne. 71

Eine Rückbuchung der transferierten Gelder konnte nicht veranlasst werden; der jeweilige Überweisungsbetrag wurde dem Zeugen jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 72

Fälle 10 und 11 – I3 (Fälle A11 und A16 der Anklageschrift) 73

Der Zeuge I3 verwendete im Rahmen seines Online-Bankings bei der T7 das SMS-TAN-Verfahren. Am 10.11.2014 **(Fall 10)** um 12:55:38 Uhr rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe den Zeugen I3 von der Nummer … aus an und stellte sich ihm als Mitarbeiterin der T1 vor. Unter dem Vorwand, ihm würde ein Code auf sein Handy gesendet, welchen er durchgeben müsse, brachte sie den Zeugen – entsprechend dem gemeinsamen Tatplan der Tätergruppe – dazu, ihr die auf sein Handy gesandte Nummer anzugeben. Hierbei handelte es sich tatsächlich um eine TAN, die dem Zeugen im Rahmen des SMS-TAN-Verfahrens auf sein Handy geleitet wurde, nachdem die Anruferin sich mit den abgephishten Daten des Zeugen Zugang zu dessen Online-Banking-Account verschafft, dort eine Änderung der Empfängernummer für TANs vorbereitet und während des Telefonats für diese Änderung eine TAN angefordert hatte. Sodann gab die Anruferin die von dem Zeugen herausgegebene TAN in dessen Online-Banking-Account ein und änderte hiermit um 12:56:40 Uhr die SMS-Empfängernummer für TANs auf die von der Tätergruppe hierfür genutzte Nummer … . Unmittelbar nach dem Gespräch gab die Telefonistin im Online-Banking-Account des Zeugen eine Überweisung in Höhe von **4.500,00 €** an einen L3 in Italien, IBAN …, ein, forderte eine TAN an, die auf die zuvor geänderte Empfängernummer geleitet wurde, und führte die Überweisung um 13:00 Uhr aus. 74

Auf die vorbeschriebene Art und Weise folgte am 13.11.2014 **(Fall 11)** eine weitere Überweisung in Höhe von **230,00 €** an L3 unter derselben IBAN. 75

Das Konto des Zeugen I3 wurde jeweils in Höhe des Überweisungsbetrages belastet. Eine Rückbuchung der transferierten Gelder konnte nicht veranlasst werden; der jeweilige Überweisungsbetrag wurde dem Zeugen jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 76

Fälle 12 bis 20 – H1 (Fälle A12, A15, A17, A18, A19, A22, A23, A25, A26 der Anklageschrift) 77

Am 10.11.2014 um 14:43:46 Uhr rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe die Zeugin H1 von der Nummer … aus an und 78

erklärte, vom Callcenter der I4 aus anzurufen. Dort verwaltete die Zeugin insgesamt sieben Konten innerhalb eines Online-Banking-Accounts, wozu sie sowohl das Chip-TAN-Verfahren, als auch das SMS-TAN-Verfahren nutze. Unter dem Vorwand, dass es um eine Änderung des PINs gehe und unter Abgleich von persönlichen Daten der Zeugin, brachte sie diese dazu, ihr im Verlauf des über 10 Minuten andauernden Gesprächs – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten – eine TAN herauszugeben. Mit dieser änderte die Anruferin innerhalb des Online-Banking-Accounts der Zeugin die für den Empfang von TANs dort hinterlegte Handynummer hin zur von der Tätergruppe hierfür genutzten Nummer …, nachdem sie sich zuvor mit den entsprechend der eingangs dargelegten Vorgehensweise der Tätergruppe abgephishten Daten Zugang zu deren Online-Banking-Account verschafft hatte. Es wurden sodann von den verschiedenen Konten innerhalb des Online-Banking-Accounts der Zeugin in der bereits beschriebenen Art und Weise unter Vorsiegelung der in Wahrheit nicht gegebenen Berechtigung verschiedene Überweisungen ausgeführt:

Am 10.11.2014 **(Fall 12)** wurden **7.150,00 €** an einen B3 in Polen, IBAN …, überwiesen, sowie **4.980,00 €** an K in Spanien, IBAN …. 79

Am 11.11.2014 **(Fall 13)** wurden **3.400,00 €** an R in Spanien, IBAN …, überwiesen. 80

Am 13.11.2014 **(Fall 14)** erfolgten Überweisungen in Höhe von **1.600,00 €** an D1 in Italien, IBAN …, und **1.600,00 €** an L3 in Italien, IBAN …. 81

Am 14.11.2014 **(Fall 15)** folgten zwei weitere Überweisungen an L3 in Höhe von **180,00 €** und **320,00 €** und am 19.11.2014 **(Fall 16)** in Höhe von **400,00 €** und **500,00 €.** 82

Am 20.11.2014 **(Fall 17)** wurden **7.300,00 €** an D2 in Italien, IBAN …, überwiesen. 83

Am 24.11.2014 **(Fall 18)** wurden ebenfalls an diese **zweimal 800,00** und einmal **900,00 €**, sowie am 25.11.2014 **(Fall 19) zweimal 900,00 €** und einmal **600,00 €** überwiesen. 84

Am 01.12.2014 **(Fall 20)** schließlich wurden **5.000,00 €** an O1 in Italien, IBAN …, überwiesen. 85

Das Konto der Zeugin wurde jeweils in Höhe des Überweisungsbetrages belastet. Eine Rückbuchung der transferierten Gelder konnte nicht veranlasst werden; der jeweilige Überweisungsbetrag wurde der Zeugin jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 86

Fall 21 – L4 (Fall A14 der Anklageschrift) 87

Am 11.11.2014 rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe den Zeugen L4 ab 12:13:48 Uhr von der Nummer … aus mehrfach an. Der Zeuge L4 ließ sein Geschäfts- und sein Privatkonto online bei der T8 im Chip-Tan-Verfahren verwalten; verfügungsberechtigt war neben ihm auch seine Ehefrau, die Zeugin L7. Um 12:19:04 Uhr wurde der Anruf weitergeleitet auf das Handy seiner Ehefrau, die sich in einer Reha-Maßnahme befand. Sie litt seinerzeit unter einer Erkrankung, die insbesondere auch ihre Konzentrationsfähigkeit stark beeinträchtigte. Unter dem Vorwand, es müsse eine Aktualisierung des Online-Banking-Accounts bei der T8 durchgeführt werden, brachte sie die Zeugin – entsprechend dem Tatplan der Tätergruppe – dazu, die EC-Karte des Geschäftskontos in den von ihr mitgeführten Chip-TAN Generator einzustecken und – in gleicher Weise wie zu Fall 7 beschrieben –, manuell eine TAN – … – zu generieren und ihr durchzugeben. Diese benötigte die Telefonistin, um eine im Online-Banking-Account des Zeugen L4 vorbereitete Überweisung an „C4“ in Polen, IBAN …, über einen Betrag in Höhe 88

von **9.890,00 €** abzusenden, was sie um 12:20 – noch während des Telefonats mit der Zeugin L7 – tat.

Das Konto des Zeugen wurde in Höhe des Überweisungsbetrages belastet. Eine Rückbuchung des transferierten Geldes konnte nicht veranlasst werden; der jeweilige Überweisungsbetrag wurde dem Zeugen jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 89

Zwei weitere, der Zeugin L7 in einem weiteren Telefonat am 12.11.2014 in der gleichen Weise abgelistete TANs wurden für die Absendung von Überweisungen an eine S3 verwandt, die jedoch gestoppt werden konnten. 90

Fall 22 – H2 (Fall A20 der Anklageschrift) 91

Am 19.11.2014 um 13:51 Uhr rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe die Zeugin H2 von der Nummer … aus an und stellte sich ihr als Mitarbeiterin der T9, bei der die Zeugin ein Konto hatte, welches sie im Online-Banking im SMS-TAN-Verfahren verwaltete, vor. Unter dem Vorwand, dass ihr Online-Banking ablaufen werde, veranlasste sie die Zeugin – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten –, ihr die auf ihr Handy gesandte TAN anzugeben. Sie wies die Zeugin an, 24 Stunden nicht in ihrem Account aktiv zu sein. 92

Am 20.11.2014 wurde die Zeugin sodann von einem namentlich nicht bekannten Telefonisten der Tätergruppe von derselben Nummer aus um 13:58 Uhr erneut angerufen, der ihr gegenüber angab, das Vorgehen am Vortag sei fehlgeschlagen, sie solle die SMS vom Vortag löschen und werde eine neue TAN erhalten, die sie durchgeben solle, was sie wiederum tat. Tatsächlich wurde der Zeugin die TAN nicht zum Zweck der Aktualisierung des Online-Bankings, sondern im Rahmen des SMS-TAN-Verfahrens auf ihr Handy geleitet, nachdem der Täter sich mit den zuvor entsprechend der eingangs dargelegten Vorgehensweise abgephishten Daten Zugang zu deren Online-Banking-Account verschafft, dort eine Überweisung über einen Betrag in Höhe von **1.420,00 €** an eine O2 in Deutschland, IBAN ..., vorbereitet und während des Telefonats für diese Überweisung eine TAN angefordert hatte. Die Überweisung wurde am 20.11.2014 – was die Zeugin nach Ablauf weiterer 24 Stunden am Abend des 21.11.2014 bemerkte – ausgeführt. 93

Das Konto der Zeugin wurde in Höhe des Überweisungsbetrages belastet. Eine Rückbuchung des transferierten Geldes konnte nicht veranlasst werden; der jeweilige Überweisungsbetrag wurde der Zeugin jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 94

Fall 23 – C5 (Fall A21 der Anklageschrift) 95

Die Zeugin C5 führte ihr Konto bei der U im Online-Banking mit dem Chip-TAN-Verfahren. Als ihre Chip-TAN-Geräte defekt waren, holte sie sich zwei neue bei der U, ließ jedoch zunächst nur eins für das Online-Banking registrieren. Am 20.11.2014 rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe die Zeugin C5 gegen 11:40 Uhr von der Nummer … aus an. Unter dem Vorwand, sie könne den zweiten Generator nunmehr telefonisch registrieren, veranlasste sie die Zeugin – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten –, ihre EC-Karte in ihren Chip-TAN Generator einzustecken, von ihr vorgegebene Zahlenfolgen in den Generator einzugeben und ihr schließlich die auf dem Generator angezeigte Zahlenfolge durchzugeben. Tatsächlich handelte es sich bei dieser Zahlenfolge um eine von der Zeugin unwissentlich – in derselben 96

Weise wie zu Fall 7 dargestellt – generierte TAN. Diese benötigte die Anruferin, die sich zuvor mittels der abgephishten Daten der Zeugin Zugang zu deren Online-Banking-Account verschafft, für eine vorbereitete Überweisung an einen P1 in Italien, IBAN …, in Höhe von **7.865,00 €**. Das Telefonat endete mit dem Hinweis, die Zeugin könne nunmehr 24 Stunden nicht auf ihr Online-Banking-Account zugreifen. Um 11:46 Uhr gab die Anruferin die von der Zeugin durchgegebene TAN unbefugt in deren Online-Banking-Account ein und gab die Überweisung frei.

Das Konto der Zeugin wurde in o.g. Höhe belastet. Der Überweisungsbetrag konnte jedoch zurückgebucht und dem Konto der Zeugin C5 wieder gutgeschrieben werden. 97

Fall 24 – M1 (Fall A24 der Anklageschrift) 98

Die Zeuge M1 führte sein Konto bei der T10 im Online-Banking mit dem Chip-TAN-Verfahren. Am 24.11.2014 rief eine namentlich nicht bekannte Telefonistin den Zeugen M1 von der Nummer … aus an und stellte sich als Mitarbeiterin der T1 namens „S4“ vor. Unter dem Vorwand, der Online-Banking-Zugang solle aktualisiert werden, veranlasste sie den Zeugen, seine EC-Karte in seinen Chip-TAN Generator einzustecken, von ihr vorgegebene Zahlenfolgen in den Generator einzugeben und ihr schließlich die auf dem Generator angezeigte Zahlenfolge durchzugeben. Tatsächlich handelte es sich bei dieser Zahlenfolge um eine von dem Zeugen – in derselben Weise wie zu Fall 7 dargestellt – generierte TAN. Diese benötigte die Anruferin, die sich zuvor mittels der abgephishten Daten des Zeugen Zugang zu dessen Online-Banking-Account verschafft hatte, für eine Überweisung an einen G3 in Deutschland, IBAN …, in Höhe von **9.898,00 €**, die sie mit der erlisteten TAN sodann ausführte. 99

Die Überweisung vom 24.11.2014 konnte nicht mehr zurückgebucht werden; der Betrag wurde dem Zeugen jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 100

Am folgenden Tag rief Frau „S4“ den Zeugen erneut von der vorbenannten Nummer aus an und brachte ihn wiederum dazu, ihr zur vermeintlichen Durchführung eines zweiten Updates eine TAN zu generieren und durchzugeben. Die hiermit freigegebene Überweisung konnte jedoch vor Belastung des Kontos gestoppt werden. Das Telefonat endete mit dem Hinweis, der Zeuge könne nunmehr bis zum Folgetag um 17:00 Uhr nicht auf sein Online-Banking-Account zugreifen. 101

Fall 25 – E3 (Fall A28 der Anklageschrift) 102

Der Zeuge E3 verwendete im Rahmen seines Online-Bankings bei der T11 das SMS-TAN-Verfahren. Am 13.01.2015 rief die gesondert Verfolgte H den Zeugen E3 um 15:52:35 Uhr von der Nummer … aus an und stellte sich gegenüber der den Anruf entgegennehmenden Frau als „E1“ von der T12 vor. Da der Zeuge E3 zu diesem Zeitpunkt – wie auch bei weiteren Anrufversuchen von der vorbenannten Rufnummer aus am 13.01.2015 um 16:30:16 Uhr und 17:38:05 Uhr – nicht zu sprechen war, rief sie, wiederum von der vorbenannten Rufnummer aus am 14.01.2015 um 13:55:09 Uhr erneut bei dem Zeugen E3 an, den sie nunmehr erreichte. Sie stellte sich wiederum als E1 vor. Unter dem Vorwand, einen Aktualisierungsantrag von ihm erhalten zu haben und ihm zur „Registrierung“ einen Code per SMS auf sein Handy zu senden, brachte sie den Zeugen – entsprechend dem gemeinsamen Tatplan mit dem Angeklagten – dazu, ihr die auf sein Handy gesandte Nummer … anzugeben. Tatsächlich handelte es sich um eine TAN, die dem Zeugen im Rahmen des SMS-TAN-Verfahrens auf sein Handy geleitet wurde, nachdem die gesondert Verfolgte H 103

sich mit den abgephishten Daten des Zeugen Zugang zu dessen Online-Banking-Account verschafft, dort eine Änderung der Empfängernummer für TANs vorbereitet und während des Telefonats um 13:57:00 Uhr für diese Änderung eine TAN angefordert hatte. Noch während des Telefonats gab die gesondert Verfolgte H die von dem Zeugen herausgegebene TAN in dessen Online-Banking-Account ein und änderte hiermit die SMS-Empfängernummer für TANs um 13:59:11 Uhr auf die von der Tätergruppe hierfür genutzte Nummer … . Das Telefonat endete um 14:00:04 Uhr mit dem Hinweis der „E1“, dass der Zeuge sich bis Freitag um 14:00 Uhr nicht in das Online-Banking einloggen könne.

Um 14:20:53 Uhr forderte die gesondert Verfolgte H eine weitere TAN zur Ausführung einer Überweisung von dem Konto des Zeugen E3 in Höhe von **5.000,00 €** auf ein Konto einer N6 in Polen, IBAN …, an, die nunmehr auf das ihr zur Verfügung stehende Handy mit der Nummer … gesendet wurde. Die Überweisung wurde zunächst ausgeführt und das Konto entsprechend belastet. Der Betrag konnte jedoch zurückgebucht und dem Zeugen E3 wieder gutgeschrieben werden. Unter Verbrauch einer weiteren generierten und auf die vorbenannte Handynummer übermittelten TAN führte H um 14:56:34 Uhr eine weitere Überweisung in Höhe von **505,00 €** an die X1 GmbH vom Konto des Zeugen E3 aus. Diese konnte ebenfalls zurückgebucht und der Betrag dem Konto des Zeugen wieder gutgeschrieben werden. 104

Fälle 26 und 27 – T13 (Fälle A29 und A30 der Anklageschrift) 105

Am 16.01.2015 rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppe die Zeugin T13 gegen 08:15 Uhr von einer „0800er-Nummer“ aus an und stellte sich ihr gegenüber als Mitarbeiterin der C3 vor. Die Zeugin verwaltete bei der C3 zwei Konten online im SMS-TAN-Verfahren. Unter dem Vorwand, es würde eine Aktualisierung des Online-Bankings durchgeführt und ihr würde ein „Sicherheitscode“ per SMS auf ihr Handy gesendet, brachte sie die Zeugin – entsprechend dem gemeinsamen Tatplan – dazu, ihr die übersandte Nummer anzugeben. Tatsächlich handelte es sich um eine TAN, die der Zeugin im Rahmen des SMS-TAN-Verfahrens auf ihr Handy geleitet wurde, nachdem die Anruferin sich mit den in der eingangs dargestellten Weise abgephishten Daten Zugang zu deren Online-Banking-Account verschafft, dort eine Änderung der Empfängernummer für TANs vorbereitet und während des Telefonats für diese Änderung eine TAN angefordert hatte. Sodann gab die Anruferin die von der Zeugin herausgegebene TAN in deren Online-Banking-Account ein und änderte hiermit die SMS-Empfängernummer für TANs auf die von der Tätergruppe hierfür genutzte Nummer …. 106

Am 16. und 17.01.2015 wurden unbefugt weitere TANs angefordert, die nunmehr auf die von der Tätergruppe hierfür eingesetzte Rufnummer geleitet und auf die vorbeschriebene Art und Weise unter Vorspiegelung der Berechtigung für Überweisungen genutzt wurden. 107

So kam es am 16.01.2015 **(Fall 26)** zu einer Überweisung an eine Q3 GmbH, IBAN …, in Höhe von **100,00 €** sowie zu drei Überweisungen an „N4“ bzw. „N7“ in Polen, IBAN jeweils …, in Höhe von **7.000,00 €, 1.850,00 €** und **1.000,00 €**. 108

Am 17.01.2015 **(Fall 27)** wurden drei Überweisungen an eine A1 GmbH, IBAN …, in Höhe von **106,42 €, 159,48 € und 265,61 €**, **sechs** Überweisungen an eine X4 GmbH, IBAN …, in Höhe von **jeweils 104,00 €** und eine Überweisung an die X1 GmbH in Höhe von **505,00 €** freigegeben, die jeweils am 19.01.2015 gebucht wurden. 109

Eine Rückbuchung des transferierten Geldes konnte nicht veranlasst werden; der jeweilige Überweisungsbetrag wurde der Zeugin jedoch später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 110

Fälle 28 und 29 – L5 (Fälle A31 und A32 der Anklageschrift) 111

Die Zeugin L5 verwendete im Rahmen ihres Online-Bankings bei der T1 das SMS-TAN-Verfahren. Nach der Dateneingabe auf der von der Tätergruppe verwendeten Internetseite rief die gesondert Verfolgte H oder eine andere, namentlich nicht bekannte Telefonistin der Tätergruppen die Zeugin L5 am 18.03.2015 um 14:10:37 Uhr von der Nummer … aus an und stellte sich ihr gegenüber als „C6“, Mitarbeiterin der T1 vor. Unter dem Vorwand, es handele sich um ein Informationsgespräch und der Zeugin zur Verifizierung eine Nummer per SMS auf ihr Handy zu senden, brachte sie die Zeugin – entsprechend dem gemeinsamen Tatplan – dazu, ihr die auf ihr Handy gesandte Nummer anzugeben. Tatsächlich handelte es sich um eine TAN, die der Zeugin im Rahmen des SMS-TAN-Verfahrens auf ihr Handy geleitet wurde, nachdem die Anruferin sich mit den abgephishten Daten Zugang zu deren Online-Banking-Account verschafft, dort eine Änderung der Empfängernummer für TANs vorbereitet und während des Telefonats für diese Änderung eine TAN angefordert hatte. Sodann gab die Anruferin die von der Zeugin herausgegebene TAN in deren Online-Banking-Account ein und änderte hiermit die SMS-Empfängernummer für TANs auf die von der Tätergruppe hierfür genutzte Nummer …. Das Telefonat endete mit dem Hinweis, dass das Online-Banking nun nicht genutzt werden könne und die Zeugin eine SMS erhalten werde, sobald sie ihr Online-Banking-Account wieder nutzen könne. 112

Am 18. und 19.03.2015 wurden unbefugt weitere TANs angefordert, die nunmehr auf die von der Tätergruppe hierfür eingesetzte Rufnummer geleitet und auf die vorbeschriebene Art und Weise unter Vorspiegelung der Berechtigung für Überweisungen genutzt wurden. 113

So kam es am 18.03.2015 **(Fall 28)** unter Verbrauch der TAN … um 14:23:34 Uhr zu einer Überweisung an U1 in Polen, IBAN …, in Höhe von **5.000,00 €**. Unter Verbrauch der TAN … um 15:56:50 Uhr kam es wiederum zu einer Überweisung an einen U1 mit vorbenannter IBAN in Höhe von **3.000,00 €** und unter Verbrauch der TAN … um 15:58:36 Uhr zu einer weiteren Überweisung an U1 mit vorbenannter IBAN in Höhe von **1.300,00 €.** 114

Am 19.03.2015 **(Fall 29)** kam es unter Verbrauch der TAN … um 08:03:56 Uhr zu einer Überweisung an einen P2 in Spanien, IBAN …, in Höhe von **2.300,00 €**. 115

Die Überweisungen konnten weder gestoppt noch die Überweisungsbeträge zurückgebucht werden, wurden der Zeugin aber später aus einem internen Sicherungsfonds der T1 kulanzweise ersetzt. 116

Weitere Überweisungen am 18. und 19.03.2015 an eine N8 B.V. und an die X5 konnten gestoppt werden. 117

b) 118

<u>Tatkomplex B:</u> Versendung von Phishingmails unter Vorspiegelung, Aussteller seien die S, die J Bank sowie die Q1 119

<u>In der eingangs dargelegten Art und Weise</u> versandte der Angeklagte zwischen dem 27.02.2015 und dem 28.05.2015 in mindestens 13 einzelnen Vorgängen unter Verwendung hierzu geeigneter Computerprogramme wie etwa des Programms „…“ massenhaft Phishingmails an die zuvor – wie vorbeschrieben – „gesammelten“ Emailadressen. Nach Inhalt und Aufmachung erweckten die Phishingmails für einen unbefangenen Adressaten den Eindruck, von der niederländischen S, der Schweizer Q1 bzw. der J3 zu stammen. 120

121

Die S ist ein international tätiger Finanzdienstleister auf genossenschaftlicher Grundlage („U.A.“), der seine Wurzeln in den Niederlanden hat und in den Bereichen Banking und Vermögensverwaltung für Privat- und Großkunden, insbesondere in der Nahrungs- und Agrarindustrie tätig ist. In den von dem Angeklagten versendeten Phishingmails betreffend die S, die als Absender etwa „S <…>" und als Betreff beispielhaft (übersetzt) „Kundenservice“ auswiesen, wurden die Adressaten in niederländischer Sprache um die Durchführung eines Updates zur Verbesserung der Sicherheit gebeten. Hierzu sollte einem in der Email enthaltenen Link wie

„http://www.....nl/...“ 122

gefolgt werden. Die Emails endeten mit einem Gruß des Kundendienstes der S5. 123

Die Q1 AG ist eine Finanzdienstleisterin und Tochtergesellschaft der Schweizerischen Q4 AG. Sie ist verbreitet im schweizerischen Zahlungsverkehr und im E-Finance, der elektronischen Kontobewirtschaftung und erbringt für Privat- und Geschäftskunden umfassende Finanzdienstleistungen in den Teilmärkten Zahlen, Sparen, Anlegen, Versorgen und Finanzieren. An Kunden dieser Bank versendete der Angeklagte im vorbenannten Zeitraum Phishingmails des folgenden Inhalts: 124

„Sehr geehrter Kunde, 125

unser Unternehmen Q1 arbeitet im Bereich des Internet-Banking 126

Bitte beachten Sie, dass Ihr Online-Banking-Zugang bald abläuft. Um diesen Dienst weiterhin nutzen zu können, klicken Sie bitte auf den untenstehenden Link um Ihren Zugang manuell mit unserem Sicherheits-Update zu aktualisieren: 127

Q1.ch Online Banking Update 128

Nach Vervollständigung dieses Schrittes werden Sie von einem Mitarbeiter unseres Kundendienstes zum Status Ihres Kontos kontaktiert. 129

Beim Online-Banking haben Sie per Mausklick alles im Griff! Mit dem komfortablen Online-Banking Ihrer Q1 haben Sie schnellen und problemlosen Zugang zu Ihrem Girokonto und erledigen Überweisungen und Daueraufträge bequem per Mausklick. Das Online-Banking bietet aber noch viele weitere Vorteile. 130

DIE VORTEILE DES ONLINE-BANKINGS AUF EINEN BLICK: 131

- Kontozugang rund um die Uhr - Schneller Zugriff aufs Girokonto - Online-Banking bequem vom PC aus - Flexibel aus jedem Winkel der Welt - Übersichtliche Kontoführung - Hohe Sicherheitsstandards Online-Banking ist kombinierbar mit Telefon-Banking 132

Um diesen Dienst weiterhin problemlos nutzen zu können, führen Sie bitte das Update so schnell wie möglich durch. 133

Mit freundlichen Gruessen, 134

Kundenservice Internet-Banking 135

. ©2015 Q1 Online.“ 136

137

Als Absender solcher Emails betreffend die Q1 verwendete der Angeklagte unter anderem „Q1 <…>“, „Q1 …“, oder „Q1 <…>“, als Betreff „unser Unternehmen Q1 arbeitet im Bereich des Internet-Banking“.

Die J ist ein international tätiger Finanzdienstleister. Die niederländische „J4 N.V.“ entspricht in ihrer Rechtsform der deutschen Aktiengesellschaft. Kunden der J3 sandte der Angeklagte im vorbenannten Zeitraum in niederländischer Sprache abgefasste Phishingmails, in denen auf die Erforderlichkeit der Durchführung eines Updates hingewiesen wurde, um zu verhindern, dass das Online-Banking auslaufe. Hierzu sollten die Adressaten dem in der Email enthaltenen Link folgen. Die Emails endeten etwa wie folgt: 138

„Met vriendelijke groeten, 139

Uw J BANK rekening afdeling beveiliging, 140

©J BANK 2015 Alle rechten voorbehouden. Reproductie alleen toestemming van J5”, 141

was ins Deutsche übersetzt bedeutet: 142

„Mit freundlichen Grüßen 143

Ihr J BANK-Konto, Sicherheitsabteilung 144

© J BANK 2015. Alle Rechte vorbehalten. Reproduktion nur mit Zustimmung der J5 BV.“ 145

Als Absender verwandte der Angeklagte für solche J-Phishingmails etwa „J BANK <…>", als Betreff etwa „Rekening“, was ins Deutsche übersetzt „Konto“ bedeutet. 146

Der Angeklagte beabsichtigte jeweils, die Empfänger der so massenhaft versendeten Emails durch den – in allen Fällen orthographisch, grammatikalisch und von der Wortwahl her zumindest im Wesentlichen unauffälligen und nicht grob fehlerhaften oder schwer verständlichen – Inhalt der Emails, insbesondere den darin angegebenen Verfasser, aber auch durch deren Aufmachung sowie den jeweiligen Betreff und Absender der Email zu täuschen. Diese sollten – so die Absicht des Angeklagten – in der Annahme, dass Verfasser und Absender der Email ihr eigenes Bankinstitut sei, auf der über den Link erreichten Phishingseite ihre persönlichen Daten und Online-Banking-Zugangsdaten entsprechend der Aufforderung eingeben, in dem Glauben, hierdurch die von der Bank im Rahmen der eigenen Vertragsbeziehungen angeforderte Erklärung abzugeben. 147

Die jeweils über den enthaltenen Link zu erreichenden Phishingseiten waren in den verschiedenen Tatzeiträumen auf unterschiedlichen Servern und unterschiedlichen Internetseiten (URLs) platziert. 148

Im Einzelnen stieß der Angeklagte in der vorbenannten Absicht folgende, voneinander getrennte Versendungen an: 149

Fall 30 – S (Fall B1 der Anklageschrift) 150

Am 27.02.2015 versandte der Angeklagte zwischen 14:05 Uhr und 14:18 Uhr eine vorgeblich von der S in den Niederlanden stammende Phishingmail mit vorgenanntem Inhalt an mindestens 9.162 Empfänger, auf deren Mail-Servern bzw. Rechnern diese abgelegt wurde. 151

Fall 31 – S (Fall B2 der Anklageschrift) 152

Am 28.02.2015 versandte der Angeklagte zwischen 11:51 Uhr und 20:43 Uhr wiederum eine vorgeblich von der S in den Niederlanden stammende Phishingmail mit vorgenanntem Inhalt an mindestens 61.179 Empfänger, auf deren Mail-Servern bzw. Rechnern diese abgelegt wurde. 153

Fall 32 – S (Fall B3 der Anklageschrift) 154

Am 01.03.2015 versandte der Angeklagte zwischen 07:49 Uhr und 12:02 Uhr ebenfalls eine vorgeblich von der S in den Niederlanden stammende Phishingmail mit vorgenanntem Inhalt an wenigstens 13.861 Empfänger, auf deren Mail-Servern bzw. Rechnern diese abgelegt wurde. 155

Fall 33 – Q1 (Fall B4 der Anklageschrift) 156

Am 16.03.2015 versandte der Angeklagte zwischen 10:21 Uhr und 18:57 Uhr eine vorgeblich von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt an zumindest 22.010 Empfänger, auf deren Mail-Servern bzw. Rechnern diese abgelegt wurde. 157

Fall 34 – Q1 (Fall B5 der Anklageschrift) 158

An weitere mindestens 1.162 Empfänger versendete der Angeklagte die vorgeblich von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt am 17.03.2015 zwischen 09:56 Uhr und 10:00 Uhr. Diese wurde auf den Mail-Servern bzw. Rechnern der Empfänger abgelegt. 159

Fall 35 – Q1 (Fall B6 der Anklageschrift) 160

Auch am 18.03.2015 versandte der Angeklagte, zwischen 09:51 Uhr und 11:51 Uhr, die scheinbar von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt an nunmehr wenigstens 3.074 Empfänger, auf deren Mail-Servern bzw. Rechnern die Email abgelegt wurde. 161

Fall 36 – J (Fall B7 der Anklageschrift) 162

Im weiteren Verlauf des 18.03.2015 versandte der Angeklagte zwischen 16:14 Uhr und 18:14 Uhr eine nunmehr vorgeblich von der J3 stammende Phishingmail mit vorgenanntem Inhalt. Diese wurde auf den Mail-Servern bzw. Rechnern der zumindest 15.640 Empfänger abgelegt. 163

Fall 37 – Q1 (Fall B9 der Anklageschrift) 164

Am 17.05.2015 versandte der Angeklagte zwischen 15:19 Uhr und 16:28 Uhr wiederum eine dem Anschein nach von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt an mindestens 14.182 Empfänger, auf deren Mail-Servern bzw. Rechnern diese abgelegt wurde. 165

Fall 38 – Q1 (Fall B13 der Anklageschrift) 166

Auch am 25.05.2015 versandte der Angeklagte zwischen 10:10 Uhr und 11:06 Uhr die vorgeblich von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt an wenigstens 40.660 Empfänger, auf deren Mail-Servern bzw. Rechnern die Email abgelegt wurde. 167

168

Fall 39 – Q1 (Fall B14 der Anklageschrift)

Ebenfalls am 25.05.2015 versandte der Angeklagte, nunmehr zwischen 19:45 Uhr und 22:58 Uhr die dem Anschein nach von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt an weitere mindestens 243.711 Empfänger, auf deren Mail-Servern bzw. Rechnern diese abgelegt wurde. 169

Fall 40 – Q1 (Fall B15 der Anklageschrift) 170

Einen Tag später, am 26.05.2015, versandte der Angeklagte zwischen 18:56 Uhr und 20:38 Uhr die vorgeblich von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt an mindestens 49.463 Empfänger, auf deren Mail-Servern bzw. Rechnern die Email abgelegt wurde. 171

Fall 41 – Q1 (Fall B16 der Anklageschrift) 172

Am nächsten Tag, dem 27.05.2015, versandte der Angeklagte die vorgeblich von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt zwischen 07:12 Uhr und 07:15 Uhr an zumindest 18.891 Empfänger, auf deren Mail-Servern bzw. Rechnern die Email abgelegt wurde. 173

Fall 42 – Q1 (Fall B17 der Anklageschrift) 174

Weiterhin versandte der Angeklagte am 28.05.2015 zwischen 12:51 Uhr und 13:50 Uhr die vorgeblich von der Q1 in der Schweiz stammende Phishingmail mit vorgenanntem Inhalt an wenigstens 730 Empfänger, auf deren Mail-Servern bzw. Rechnern diese abgelegt wurde. 175

Die vorgenannten Taten beging der Angeklagte während seiner regelmäßigen Aufenthalte bei J2 in der A-Straße … in F4. Er nutzte hierfür verschiedene technische Geräte, wobei die Verbindung zum Internet durch einen sog. „Surfstick“ oder mit Hilfe eines anderen internetfähigen Gerätes aufgebaut wurde. 176

III. Beweiswürdigung 177

1. Feststellungen zur Person 178

Die Feststellungen zu den persönlichen Verhältnissen des Angeklagten beruhen auf seiner entsprechenden insoweit glaubhaften Einlassung sowie auf dem verlesenen Bundeszentralregisterauszug vom 07.11.2016. Die Feststellungen zu seinem niederländischen Reisepass werden gestützt durch die Angaben des im Rahmen der Hauptverhandlung in Augenschein genommenen und verlesenen Ausweisdokuments. Die Angaben zur Staatsbürgerschaft der Frau J2, deren Wohnort in T und ab dem 01.12.2014 an der A-Straße … in F1 werden gestützt und in Details ergänzt durch den diese Daten ausweisenden Ausdruck aus dem Meldeportal der Behörden betreffend J2. Dass der Angeklagte neben dem Englischen auch des Pidgin-Englischen in Wort und Schrift mächtig ist, folgt insbesondere aus – ihm aufgrund der Beweisaufnahme eindeutig zuzuordnenden – Internet-Chats. 179

2. Feststellungen zur Sache 180

Die Feststellungen zur Sache beruhen auf der Beweisaufnahme, wie sie sich aus dem Sitzungsprotokoll ergibt. 181

182

a) Einlassungen des Angeklagten

Der Angeklagte hat sich im Rahmen der Hauptverhandlung lediglich dahingehend zur Sache eingelassen, er habe „das“ nicht gemacht. 183

Während des Ermittlungsverfahrens hatte er sich anlässlich der Verkündung des Haftbefehls am 30.06.2016 bei dem Amtsgericht C wie folgt eingelassen: 184

Er habe „das“ – nämlich das, was ihm von der Polizei gesagt worden sein soll – nicht getan. „Es“ solle 2014 in der A-Straße geschehen sein. Sein Kind habe zu dieser Zeit nicht dort gewohnt. Er sei die meiste Zeit in F1. Dort besuche er in der A-Straße die Mutter seines Kindes, Frau J2. Sie habe keinen anderen Partner; er könne garantieren, dass sie keine anderen Männer habe. Sie wohne dort allein mit den Kindern. Er wohne seit 8 Jahren in der W-Straat in S1 und habe eine Aufenthaltserlaubnis. Er sei Taxifahrer. Die Taxifahrerlizenz habe er seit 2010 oder 2011. Damit verdiene er seinen Lebensunterhalt. Wenn er kein Geld habe, fahre er für das Internettaxi, wo auch viele Fahrten von Land zu Land anstünden. Er kenne die gesondert Verfolgte H als Taxifahrgast. Daher habe er auch ihre Handynummer. Nach Deutschland habe er sie nie gefahren. Kennengelernt habe er sie vor ein paar Jahren in S1. Er kenne ihren Nachnamen nicht. Sie sei noch nie bei ihm zu Hause gewesen und kenne seine Frau und seine Kinder nicht. Er „habe keine Email“ und könne sich nicht daran erinnern, mal mit der gesondert Verfolgten H gechattet zu haben. Ein Telefon, welches in seinem Auto gefunden worden sei, sei dort liegen geblieben. Er fahre Leute, die aus Afrika kämen, um hier Autos zu kaufen. Diese ließen teilweise Sachen in seinem Auto. Das Programm, welches die Polizei auf seinem Computer in seiner Wohnung in S1 gefunden habe, sei kein Programm für Emails. Es sei eine kostenfreie Software, um unterbrechungsfrei Z1 sehen zu können und sei von einem Freund heruntergeladen worden. 185

„V“, „X2“, „P3“, „V3“ und „O3“ sagten ihm nichts; den Spitznamen „L“ kenne er nicht. J7 und dessen Frau kenne er. Er habe ihn im Club N9 in F1 kennengelernt, wisse aber nicht, was dieser mache und habe auch keine Geschäfte mit ihm gemacht. Zuletzt habe er ihn gesehen, als er ihn vor Weihnachten zum Flughafen gebracht habe. 186

b) Beweiswürdigung 187

Die Kammer ist von der generellen Arbeitsweise der Tätergruppe im Sinne der getroffenen Feststellungen überzeugt. 188

Dies gilt namentlich für 189

- die Datenerlangung durch Versendung von einen Link auf eine tätereigene Phishingseite enthaltenden Phishingmails (**hierzu aa)**) einschließlich der Geeignetheit der Inhalte und Aufmachungen dieser zur Täuschung (**hierzu bb)**), 190

- die Platzierung der Phishingseiten auf fremden Servern und Hinterlegung derer mit php-Skripten, die die eingegebenen Daten in tätergruppeneigene Emailpostfächer leiteten (**hierzu cc)**), 191

- die Inhalte der durchgeführten Telefonanrufe in Abhängigkeit von dem jeweiligen TAN-Verfahren einschließlich der Nutzung der Dienste der Firma W1 zur Durchführung der Telefonate (**hierzu dd)**) 192

- die Eingabe der erlisteten TAN zur Durchführung der vorbereiteten Überweisung bzw. Nummernänderung durch den jeweiligen Telefonisten/die jeweilige Telefonistin (hierzu **ee)**). 193

Die Kammer ist weiterhin davon überzeugt, dass der Angeklagte – alias „L“ und „N1“ –, die gesondert Verfolgte H – alias „Q2“ und „E1“ –, sowie der gesondert Verfolgte V – alias „X2“ – Mitglieder der vorbenannten arbeitsteilig vorgehenden Tätergruppe waren und in der festgestellten Art und Weise an dem Tatgeschehen beteiligt waren (**hierzu ff)**). Aufgrund der Beweisaufnahme steht zudem fest, dass diese Tätergruppe unter Einschluss des Angeklagten die im Tatkomplex A festgestellten Taten begangen hat (**hierzu gg)** bis **ii)**). 194

Schließlich ist die Kammer von der Begehung der zum Tatkomplex B dargelegten Taten durch den Angeklagten überzeugt (**hierzu jj)**). 195

aa) Datenerlangung der Tätergruppe durch Versendung von Phishingmails 196

Die Überzeugung der Kammer von der Datenerlangung der Tätergruppe durch Versendung von Phishingmails beruht zum einen auf den glaubhaften Bekundungen des Zeugen E4, der auf der Basis seiner umfangreichen Ermittlungstätigkeiten im vorliegenden Verfahren die Vorgehensweise der Tätergruppe im Sinne der Feststellungen bekundet hat. Seine Aussage wird gestützt und ergänzt durch seinen eben diese Arbeitsweise darlegenden Aktenvermerk vom 23.01.2015, aus welchem zudem der Inhalt einer versandten T1-Phishingmail sowie auch die durch den Link erreichte Seite ersichtlich sind. Der Zeuge E4 hat den Inhalt des Vermerks im Rahmen seiner Vernehmung glaubhaft bestätigt. 197

Zum anderen beruht die Überzeugung der Kammer auf den ebenfalls glaubhaften Bekundungen der Zeugen T4, N5, I3 und E3 im Sinne der getroffenen Feststellungen sowie den zu dem Fall L5 verlesenen Dokumenten und insbesondere auf der Gesamtschau der einzelnen Aussagen bzw. verlesenen Dokumente zu diesen Fällen. Die Zeugen T4, I3 und E3 haben im Kern übereinstimmend auch mit den verlesenen Angaben der Frau L5 jeweils detailliert und plausibel ausgesagt, eine dem Anschein nach von der T1 – bei welcher sie jeweils zumindest ein Konto im Online-Banking verwalteten – stammende Email erhalten zu haben. In dieser seien sie aufgefordert worden, einem darin enthaltenen Link zum Zwecke einer Aktualisierung bzw. eines Updates zu folgen. Dieser Aufforderung seien sie nachgekommen und hätten auf der hierdurch erreichten Seite die abgefragten Daten, nämlich ihre persönlichen Daten eingegeben. Insbesondere die Aussage des Zeugen E3 und die Angaben der Zeugin L5 werden durch die seinerzeit jeweils zur Ermittlungsakte gereichte, in den Feststellungen im Wortlaut dargelegte vermeintliche T1-Email gestützt und ergänzt. Gerade der Umstand, dass die Zeugen unabhängig voneinander und ohne ersichtliche Verbindung zueinander im Kern ein übereinstimmendes Geschehen bekundet haben, führt die Kammer zu der Überzeugung, dass es sich um eine gleichförmige Vorgehensweise der Tätergruppe handelt. 198

Dass andere in den Fällen des Tatkomplexes A betroffene Bankkunden ausgesagt haben, keine Email erhalten zu haben, dem Link nicht gefolgt zu sein bzw. auf der so erreichten Phishingseite keine Daten eingegeben zu haben bzw. sich insoweit nicht erinnern konnten, vermag die Überzeugung der Kammer nicht in Zweifel zu ziehen. Die Kammer hat in diesem Zusammenhang insbesondere geprüft, ob Anhaltspunkte dafür vorhanden sind, dass die Täter auf einem anderen als dem festgestellten Weg an die erforderlichen Daten der Bankkunden gelangt sein können. Dies war nach dem Ergebnis der Beweisaufnahme jedoch zu verneinen. So haben die vernommenen Bankkunden übereinstimmend bekundet, die auf ihren Computern installierten Virenschutzprogramme hätten weder im unmittelbaren Vorfeld der unautorisierten Überweisungen noch bei nachträglichen Virenscans Hinweise auf etwaig installierte Trojaner oder andere Schadprogramme geliefert. Wie der hierzu vernommene Zeuge E4 zudem glaubhaft bekundet hat, haben sich während der gesamten, von ihm zusammengeführten Ermittlungen auch keine Hinweise auf einen etwaigen „Datendiebstahl“ 199

bei den betroffenen T1 ergeben. Auch vor diesem Hintergrund waren die teilweise abweichenden Angaben von betroffenen Konteninhabern zum Erhalt bzw. der Bearbeitung der Phishingmail zur Überzeugung der Kammer zum einen dem Umstand geschuldet, dass sich betroffene Konteninhaber an die – aus ihrer damaligen Sicht – als Routine erscheinenden Vorgänge nicht mehr bzw. nicht zutreffend erinnern konnten. Zum anderen war zu bedenken, dass die Betroffenen Scham und Ungläubigkeit über den Umstand geäußert haben, auf einen Internetbetrug der vorliegenden Art „hereingefallen“ zu sein. Dies legte für die Kammer auch die Annahme nahe, dass Erhalt und Bearbeitung der Phishingmails durch Anklicken des Links und Eingabe persönlicher Daten auf der folgenden Internetseite entweder verdrängt oder bewusst verschwiegen wurden.

Auch der spätere Anruf durch die Tätergruppe scheidet als alleinige Erkenntnisquelle für persönliche und Online-Banking-Zugangsdaten aus. Dies ergibt sich bereits daraus, dass verschiedene Bankkunden ausgesagt haben, im Telefonat sei ein Datenabgleich durchgeführt worden, bei welchem ihre Daten dem Anrufenden bereits vorgelegen hätten. Zudem muss die Tätergruppe bereits vor dem Anruf bei dem jeweiligen Bankkunden über dessen Daten verfügt haben, zumal ihr anderenfalls Name, Rufnummer und der Umstand, dass es sich um einen Kunden einer bestimmten Bank handelt, nicht bekannt gewesen wären. 200

bb) Geeignetheit des Inhalts und Aufmachung der Phishingmails und Phishingseiten zur Täuschung 201

(1) Die Überzeugung der Kammer von der Geeignetheit der **T1-Phishingmails** und -Phishingseiten zur Täuschung über deren tatsächlichen Verfasser ergibt sich aus dem Aktenvermerk des Zeugen E4 vom 23.01.2015, aus welchem der Inhalt der versandten – in den Feststellungen im Wortlaut wiedergegebenen – T1-Phishingmail sowie auch die durch den Link erreichte Seite ersichtlich sind. Diese Phishingmail erhielten auch die Zeugen E3 und L5. Hieraus ist ersichtlich, dass der Inhalt der versendeten Phishingmails weder orthographisch, noch grammatikalisch, noch von der Wortwahl her grob fehlerhaft oder schwer verständlich wäre. Insofern ist nicht ersichtlich, aus welchem Grund die Empfänger hätten davon ausgehen sollen, dass die Email nicht von ihrem ausgewiesenen Unterzeichner, der „T1“, stammt. Dies gilt umso mehr angesichts der festgestellten Absenderangaben, von denen die Kammer aufgrund der zu den Fällen E3 und L5 verlesenen Emailausdrucken überzeugt ist. Diese enthalten die Angabe „T1 Online-Banking“, was geeignet ist, den Empfänger annehmen zu lassen, dass die T1 Absender der Email sei. Auch die Phishingseite, auf die der Link der Email leitete, erweckt zur Überzeugung der Kammer keine Zweifel daran, dass es sich um eine echte T1-Seite handelt. Insbesondere wurden dort das T1-Emblem und insgesamt das von der T1 bekannte Design verwendet, was geeignet ist, einen Irrtum über den tatsächlichen Aussteller dieser Seite hervorzurufen. 202

(2) Dass die betreffend die **S** massenhaft versandten Phishingmails geeignet waren, bei den Empfängern den Eindruck zu vermitteln, von dieser zu stammen, steht zur Überzeugung der Kammer fest aufgrund des Aktenvermerks des Zeugen E4 vom 27.02.2015, der durch den Zeugen im Rahmen seiner Vernehmung inhaltlich bestätigt wurde. Der dort wiedergegebene Text einer Phishingmail ist orthographisch, grammatikalisch und von der Wortwahl her nicht grob fehlerhaft oder schwer verständlich und gibt keinen sich dem unbefangenen Adressaten aufdrängenden Anhaltspunkt dafür, dass sie tatsächlich nicht von dem ausgewiesenen Aussteller, der „S5“, stammt. Dies ergibt sich zur Überzeugung der Kammer auch aus den entsprechenden überzeugenden, weil detaillierten und nachvollziehbaren Angaben des Sprachsachverständigen I5. Für eine Eignung zur Täuschung sprechen auch die Absender- 203

und Betreffangaben, die sowohl die „S“, als auch einen „Klantenservice“ – übersetzt „Kundenservice“ - benennen. Die im Aktenvermerk vom 27.02.2015 dargestellte Phishingseite entspricht ihrer Aufmachung nach dem „echten“ Design der S.

(3) Hinsichtlich der **Q1**-Phishingmails und -Phishingseiten beruht die Überzeugung der Kammer von der Geeignetheit dieser zur Täuschung auf den Ergebnissen der zu dem Gerät mit der IMEI mit der Endziffer -… durchgeführten Telekommunikationsüberwachung, wie sie in den Aktenvermerken des Zeugen S6 vom 19.05.2015 und 29.05.2015 niedergelegt sind und deren Inhalt der Zeuge im Rahmen seiner Vernehmung glaubhaft bestätigt hat. Die entsprechenden Emailtexte, die dem in den Feststellungen wiedergegebenen Wortlaut entsprechen, geben dem unbefangenen Empfänger weder im Hinblick auf die Orthographie oder die Grammatik, noch im Hinblick auf die Wortwahl greifbare Anhaltspunkte, dass die Email tatsächlich nicht von ihrem ausgewiesenen Aussteller, der „Q1 Online“, stammen würde. Dies gilt umso mehr im Hinblick auf die – sich ebenfalls aus den vorbenannten Vermerken ergebenden – Absender- und Betreffangaben, die das Wort „Q1“ enthalten. Die korrespondierende Phishingseite entspricht in ihrem Design demjenigen der Q1 und ist daher geeignet, über ihren tatsächlichen Aussteller zu täuschen. 204

(4) Dass die betreffend die **J3** massenhaft versendeten Phishingmails wie auch die dazugehörigen Phishingseiten ebenfalls täuschungsgeeignet waren, ergibt sich aus der auch insoweit überzeugenden Ausführungen des Sprachsachverständigen I5. Dieser hat bekundet, dass vorhandene orthographische Fehler oder Ungewöhnlichkeiten bei der Wortwahl der von ihm übersetzten J-Phishingmail jedenfalls nicht derart ins Gewicht fielen, dass sie bei einem „Darüberlesen“ sofort aufgefallen wären oder gar den Eindruck erweckt hätten, die Email stamme nicht von der Bank. Dass es sich bei der von dem Zeugen I5 übersetzten Email um diejenige handelte, die massenhaft versendet wurde, ergibt sich aus der glaubhaften Aussage des Zeugen E4. Dieser hat auf der Basis seiner umfangreichen Ermittlungstätigkeiten im vorliegenden Ermittlungsverfahren bekundet, die ihm vorgehaltene, von ihm erstellte Tabelle, in welcher die von dem Zeugen I5 übersetzte Email enthalten ist, weise die versendeten Phishingmails nach Anzahl und enthaltenem Link aus. Betreff- und Absenderangaben, die sich ebenfalls aus dem von dem Zeugen E4 bestätigten Tabelleninhalt ergeben, deuten durch die Verwendung der Worte „J BANK“ und „Konto“ irrtumserregend auf eine Versendung durch die „echte“ J3 hin. Das Design der entsprechenden Phishingseite entspricht demjenigen der J3 und ist daher geeignet, über ihren „Verfasser“ zu täuschen. 205

cc) Platzierung der Phishingseiten und Weiterleitung der Daten 206

Die Feststellungen, dass die Phishingseiten auf fremden Servern platziert und mit php-Skripten hinterlegt wurden, durch welche die eingegebenen Daten an tätergruppeneigene Emailpostfächer weitergeleitet wurden – was letztlich zum Erhalt der „abgephishten“ Daten führte –, beruhen auf den Bekundungen der Zeugen E4 und B4, an denen zu zweifeln die Kammer keinen Anlass hat. Diese stehen zudem im Einklang mit den Ergebnissen der durchgeführten Telekommunikationsüberwachung sowie der Auswertung der in der Wohnung des Angeklagten in S1 sichergestellten Geräte. Insbesondere in der Gesamtschau dieser einzelnen Beweisergebnisse ist der Kammer kein Zweifel an der Vorgehensweise der Tätergruppe im Hinblick auf die Erlangung der Daten verblieben. 207

Die insoweit getroffenen Feststellungen entsprechen den Bekundungen zunächst des Zeugen E4, der sich insoweit auf die Ergebnisse der Auswertung von Datenprotokollen durch Datenprogramme bezog. Seine detailreichen, fachlich fundierten Bekundungen im Sinne der getroffenen Feststellungen zur Platzierung der Phishingseiten und Weiterleitung der abgephishten Daten– die durch das übrige Ergebnis der Beweisaufnahme nicht in Zweifel 208

gezogen werden –, lassen sich ohne Weiteres mit den Ergebnissen der im Zusammenhang mit den vorliegend in Rede stehenden Taten durchgeführten TKÜ-Maßnahmen in Einklang bringen. Etwa aus seinem auf diesen Ergebnissen beruhenden Aktenvermerk vom 27.02.2015 – dessen Inhalt der Zeuge im Rahmen seiner Vernehmung bestätigt hat – ergibt sich insoweit, dass über den Link in einer Phishingmail betreffend die S die URLs http://www.....net/....nl/....html sowie http://www.....net/....nl/....html erreicht wurden. Auf diesen – nicht tätergruppeneigenen – URLs befand sich eine gefälschte Seite der S, auf der zur Dateneingabe aufgefordert wurde. Dabei war erkennbar, dass diese Seite zuvor auf den Server http://www.....net hochgeladen wurde. Aus dem hochgeladenen php-Skript war weiterhin erkennbar, dass die Daten automatisch an die Emailadressen …@....com sowie …@....com gesendet wurden.

Gestützt werden die Erkenntnisse aus der Aussage des Zeugen E4 sowie der Telekommunikationsüberwachung im Sinne der getroffenen Feststellungen, zumal die Kammer – insoweit wird auf die nachfolgenden Ausführungen verwiesen – davon überzeugt ist, dass der Angeklagte Teil der in Rede stehenden Tätergruppe ist, durch die Ergebnisse der Auswertung der in der Wohnung des Angeklagten in S1 sichergestellten Geräte. Auf dem in der Wohnung des Angeklagten in S1 sichergestellten Laptop I6 waren neben Texten für Phishingmails und Dateien für gefälschte Bankseiten auch webbasierte Zugriffe auf diverse Emailpostfächer feststellbar. In diesen wiederum konnten ausgespähte Daten aufgefunden werden, was für eine Weiterleitung abgephishter Daten in Emailpostfächer, auf die der Angeklagte Zugriff hat, spricht. 209

Auf den ebenfalls in der Wohnung des Angeklagten sichergestellten USB Sticks waren – was sich zwanglos mit den übrigen Ergebnissen der Beweisaufnahme in Einklang bringen lässt –, php-Skripte gespeichert, die für eine Weiterleitung von Daten an die darin hinterlegten Emailadressen sorgten. Hinterlegt waren in diesen Skripten u.a. die Emailadressen …@....com, …@....com und …@....com, …@....com, …@....com, …@....com und …@....com. Zu den Skripten passende gefälschte Bankseiten fanden sich ebenfalls auf den vorbenannten Asservaten. Weitere gefälschte Bankseitendateien nebst php-Skript fanden sich auf anderen in der Wohnung des Angeklagten asservierten USB Sticks. Bereits in der Gesamtschau der Ergebnisse der Asservatenauswertung verbleibt daher kein vernünftiger Zweifel an der Datenerlangung durch die Tätergruppe im Sinne der getroffenen Feststellungen und der maßgeblichen Beteiligung des Angeklagten an diesen Vorgängen. 210

Hieran schließen im Übrigen die Bekundungen des Zeugen B4 nahtlos an. Dieser hat auf der Grundlage der von ihm durchgeführten Auswertung der Inhalte der Emailpostfächer ...@....com, …@....com und …@....com unter detaillierter Schilderung seiner Vorgehensweise ausgesagt, er habe bei der Aufbereitung der vorbenannten Emailpostfächer Daten, die auf Phishingseiten eingegeben worden seien, extrahieren können. Pro solcher Daten enthaltender Email sei jeweils ein Datensatz enthalten gewesen. Von allen 3 Accounts seien zudem php-Phishing-Skripte versendet worden. Auch das von ihm (eingeschränkt) ausgewertete Emailpostfach …@....com habe Emails enthalten, die ihrem Anschein nach von einem php-Skript stammten. 211

dd) Inhalt und Rufnummern der Telefonanrufe 212

Die Feststellungen der Kammer zum Inhalt und Ablauf der Anrufe zur Erlangung einer TAN beruhen insbesondere auf der Aussage des Zeugen E4 sowie hierzu vernommenen Bankkunden. Der Zeuge E4 hat – was auch durch die Inhalte seiner Aktenvermerke vom 15.01.2015 und 22.01.2015 gestützt wird – den Umstand, dass Telefonanrufe seitens der Tätergruppe an Bankkunden erfolgten, sowie den grundsätzlichen inhaltlichen Ablauf der 213

Gespräche im Sinne der getroffenen Feststellungen sowohl für den Fall des Chip-TAN-Verfahrens als auch für den Fall des SMS-TAN-Verfahrens aufgrund der gewonnenen Ermittlungsergebnisse bekundet. Zweifel an der Glaubhaftigkeit der Aussage des Zeugen E4 sind auch insoweit nicht gegeben.

Dies gilt umso mehr, als sich seine Bekundungen hinsichtlich des Gesprächsverlaufs im Fall des Chip-TAN-Verfahrens mit den Aussagen der Zeugen G1, N5, C5 und M1 im Wesentlichen deckten. Gleiches gilt im Fall des SMS-TAN-Verfahrens für die Aussagen der Zeugen I, I2, T4, X3, S2, I3, H2, E3 und T13 sowie den Feststellungen zum Fall L5. Dass die Zeuginnen H1 und L7 bekundet haben, keine TAN oder sonstige Zahlenfolge herausgegeben zu haben, steht den getroffenen Feststellungen schon insofern nicht entgegen, als die Kammer – wie zu den einzelnen Fällen des Tatkomplexes A noch gezeigt werden wird – davon überzeugt ist, dass auch diese Zeuginnen im Rahmen des Telefonates zumindest eine TAN herausgaben. Sämtliche zu den Fällen des Tatkomplexes A vernommenen Zeugen haben bestätigt, zumindest einen Telefonanruf erhalten zu haben, in welchem der/die Anrufende sich als T1-Mitarbeiter und Mitarbeiter des T1-Callcenters vorgestellt habe. 214

Schließlich deckten sich die Bekundungen des Zeugen E4 zum Gesprächsverlauf im wesentlichen Kern auch mit dem Inhalt der „Anleitung“ für Telefonanrufe zur Erlistung einer TAN, welche auf einem in der Wohnung des Angeklagten in S1 sichergestellten USB aufgefunden wurde. Hierzu hat der Zeuge E4 ergänzend bekundet, auf anderen sichergestellten Datenträgern seien diverse sich ähnelnde Gesprächsleitfäden aufgefunden worden. 215

Soweit die Kammer im Hinblick auf die durchgeführten Telefonanrufe zudem festgestellt hat, dass sich die Tätergruppe der Dienste der Firma W1 für die Anrufe bediente, beruht auch dies auf den glaubhaften Bekundungen des Zeugen E4, der detailliert und nachvollziehbar zu den Diensten der Firma W1 und deren Verwendung durch die Tätergruppe ausgesagt hat. 216

ee) Eingabe der abgelisteten TAN 217

Dass die telefonisch abgelistete TAN durch den jeweiligen Telefonisten/die jeweilige Telefonistin zur Ausführung der Überweisung bzw. Änderung der Empfängernummer für TANs per SMS eingegeben wurde, ergibt sich aus der Gesamtschau der hierzu jeweils erhobenen Daten der T1 sowie aus rückwirkenden Verbindungsdaten oder Telekommunikationsüberwachungsprotokollen aus den im Tatkomplex A abgeurteilten Fällen. Die sich hieraus ergebenden Uhrzeiten von Anrufen einerseits und TAN-Entwertungen andererseits lassen auch auf eine Vorbereitung des TAN-pflichtigen Vorgangs vor dem Telefonat schließen. 218

So ergibt sich etwa im Fall E3 aus dem Protokoll über das zur unberechtigten Überweisung führende Telefonat, dass dieses von 13:55:09 Uhr bis 14:00:04 Uhr andauerte, während die erste erlistete TAN – wie es sich aus den Details des Geschäftsvorfalls ergibt – bereits um 13:59:11 Uhr – und damit während des Telefonats entwertet wurde. Überdies waren nach der Durchgabe der erlisteten TAN im Hintergrund des Anrufenden Tippgeräusche hörbar, die bereits für sich genommen die Eingabe der erlisteten TAN durch den Anrufenden nahelegen. Der Zeuge N5 wurde nach den rückwirkenden Verbindungsdaten um 15:04:38 Uhr für ca. acht Minuten angerufen. Die unberechtigte Überweisung erfolgte gemäß seinem diese ausweisenden Kontoauszug um 15:09 Uhr und damit noch während des Telefonates. Der Zeuge X3 wurde nach den rückwirkenden Verbindungsdaten um 12:50:24 Uhr angerufen. Die von ihm in diesem Telefonat herausgegebene TAN wurde nach den Details des Geschäftsvorfalls um 12:53:10 Uhr entwertet. Die Zeugin L7 wurde laut rückwirkender 219

Verbindungsdaten um 12:19:04 Uhr für ca. vier Minuten angerufen. Eine erste Überweisung erfolgte ausweislich der entsprechenden Umsatzdetails um 12:20 Uhr – während des Telefonates.

Konkrete Anhaltspunkte für eine Vorbereitung des TAN-pflichtigen Vorgangs und die Eingabe der erlisteten TAN durch eine andere Person als die jeweilige Telefonistin/den jeweiligen Telefonisten – insbesondere für eine Eingabe durch den Angeklagten selbst – hat die Beweisaufnahme demgegenüber nicht ergeben. 220

ff) Konkrete Beteiligung an den verfahrensgegenständlichen Taten 221

Dass der Angeklagte und die gesondert Verfolgten H und V dieser Tätergruppe angehörten und in der festgestellten Art und Weise an den Taten beteiligt waren, folgt insbesondere aus den glaubhaften Aussagen der hierzu vernommenen Ermittlungsbeamten, den Ergebnissen der Telekommunikationsüberwachung sowie den Auswertungen der in der Wohnung des Angeklagten in S1, der Wohnung der gesondert Verfolgten H in N13 und der Wohnung der J2 an der A-Straße in F1 sichergestellten Asservate. Die hieraus gewonnenen einzelnen Beweisergebnisse bestätigten, stützen und ergänzten sich untereinander und wechselseitig, weshalb der Kammer insbesondere in deren Gesamtschau kein begründeter Zweifel an dem gemeinsamen Vorgehen des Angeklagten mit den weiteren Beteiligten in der festgestellten Weise verblieben ist. 222

Im Einzelnen: 223

(1) Der Angeklagte, L und N1 sind eine Person 224

Für die Kammer steht nach dem Ergebnis der Beweisaufnahme zunächst – was Grundlage der weiteren Überzeugungsbildung war – zweifelsfrei fest, dass es sich bei dem Angeklagten, L und N1 um dieselbe Person handelt. 225

Dieser Überzeugung liegt Folgendes zugrunde: 226

- Zu der Mobilfunknummer **…**, die die Tätergruppe als Empfängernummer für TANs in den Fällen E3, T13 und L5 verwendete, konnten – ebenso wie für das Gerät mit der IMEI …, in welchem die vorbenannte Rufnummer u.a. verwendet wurde – im Rahmen der Ermittlungen in dem vorliegenden Verfahren Standortdaten für F4 ermittelt werden, wo der Angeklagte sich bereits nach seinen eigenen Angaben im Ermittlungsverfahren, seit dem Einzug der Frau J2 in die Wohnung an der A-Straße …, regelmäßig aufhielt. Dies ergibt sich aus der entsprechenden Aussage des Zeugen E4, an der zu zweifeln die Kammer keinen Anlass hat und welche gestützt wird durch den Inhalt seiner Aktenvermerke vom 22.01.2015, 30.01.2015 und 16.02.2016. Deren Inhalt wurde durch den Zeugen E4 im Rahmen seiner Vernehmung als zutreffend bestätigt. 227 228

- Über das vorbenannte Gerät mit der IMEI mit der Endziffer … hat L in einem Z-Chat, wie der Zeuge E4 glaubhaft bekundete, kommuniziert. Wie sich aus der glaubhaften Aussage sowie dem Aktenvermerk des Zeugen E4 vom 16.02.2015 ergibt, wurde in diesem Gerät ab dem 11.02.2015 die SIM-Karte mit der Rufnummer … betrieben, welche im Call Shop W2, X6-Straße … in F1 gekauft wurde. Die entsprechende SIM-Karte wurde, wie sich aus der Auswertung der Asservate ergibt, in der Wohnung des Angeklagten in S1 sichergestellt. 229 230

- Der Zeuge E4 hat weiterhin glaubhaft bekundet, dass die Überwachung des Gerätes mit der vorbenannten IMEI ergeben habe, dass dieses ab dem 26.02.2015 mit der Rufnummer … genutzt worden sei. Diese Aussage wird bestätigt und ergänzt durch den Inhalt des Aktenvermerks vom 26.02.2015 zu den Ergebnissen der seinerzeitigen Telekommunikationsüberwachung. Aus dem Aktenvermerk des Zeugen E4 vom 27.02.2015 ergibt sich hieran anschließend, dass die auf -**…** endende Rufnummer später in einem Gerät mit der IMEI … verwendet wurde. Im Hinblick auf den Wechsel der Geräte und Rufnummern hat der Zeuge E4 auf der Grundlage der von ihm durchgeführten bzw. ausgewerteten Telekommunikationsüberwachung bekundet, dass sich die Gesprächs- bzw. Chatinhalte jeweils nicht verändert hätten, woraus die Kammer den Schluss zieht, dass sämtliche vorbenannten Geräte und Rufnummern der unter L handelnden Person zuzuordnen sind. 2331 2332

- Anhand weiterer Ermittlungsmaßnahmen – wie der Zeuge E4 ebenfalls detailreich und nachvollziehbar bekundet hat – habe man den Standort des L konkret in der Wohnung der J2 an der A-Straße in F1 – wo der Angeklagte sich regelmäßig aufhielt – ausmachen können. Hierzu hat der Zeuge E4 ergänzend bekundet, mittels eines eingesetzten IMSI-Catchers habe man das Gerät mit der IMEI … im Bereich der A-Straße … in einer der oberen Etagen lokalisieren können. Dies hat zudem der Zeuge L6, der den Auftrag, die Lokalisierung durchzuführen, ausgeführt hat, in seiner Aussage bestätigt. Dieser hat detailreich und schlüssig zu Ortungstechnik und dem konkreten Auftrag ausgesagt. Den Standort des Geräts mit der auf -**…** endenden IMEI in F4 während der Aktivität dieses Gerätes hat auch der Zeuge S6, der mit der Telekommunikationsüberwachung dieses Gerätes befasst war, in seiner Aussage bestätigt. Dieser hat auf der vorbenannten Grundlage zudem bekundet, dass das vorbenannte Gerät durch L genutzt worden sei. 2333 2334

- Hiermit im Einklang stehend hat der Zeuge E4 weiterhin ausgesagt, über das Gerät mit der auf -**…** endenden IMEI habe L die Nummer … als seine Erreichbarkeit angegebenen. Im Rahmen der Telekommunikationsüberwachung zu dieser Rufnummer habe man anhand der Sprache feststellen können, dass es sich bei L – wie bei dem Angeklagten – um einen Afrikaner handele. Auch habe man Kinder im Hintergrund gehört, weshalb man im Bereich der A-Straße … eine Eingrenzung auf zwei dort wohnende afrikanische Mütter mit Kindern habe vornehmen können. Da bei der Standortbestimmung auch eine Funkzelle an der A 57 Richtung Niederlande betroffen gewesen sei, habe man das Vorhandensein eines Pkw überprüft und hierbei festgestellt, dass nur auf eine der beiden Mütter, nämlich die J2, ein Kfz angemeldet sei, dessen vorherige Überführungskennzeichen auf den Angeklagten angemeldet gewesen seien, was eine eindeutige Verbindung zwischen L und dem Angeklagten darstellt. Der Name der Frau J2 sei, so hat der Zeuge E4 hierzu ergänzend bekundet, im Rahmen der durchgeführten Telekommunikationsüberwachung auch dadurch aufgefallen, dass er von L – der mithin wie der Angeklagte mit Frau J2 in Verbindung steht – als Empfänger für eine Geldzahlung benannt worden sei. Insoweit deckt sich die Aussage des Zeugen E4 im Übrigen auch mit den Erkenntnissen aus der Telefonüberwachung zur Rufnummer …, wie sie im Aktenvermerk des Zeugen E4 vom 25.05.2015 dargelegt sind. 2335 2336

- Für die insoweit getroffenen Feststellungen sprach auch ein Abgleich zwischen der Aktivität des L im Internet in der Funkzelle in F4 mit der Anwesenheit des – GPS- 2337 2338

überwachten – Pkw der Frau J2, wie ihn der Zeuge N10 durchführt hat. Der Zeuge hat hierzu detailliert und gestützt durch im Aktenvermerk vom 04.07.2015 niedergelegte Details glaubhaft bekundet, dass bei Anwesenheit des Pkw der Frau J2 mit dem amtlichen Kennzeichen … in F1 eine Aktivität des Gerätes mit der IMEI … zu verzeichnen gewesen sei, bei Abwesenheit dessen nicht. Ergänzend hierzu hat der Zeuge E4 ausgesagt, die Daten aus der GPS-Überwachung des Fahrzeugs hätten ergeben, dass das überwachte Fahrzeug in der Nacht vom 10.05.2015 auf den 11.05.2015 von der A-Straße … in F1 zur W-Straat … in S1 – der Wohnanschrift des Angeklagten – bewegt worden sei. Der Zeuge N10 hat – was sich insoweit zwanglos einfügt – darüber hinaus bekundet, es habe ein stets ähnliches Bewegungsbild des Pkw vom Bereich der A-Straße in F1 zum Bereich der W-Straat in S1 gegeben. Aus dieser Verbindung ergibt sich zur Überzeugung der Kammer, dass die den Pkw der Frau J2 nutzende Person einerseits L, andererseits der Angeklagte ist, also eine Personenidentität vorliegt.

Für eine solche Personenidentität sprachen auch die anhand der glaubhaften Aussage des Zeugen E4 sowie der hierzu jeweils angefertigten Aktenvermerke festgestellten Ergebnisse der Auswertung mehrerer weiterer, im Rahmen des Ermittlungsverfahrens sichergestellter Asservate: 239

- Bei der Durchsuchung der Wohnung an der A-Straße wurde im Handy der Frau J2 der Kontakt „Q5 – **…**“ gefunden, der bei WhatsApp am 04.04.2016 ein Foto des Angeklagten als Profilbild zugeordnet war, was belegt, dass es sich um die Nummer des Angeklagten handelt. Im ebenfalls dort aufgefundenen C7 Handy befand sich die vorbenannte Rufnummer zudem unter dem Namen „Q6“. Diese Nummer teilte L im Chat als seine Kontaktnummer mit, woraus sich ergibt, dass es sich zugleich um die Rufnummer des L handelt. 2401

- Weiterhin wurde in der Wohnung in der A-Straße ein W3-Handy mit der IMEI … aufgefunden. In diesem wurde ab dem 09.05.2015 die vorbenannte, L zuzuordnende Rufnummer … genutzt, deren SIM-Karte ebenfalls in der Wohnung der Frau J2 aufgefunden wurde. Auch dies spricht dafür, dass der dort häufig aufhältige Angeklagte L ist, zumal sich Anhaltspunkte für eine Verbindung der J2 oder anderer Personen zu Aktivitäten von „L“ nicht ergeben haben. Dies wird auch dadurch gestützt, dass in der Wohnung an der A-Straße eine Plastikkartenhalterung zum Heraustrennen für die SIM-Karte mit der IMEI … sowie deren Umverpackung und Plastikkarte zum Heraustrennen aufgefunden wurde, welche L für Chats und die Erstellung von Bankseiten sowie Versendung von Phishingmails nutze. 2423

- Auf den in der Wohnung des Angeklagten aufgefundenen Laptop I6 und Netbook N11 wurden – wie die Auswertung der Asservate aus dieser Wohnung ergeben hat - Nachweise für einen Zugriff auf die Accounts „L“ und „N12“ gefunden. Auf dem Netbook N11 war zudem in einer Datei die Emailadresse …@....com abgespeichert. Auf dem ebenfalls in der Wohnung des Angeklagten aufgefundenen USB Stick … 16 GB fanden sich php-Skripte zur Weiterleitung von Daten an die darin hinterlegten Emailadressen …@....com, …@....com und …@....com. In der Wohnung des Angeklagten in S1 wurde die SIM-Karte zur Rufnummer …, welche L am 18.09.2015 als seine Erreichbarkeit 2445

angab, aufgefunden.

Gerade angesichts der Vielzahl der aufgefundenen Geräte in der Wohnung des Angeklagten, die auf verschiedene Weisen Verbindungen zu der als L auftretenden Person aufweisen, sowie der Angabe des Angeklagten, allein in dieser Wohnung zu wohnen, liegt es auf der Hand, dass es sich bei dem Angeklagten und L um dieselbe Person handelt. Dies gilt umso mehr, als auch in der Wohnung der J2, in der der Angeklagte sich ebenfalls regelmäßig aufhielt, Geräte aufgefunden wurden, die in Verbindung mit L stehen. 246

Die Feststellung, dass es sich bei dem Angeklagten bzw. L auch um N1 handelt, beruht auf Folgendem: 247

- In zwei in der Wohnung der gesondert Verfolgten H aufgefundenen Mobiltelefonen (O4 mit SIM M2 sowie J6) war als Kontakt jeweils „N1 - …“ abgelegt. Wie sich aus dem inhaltlich vom dem Zeugen E4 im Rahmen seiner Vernehmung bestätigten Vermerk vom 05.10.2016 betreffend die Durchsuchung der Wohnung des Angeklagten in S1 ergibt, wurde die SIM-Kartenverpackung für die SIM-Karte zu der vorbenannten Nummer bei der Durchsuchung aufgefunden, weshalb ihm diese Nummer zuzuordnen ist. Dies wiederum stellt eine naheliegende Verbindung zwischen N1 und dem Angeklagten dar. Aus der von dem Zeugen E4 bekundeten und in einem Aktenvermerk vom 26.05.2015 niedergelegten Telekommunikationsüberwachung des Gerätes mit der IMEI … ergibt sich zudem, dass L - mithin der Angeklagte - diese Nummer gegenüber einem „Q7“ als seine Erreichbarkeit angab. 248 249

- Auch wurde in der Wohnung der gesondert Verfolgten H ein Notizbuch aufgefunden, welches den handschriftlich eingetragenen Kontakt „N1 L …“ enthält, woraus die Kammer schließt, dass es sich bei dem Angeklagten, N1 und L um dieselbe Person handelt. 250 251

- Überdies ergab die Auswertung des in der Wohnung des Angeklagten in S1 sichergestellten Handys O5 mit SIM-Karte, dass mit diesem Gerät SMS empfangen wurden in denen der Empfänger einerseits – von der Firma V1 – mit N, andererseits – in einer SMS von einer nigerianischen Nummer – mit N1 angesprochen wird. Bilder aus einem Video, welches sich auf einer DVD im Computer des Angeklagten befand, zeigen den Angeklagten und darunter den Schriftzug „N1“. 252 253

- Verbindungen zwischen dem Angeklagten bzw. L und N1 ließen sich zudem den Ergebnissen der weiteren Telekommunikationsüberwachung entnehmen. Im Rahmen der Telekommunikationsüberwachung des Gerätes mit der auf -**…** endenden IMEI konnte – entsprechend den glaubhaften Bekundungen des Zeugen S6 sowie einem hierüber gefertigten Aktenvermerk vom 07.04.2015 – festgestellt werden, dass dieses Gerät am 01.04.2015 durch „N12“, vom 02.04.2015 bis 06.04.2015 durch L genutzt wurde. Der Zeuge E4 hat zudem im Hinblick auf die Ergebnisse der Überwachung der L – und damit nach dem zuvor Dargelegten dem Angeklagten zuzuordnenden – auf -**…** endenden Rufnummer glaubhaft bekundet, dass deren Nutzer sich selbst N1 genannt und mehrfach seinen Nachnamen „K1“ buchstabiert habe. 254 255

- Nach Aussage des Zeugen A2 – an deren Glaubhaftigkeit zu zweifeln die Kammer keinen Anlass hatte – war dem J7 der Angeklagte nur unter dem Namen „N1“ bekannt. 257

Gerade angesichts der Vielzahl der sich ergebenden Verbindungen verblieb in der Gesamtschau für die Kammer kein Zweifel, dass der Angeklagte, L und N1 eine Person sind und der Angeklagte unter den genannten Namen bzw. „Nicknames“ agierte. 258

Anhaltspunkte dafür, dass eine konkrete andere Person als der Angeklagte L und/oder N1 sein könnte, hat die Beweisaufnahme nicht ergeben. 259

Auch vermag die Einlassung des Angeklagten im Rahmen des Ermittlungsverfahrens, den Namen L nicht zu kennen, die insoweit getroffene Feststellung der Kammer nicht in Zweifel zu ziehen. Sie stellt sich vielmehr auch im Gesamtkontext der erfolgten Einlassung, die ersichtlich darauf gerichtet ist, jeglichen Zusammenhang mit den in Rede stehenden Taten zu negieren, angesichts der Vielzahl der festgestellten Verbindungen als Schutzbehauptung dar. 260

(2) Die gesondert Verfolgte H, Q2 und E1 sind eine Person 261

Die Kammer ist weiterhin – was ebenfalls Grundlage der weiteren Überzeugungsbildung war – davon überzeugt, dass es sich bei der gesondert Verfolgten H, Q2 und E1 um dieselbe Person handelt. 262

- Dass es sich bei der im Z-Chat als Q2 auftretenden Person um die gesondert Verfolgte H handelt, ergibt sich zur Überzeugung der Kammer zunächst insbesondere aus der glaubhaften Aussage des Zeugen E4. Dieser hat detailliert und nachvollziehbar bekundet, dass Q2 bereits im Rahmen einer sog. „open-source“-Recherche als H identifiziert werden konnte. So führte die Recherche zu „H“ in öffentlich zugänglichen Quellen im Internet zu einem Account auf der Internetseite www. … .com unter dem Namen „Q8“. Weiterhin hat der Zeuge X7 – ohne dass Zweifel an der Glaubhaftigkeit seiner detaillierten und in sich schlüssigen Aussage betreffend das Vorgehen und die Ergebnisse der Recherchen bestünden – bekundet, im Rahmen der von ihm durchgeführten „open-source“-Recherche Q9 anhand von Einträgen ebenfalls als H identifiziert zu haben. 263 264

- Der Zeuge E4 hat mit Blick auf die Ergebnisse der durchgeführten Telekommunikationsüberwachung und die Durchsuchung der Wohnung der gesondert Verfolgten H in N13 zudem bekundet, im Rahmen der Telekommunikationsüberwachung habe Q2 mitgeteilt, von ihrem Ehemann nur einmal etwas gehört zu haben, als man ihm erlaubt habe, zu telefonieren. Im Rahmen der Durchsuchung der Wohnung der gesondert Verfolgten H sei eine Besuchserlaubnis aufgefunden worden, aus der sich ergebe, dass ihr Ehemann in Norwegen in Haft sei. 265 266

- Auch der Umstand, dass – wie sich aus dem inhaltlich durch den Zeugen E4 bestätigten Aktenvermerk vom 17.10.2016 ergibt – von dem in der Wohnung der gesondert Verfolgten H aufgefundenen Laptop N14 auf das Emailpostfach „…@....com“ zugegriffen wurde, bestärkt die Annahme der Identität beider. 267 268

- 269 270

Die Auswertung eines in der Wohnung des Angeklagten in S1 aufgefundenen Handys O6 mit der IMEI … ergab zudem, dass auf dieses Gerät am 12.06.2014 von der Nummer … aus eine Nachricht des Inhaltes „…@....com“ gesendet wurde. Diese Rufnummer gab die gesondert Verfolgte H im Verfahren der Staatsanwaltschaft C8 zum Az. … als ihre Erreichbarkeit an, was ebenfalls eine naheliegende Verbindung zwischen der gesondert Verfolgten H und „Q2“ darstellt.

Bei der unter dem Namen „E1“ auftretenden Person handelt es sich zur Überzeugung der Kammer ebenfalls um die gesondert Verfolgte H. 271

- Der Angeklagte hat sich anlässlich der Verkündung des Haftbefehls dahingehend eingelassen, die gesondert Verfolgte H – wenn auch als Taxifahrgast – zu kennen. Seine Verbindung zu der gesondert Verfolgten H, der Inhalt der von ihm (alias „L“) mit ihr (alias Q2) geführten Chats sowie die Auswertung der in der Wohnung in N13 sichergestellten Asservate legten dabei nicht nur eine generelle Beteiligung der H an den Taten aus Tatkomplex A, sondern gerade ihre Funktion als „Telefonistin“ nahe. 272 273

- Für ihr Auftreten als E1 spricht die glaubhafte Aussage des Zeugen E4, der bekundet hat, eine Aufzeichnung eines im Rahmen der Telekommunikationsüberwachung geführten Gesprächs, in welchem sich die Anruferin als E1 vorgestellt habe, sei von dem in einem gleich gelagerten Umfangsverfahren in X8 ermittelnden Polizeibeamten – Herrn S7 von der Landespolizeidirektion X8 – als Stimme der gesondert Verfolgten H erkannt worden. Der angesichts der Fehleranfälligkeit einer solchen Wiedererkennensleistung nur eingeschränkte Beweiswert war der Kammer hierbei bewusst. 274 275

- Bei der Durchsuchung der Wohnung der gesondert Verfolgten H in N13 wurde zudem ein Zettel gefunden, auf welchem handschriftlich Emailaccounts nebst Passwörtern, u.a. „…@....com“, notiert waren, was eine weitere Verbindung zwischen der gesondert Verfolgten H und der als E1 auftretenden Telefonistin darstellt. 276 277

Das Ergebnis der weiteren Beweisaufnahme stand dem nicht entgegen. In der Gesamtschau der einzelnen Indizien sind der Kammer nach alledem keine Zweifel an der Identität von E1 bzw. Q2 und H geblieben. 278

(3) Der gesondert Verfolgte V und X2 sind eine Person 279

Weiterhin steht für die Kammer zweifelsfrei fest, dass es sich bei dem gesondert Verfolgten V und X2 um dieselbe Person handelt. 280

Dies folgt insbesondere aus dem Ergebnis der Telekommunikationsüberwachung der – nach dem zuvor Dargelegten dem Angeklagten zuzuordnenden – Nummer …. Hiernach teilte X2 gegenüber L im Chat am 25.05.2015 auf dessen Nachfrage seinen Namen – V – mit, der in einem späteren Telefongespräch von L auch mit „B5“ angesprochen wurde. Ergänzend hierzu wurde im Rahmen der Durchsuchung der Wohnung in der A-Straße ein Handy mit SIM-Karte sichergestellt, in welchem als Kontakt V mit seiner aus den durchgeführten Ermittlungsmaßnahmen bereits bekannten Telefonnummer abgelegt war. 281

(4) Der Angeklagte, H und V waren Mitglieder der hier in Rede stehenden Tätergruppe 282

Dass die drei vorbenannten Personen – der Angeklagte und die gesondert Verfolgten H und V – neben weiteren Personen Mitglieder der hier in Rede stehenden Tätergruppe zur Begehung von Phishingtaten waren, ergibt sich zur Überzeugung der Kammer aus den Bekundungen des Zeugen E4 zur geführten Chat-Kommunikation zwischen L und Q2 einerseits, sowie L und X2 andererseits. Seine glaubhafte, da detailreiche und plausibel nachvollziehbare Aussage wird gestützt und ergänzt durch die Ergebnisse der Auswertung der in der Wohnung des Angeklagten in S1 sichergestellten Asservate. 283

- So hat der Zeuge E4 auf der Grundlage der von ihm durchgeführten bzw. ausgewerteten Telefonüberwachung glaubhaft, da detailliert, sachlich und ohne erkennbare Widersprüche etwa bekundet, dass L und X2 sich im Chat über die Erstellung von Phishingseiten unterhalten haben, wobei klar ersichtlich gewesen sei, dass L die Anordnungen gegeben habe. Ergänzend hierzu ergibt sich aus den Ergebnissen der durchgeführten Telekommunikationsüberwachungsmaßnahmen eine in pidgin-englischer Sprache geführte Chat-Kommunikation zwischen beiden vom 13.02.2015, in welcher L X2 mitteilte, die T1 „darin“ gesehen zu haben, woraufhin dieser antwortete, zu versuchen, „das so“ zu managen. Weiterhin forderte X2 L auf, ihm etwas zu geben, damit er es ausprobieren könne, woraufhin L eine URL an ihn sandte, mitteilte, dass 60 Tage frei hochgeladen werden könne und vorgab „domain and hosting“. Hierauf teilte X2 L am 14.02.2015 eine URL mit, deren Aufruf zu einer gefälschten T1-Seite führte, was aus Sicht der Kammer keinen anderen vernünftigen Schluss zulässt, als dass beide gemeinsam an der Erstellung und dem Hochladen gefälschter Bankseiten arbeiteten. Vor diesem Hintergrund ist die Einlassung des Angeklagten im Ermittlungsverfahren, V und X2 nicht zu kennen, ebenfalls als Schutzbehauptung zu werten. 284 285

- Auch hat der Zeuge E4 bekundet und ausgeführt, es habe verfahrensrelevante Chats zwischen L und Q2 gegeben, etwa einen solchen, in welchem Q2 L gefragt habe, wann sie zusammen arbeiten würden und in welchem zugleich über „T14“ – T1 – sowie „Q10“ – Q1 Accounts – geschrieben worden sei. Weitere Chats, in denen es im Zeitraum vom 13. bis 18.01.2016 um Geld, Jobs und die T1 ging, konnten auf dem in der Wohnung des Angeklagten in S1 aufgefundenen Laptop I6 festgestellt werden. 286 287

- Auf dem in der Wohnung des Angeklagten in S1 aufgefundenen Laptop I6 konnten Fragmente einer von …@....com versandten Email vom 19.04.2015 mit einem Text, in dem es offenkundig um Phishingmails in portugiesischer Sprache ging, aufgefunden werden. Der ebenfalls in der Wohnung in S1 aufgefundene USB Stick … 16 GB enthält eine Datei namens „gin woman conversation.txt“, in welcher Chatverläufe zwischen L und Q2 bis zum 11.09.2014 abgespeichert sind, die das arbeitsteilige Vorgehen betreffen und belegen. So gibt L die Anweisungen zum Vorgehen, etwa „ok do this“, „tomorrow morning u work it and update me“, oder „call the second job“ und zur Durchführung von Anrufen. Weitere Chats betreffen die Versendung von Bankdaten von L an Q2 und eine Absprache betreffend den auf Q2 entfallenden Anteil. Sie verlangt zunächst 30%, wohingegen L ihr „25“ zugesteht. 288 289

- Im Rahmen der Telekommunikationsüberwachung festgestellte Chats vom 16.03.2015 bis zum 19.03.2015, in welchem beide sich über das Arbeiten, die D3 Bank, Logins, die X5, Anrufe, Accounts, „Express-Jobs“, Bankkonten mit Pin und Passwort und das 290 291

Ankommen von Geld unterhalten, belegt zusätzlich den Bezug der Kommunikation zwischen L und Q2 zu den verfahrensgegenständlichen Taten. Dies ergibt sich insbesondere aus der in dem Aktenvermerk des Zeugen E4 vom 23.03.2015 im Wortlaut wiedergegebenen, in der Hauptverhandlung ins Deutsche übersetzten Kommunikation, die der Zeuge als Ergebnis der insoweit durchgeführten Überwachungsmaßnahmen bestätigt hat. Im Rahmen der Telekommunikationsüberwachung konnte zudem, wie im Aktenvermerk des Zeugen N10 vom 29.06.2015 dargelegt, die Übersendung einer spanischen Kontoverbindung nebst Zugangsdaten und Passwort von L an Q2 festgestellt werden.

- Weiterhin erfolgten von der Nummer **…**, die im Rahmen von unberechtigten Kontenzugriffen als Empfangsnummer für TANs im SMS-TAN-Verfahren hinterlegt wurde, am 12.01.2015 gegen 12:00 Uhr sowie am 13.01.2015 gegen 16:30 Uhr Anrufe auf die für Anrufe bei Bankkunden genutzte Nummer …. Dies ergibt sich aus dem Inhalt des auf rückwirkenden Verbindungsdaten beruhenden Aktenvermerks des Zeugen E4 vom 22.10.2015, dessen Inhalt der Zeuge bestätigte. Zu dieser Zeit konnte die Rufnummer **…** in F4 lokalisiert werden, während im selben Zeitraum, nämlich am 13.01.2015 um 15:52:35 Uhr, H alias „E1“ von der Nummer … aus auf der Nummer des Zeugen E3 anrief. Auch diese zeitlichen und örtlichen Zusammenhänge – die A-Straße … befindet sich im Stadtteil F4 – sprachen aus Sicht der Kammer für eine Abstimmung des Angeklagten mit der gesondert Verfolgten H im Hinblick auf verfahrensgegenständliche Taten. 292 293

Vor dem Hintergrund der Vielzahl der zu ziehenden Verbindungen zwischen L und Q2 und insbesondere der belegten Chatinhalte erscheint die Einlassung des Angeklagten, die gesondert Verfolgte H lediglich als Taxifahrgast zu kennen, als Schutzbehauptung. Seine Einlassung vermag – ebenso wie das übrige Ergebnis der Beweisaufnahme – die auf der dargestellten Grundlage gebildete Überzeugung der Kammer von einem Zusammenwirken der Beiden zum Zwecke der Begehung von Phishingtaten nicht in Zweifel zu ziehen. 294

(5) Aufgabenteilung innerhalb der Tätergruppe 295

Die Feststellungen der Kammer zur Aufgabenteilung innerhalb der Tätergruppe beruhen insbesondere auf den Ergebnissen der Auswertung der bei den Durchsuchungen sichergestellten Geräte, den Ergebnissen der Telekommunikationsüberwachung, den Aussagen der Zeugen E4, X7 und B4 sowie der Gesamtschau der Ergebnisse der einzelnen Erkenntnisquellen, die insoweit ein einheitliches, in sich schlüssiges Bild zeichneten. 296

(a) Erlangung von Emailadressen durch den Angeklagten 297

Dass dem Angeklagten die Aufgabe zukam, Empfängeremailadressen zur Versendung der Phishingmails zu besorgen, ergibt sich zur Überzeugung der Kammer insbesondere aus einer Gesamtschau der folgenden Umstände: 298

- Auf dem PC I6, welcher in der Wohnung des J2 in der A-Straße aufgefunden wurde, war das Programm … installiert und wurde – jedenfalls im Zeitraum Oktober 2015 bis Februar 2016 –mehrfach verwendet. Dieses Programm durchsucht Internetseiten nach Emailadressen, sammelt diese und speichert sie in Textdateien ab. Überdies war auf dem in der Wohnung des Angeklagten in S1 im Rahmen der Durchsuchung 309 310

aufgefundenen Computer B6 das ebendiesem Zweck dienende Programm … installiert und – wie der Zeuge X7 glaubhaft bekundet hat – zur Zeit der Durchsuchung aktiv.

- Aus der Auswertung der Asservate betreffend die Wohnung des Angeklagten in S1 ergibt sich darüber hinaus, dass sich auf dem vorbenannten Computer das Programm … mit 78 Unterverzeichnissen, in denen Suchläufe nach Emailadressen protokolliert waren, befand. Ebenso auf dem dort sichergestellten USB Stick … 8 GB, dessen Protokolldateien auf eine Nutzung im Zeitraum vom 20.01. bis 12.03.2014 hinweisen. Auf dem ebenfalls sichergestellten USB Stick 2 GB befand sich wiederum das Programm …, dessen Protokolldateien ein Scannen nach Emailadressen seit September 2009 belegen. 301 302

- Dateien mit Empfängeremailadressen, etwa die Datei „German recent 1millio200thousand.txt“, fanden sich auf dem in der Wohnung des Angeklagten sichergestellten USB Stick … 2 GB sowie auch auf dem sichergestellten Netbook N11. Auch hier fand sich das Programm …, dessen Protokolldateien Suchläufe im Zeitraum vom 23.01.2014 bis 18.02.2014 auswiesen. 303 304

- Ergänzend ergeben sich auch Anhaltspunkte für eine Emailadressenerlangung durch den Angeklagten aus der Telekommunikationsüberwachung zu dem Gerät mit der auf -**…** endenden IMEI. Aus dem Aktenvermerk des Zeugen S6 vom 01.04.2015 lässt sich – wie dieser im Rahmen seiner Aussage auch bestätigt hat – entnehmen, dass der Nutzer dieses Gerätes – mithin L – sich vermehrt auf Webseiten mit einer größeren Anzahl von fremden Emailadressen – so etwa am 31.03.2015 auf der Seite www…..de/…/…/….htm aufhielt. 305 306

Bei der Gesamtschau der insoweit maßgeblichen Umstände verblieben - schon aufgrund der Vielzahl der aufgefundenen Geräte, die das Programm … oder Dateien aus diesem Programm enthielten – für die Kammer keine begründeten Zweifel, dass es die Aufgabe des Angeklagten war, Email-Adressen zu „sammeln“, die später auch dem Versand der verfahrensgegenständlichen Phishingmails dienten. 307

(b) Platzierung von Phishingseiten auf fremden Servern durch den Angeklagten 308

- Dass dem Angeklagten darüber hinaus die Aufgabe zukam, die erstellten Phishingseiten auf fremden Servern zu platzieren, ergibt sich insbesondere aus der glaubhaften Aussage des Zeugen E4. Dieser hat bekundet, im Rahmen der umfangreichen durchgeführten TKÜ-Maßnahmen sei festgestellt worden, dass L auf fremde Server zugegriffen habe und sich zudem aus einer Auswertung von Datenprotokollen ergeben habe, dass die hochgeladenen php-Skripte teilweise mit dem Vermerk „from L“ versehen gewesen seien, was auf den Angeklagten hinweist. Dies wird zudem gestützt durch den bereits dargelegten Chat, wonach L X2 – im Zusammenhang mit der Erwähnung der „T1“ und einem freien Hochladen für 60 Tage – eine URL übersandte und als Anweisung „domain and hosting“ vorgab. 309 310

- 311 312

Aus der Auswertung der in der Wohnung des Angeklagten sichergestellten Asservate ergibt sich hierzu ergänzend, dass der Angeklagte über so genannte „Cpanels“, die dem unberechtigten Zugriff auf Server dienen, um dort Seiten zu platzieren, verfügte. Auch fanden sich Dateien mit einer Vielzahl gefälschter Bankseiten nebst php-Skripten. Den Erwerb solcher CPanels bestätigt auch die zu dem Gerät mit der auf -**…** endenden IMEI durchgeführte Telekommunikationsüberwachung. Hierzu ergänzend ergibt sich aus der durchgeführten Telekommunikationsüberwachung betreffend das Gerät mit der auf -**…** endenden IMEI, wie in den Aktenvermerken des Zeugen S6 vom 01.04.2015 und 02.04.2015 niedergelegt und inhaltlich im Rahmen seiner Vernehmung bestätigt, dass der Nutzer dieses Gerätes – also L – sowohl am 30.03.2015 als auch am 31.03.2015 jeweils T1-Phishingseiten ins Internet brachte. Diese legte er auf den Seiten http://....de bzw. http://....de/ ab und testete deren Funktionalität.

- Im Rahmen der Telekommunikationsüberwachung konnte auch ein Upload gefälschter Bankseiten durch L auf die Domain http://....org, die in einer Datei auf dem in der Wohnung des Angeklagten sichergestellten USB Stick … 8 GB zu finden war, festgestellt werden. Gleiche Vorgehensweisen konnten im Rahmen der Überwachung der Rufnummer … im Zeitraum vom 13. bis 18.03.2015, wie im Aktenvermerk des Zeugen E4 vom 20.03.2015 dargelegt und von ihm im Rahmen der Vernehmung bestätigt, festgestellt werden. 313 314

(c) Aufbereitung der „abgephishten“ Daten durch den Angeklagten 315

Die Feststellungen zu der Auswertung und Aufbereitung der über die php-Skripte in tätereigene Emailpostfächer geleiteten Daten durch den Angeklagten beruhen insbesondere auf einer Gesamtschau der folgenden Umstände: 316

- Bei der Auswertung des in der Wohnung des Angeklagten in S1 sichergestellten Laptop I6 konnten webbasierte Zugriffe auf die Emailpostfächer …@....com, …@....com, …@....com, …@....com, …@....de, …@....com und …@....com von dem vorbenannten Laptop aus festgestellt werden. Die Zugangsdaten zu einigen der vorbenannten Emailpostfächer konnten dem ebenfalls in der Wohnung in S1 sichergestellten USB Stick … 8 GB entnommen werden. 317 318

- Die Emailadresse …@....com gab L, wie sich aus den Telekommunikationsmaßnahmen zum Gerät mit der auf -**…** endenden IMEI gemäß dem Aktenvermerk des Zeugen E4 vom 26.05.2015 ergibt und durch den Zeugen bestätigt wurde, gegenüber einem „Q7“ auf dessen Nachfrage nach seiner Emailadresse an. Darauf, dass der Angeklagte von dem vorbenannten Laptop auf die in Rede stehenden Emailpostfächer zugegriffen hat, lässt auch die Aussage des Zeugen E4 schließen, der bekundet hat, dass für das Email-Account …@....com die dem Angeklagten zuzuordnende, auf -**…** endende Rufnummer hinterlegt wurde. 319 320

- Zudem ergab die Auswertung der Emailpostfächer …@....com, …@....com und …@....com ergab – wie bereits dargelegt – nach der glaubhaften Aussage des Zeugen B4, dass sich hierin Emails mit „abgephishten“ Datensätzen befanden. Dies hat auch die Aussage des Zeugen E4, der auf der Grundlage der von ihm durchgeführten 321 322

Ermittlungen insoweit zusammenfassende Angaben machen konnte, bestätigt. Gleiches gilt – wie der Zeuge B4 auf der Grundlage seiner auch insoweit erfolgten Auswertung weiter bekundet hat – auch für die Emailpostfächer …@....de – in der auch eine Aktivierungsemail und 9 Benachrichtigungen für den Benutzernamen „L8“, was auf den Nutzer L schließen lässt, vorhanden gewesen seien - und …@....com.

- Php-Skripte, die zu ebenfalls aufgefundenen gefälschten Bankseiten passten und die Daten in einen Teil der vorbenannten Emailpostfächer leiteten, fanden sich auf dem in der Wohnung des Angeklagten in S1 aufgefundenen USB Stick … 16 GB und USB Stick „schwarz mit silberner Kette“. Auf dem USB Stick „schwarz mit silberner Kette“ fanden sich weiterhin die Zugangsdaten zu dem Outlook-Account …@....com, was zusätzlich auf eine Verwendung durch den Angeklagten schließen lässt. 3224

- Auch die Erkenntnisse aus der Telekommunikationsüberwachung des L zuzuordnenden Geräts mit der auf -**…** endenden IMEI stehen hiermit in Einklang. Den hierüber gefertigten und von ihm als inhaltlich zutreffend bestätigten Aktenvermerken des Zeugen S6 01.04.2015 und 02.04.2015 ist insoweit zu entnehmen, dass die von dem Nutzer am 30.03.2015 und am 31.03.2015 ins Internet gebrachten T1-Phishingseiten jeweils mit einem php-Skript hinterlegt waren, welches die eingegebenen Daten in die Emailpostfächer …@....com und …@....com weiterleitete. 3226

In der Gesamtschau der Umstände, dass mithin die mittels php-Skripten abgephishten Daten in die eingangs benannten Postfächer geleitet wurden, auf die der Angeklagte Zugriff hatte und Zugriff nahm, hat die Kammer keinen Zweifel, dass der Angeklagte derjenige war, der die abgephishten Daten zur Weiterleitung und Instruktion der Telefonistinnen aufbereitete. 327

Dies gilt umso mehr als sich auf dem in der Wohnung des Angeklagten sichergestellten USB Stick … 16 GB in einer auf den 22.09.2014 datierenden Datei namens „gin woman info.txt“ ebensolche bereits aufbereiteten Datensätze von Bankkunden fanden. Neben PIN, Namen und weiteren persönlichen Daten enthielt diese Datei Anmerkungen zu den einzelnen Datensätzen wie „1k800 sms changeable send to ugin woman“ oder „1300 tan send gin woman“. Diese Anmerkungen beziehen sich offenkundig auf verfügbare Beträge, das genutzte TAN-Verfahren sowie den Mitteilungsstatus gegenüber „gin woman“ und legen daher auch nahe, dass sich der Angeklagte – entsprechend den getroffenen Feststellungen – bereits einen ersten Zugriff auf die in Rede stehenden Konten verschafft hatte. Auf dem vorbenannten USB Stick … 8 GB befanden sich darüber hinaus Kontodaten deutscher Konteninhaber. 328

Weiterhin ergab die Auswertung der in der Wohnung der Frau J2 in der A-Straße – wo der Angeklagte sich ebenfalls aufhielt – aufgefundenen Geräte – wie im Aktenvermerk des Zeugen E4 vom 18.08.2016 dargelegt –, dass sich auch auf einem dort aufgefundenen J8 aus 8 verschiedenen Google-Mail-Accounts stammende Personal- und Online-Banking-Zugangsdaten betreffend den Zeitraum vom 29.06.2011 bis zum 28.09.2013 befanden. 329

(d) Massenhafte Versendung der Phishingmails durch den Angeklagten 330

Die Feststellung zur massenhaften Versendung von Phishingmails durch den Angeklagten beruht im Wesentlichen auf den Ergebnissen der Auswertung der in der Wohnung des Angeklagten aufgefundenen Asservate. So befanden sich auf dem sichergestellten Laptop I6 331

und auf dem USB Stick … 16 GB jeweils Texte von Phishingmails, auf letztgenanntem zudem Zugangsdaten zu smpt-Servern, die dem massenhaften Versand von Emails dienen. Auf einem USB Stick 2 GB befanden sich die Programme „…“ und „…“, die dem massenhaften Emailversand dienen. Letztlich ergibt sich die Überzeugung der Kammer insoweit auch aus der Begehung der im Tatkomplex B abgeurteilten Taten durch den Angeklagten. Auf die dortigen Ausführungen wird zur Vermeidung von Wiederholungen verwiesen.

(e) Bedeutung des Angeklagten für den weiteren Tatverlauf 332

Die festgestellte Bedeutung des Angeklagten auch für den weiteren Tatverlauf ergibt sich insbesondere aus den bereits dargelegten Erkenntnissen aus Telekommunikationsüberwachungsmaßnahmen sowie der Auswertung der Asservate aus der Durchsuchung der Wohnung des Angeklagten. Hieraus ergeben sich – wie bereits dargelegt – Anweisungen des L gegenüber X2 im Hinblick auf die Erstellung von Phishingseiten und deren „Upload“, Anweisungen zur Durchführung von Anrufen nebst Übersendung von Bankdaten sowie Entscheidungen zur Beteiligungshöhe gegenüber Q2. Auch die glaubhafte, weil detaillierte, in sich schlüssige und sachliche Aussage des Zeugen A2, der insoweit bekundet hat, der Angeklagte habe dem J7 gemäß dessen Angaben ein Empfängerkonto im Zusammenhang mit Überweisungsträgerbetrügereien mitgeteilt, lässt sich hiermit zwanglos in Einklang bringen. Dies zeigt, dass der Angeklagte über Zugang zu Empfängerkonten verfügte, wie sie auch für die verfahrensgegenständlichen Überweisungen benötigt wurden. 333

(f) Erstellung von Phishingseiten durch den gesondert Verfolgten V 334

Dass V alias X2 die Aufgabe zukam, Phishingseiten zu erstellen und nach Absprache mit dem Angeklagten hochzuladen, ergibt sich zur Überzeugung der Kammer aus den bereits dargelegten Chats zwischen L und X2 über die Erstellung solcher Seiten im Internet. Insoweit wird auf die obigen Ausführungen verwiesen. 335

Auch belegen weitere, im Rahmen der Telekommunikationsmaßnahmen bekannt gewordene Chats zwischen X2 und L eine intensive gemeinsame Beschäftigung mit der Erstellung von Phishingseiten. So ist etwa einem in die Hauptverhandlung eingeführten Chat zu entnehmen, dass X2 L um die Prüfung der Links „…“ und „http://...“, bei denen es sich um eine Phishingseite der T1 und eine der schweizer Q1 handelte, aufgrund seiner langsamen Internetverbindung bat. Auch dies legte eine Erstellung der Seiten durch V und eine Überprüfung durch den Angeklagten nahe. 336

Zwangslos fügt sich insoweit der Umstand ein, dass sich – nach der Auswertung der in der Wohnung des Angeklagten sichergestellten Asservate – auf dem sichergestellten USB Stick … 2 GB eine Datei namens „B5 details and link.txt“ befand, deren Inhalt URLs waren, auf denen gefälschte Bankseiten hochgeladen wurden. 337

(g) Durchführung der Telefonanrufe und TAN-Eingabe durch die gesondert verfolgte H 338

Als Telefonistin kam der gesondert Verfolgten H zur Überzeugung der Kammer neben der Ausführung der Telefonanrufe bei den Bankkunden auch die Aufgabe zu, die Überweisung bzw. Rufnummernänderung vorzubereiten und den TAN-pflichtigen Vorgang durch Eingabe der erlisteten TANs freizugeben. 339

Dies steht im Einklang mit den Ergebnissen der Auswertung der Asservate, welche in der Wohnung des Angeklagten aufgefunden wurden. So enthält der USB Stick … 16 GB – wie bereits dargelegt – Chatverläufe zwischen L und Q2, aus denen sich ergibt, dass Q2 von L 340

Kontendaten sowie die Anweisung erhält, Anrufe durchzuführen, was diese bestätigt.

Die Aufgabe der gesondert Verfolgten H ergibt sich zudem aus der Zuordnung des Aliasnamens „E1“, die, wie ebenfalls bereits dargelegt, sich in zumindest zwei der in Tatkomplex A abgeurteilten Fälle ausdrücklich als solche im Telefonat vorstellte. 341

Die Kammer hat in diesem Zusammenhang auch geprüft, ob es sich bei dem Namen „E1“ um einen von mehreren Telefonistinnen verwendeten Aliasnamen gehandelt haben könnte. Konkrete Anhaltspunkte für ein solches Geschehen hat die Beweisaufnahme jedoch nicht ergeben. 342

Gegen eine solche Annahme sprachen vielmehr die ausführlichen und nachvollziehbaren Ausführungen der Sprachsachverständigen B7 in ihrem Gutachten vom 29.06.2016, denen sich die Kammer im Ergebnis nach eigener Prüfung anschließt. Die Sachverständige hat eine stimmenvergleichende Begutachtung von 21 Sprachaufzeichnungen durchgeführt, in denen die Sprechende sich jeweils als Mitarbeiterin eines Geldinstitutes vorstellt. Diese Aufzeichnungen stammten – dies ergibt sich aus dem Antrag auf Erstellung eines Behördengutachtens zur Stimmanalyse beim LKA NRW vom 28.01.2015 – einerseits aus Aufzeichnungen im Rahmen der im vorliegenden Ermittlungsverfahren durchgeführten Telekommunikationsüberwachung, andererseits aus Aufzeichnungen im Rahmen der Telekommunikationsüberwachung in einem anderen Verfahren außerhalb Deutschlands. Auf der Grundlage von Analysen der drei Bereiche des verbalen Verhaltens des Menschen – Stimme, Sprache und Sprechweise – ist die Sachverständige in sich schlüssig und widerspruchsfrei zu dem Ergebnis gelangt, dass die untersuchten Aufzeichnungen mit hoher Wahrscheinlichkeit drei verschiedenen Sprecherinnen – „E1“, „S8“ und „C9“ – zuzuordnen sind. Dies belegt zugleich, dass es neben der gesondert Verfolgten H weitere Telefonistinnen innerhalb der Tätergruppe gab. Innerhalb der einzelnen Sprechergruppen – E1, S8 und C9 – bestehe mit hoher Wahrscheinlichkeit jeweils Sprecheridentität. E1 und S8 seien dabei sowohl Aufzeichnungen aus dem vorliegenden, als auch aus dem ausländischen Ermittlungsverfahren zuzuordnen. C9 seien nur zwei Aufnahmen des ausländischen Ermittlungsverfahrens zuzuordnen. In diesem Zusammenhang hat die Sachverständige sich auch mit der Qualität der ihr vorliegenden Aufzeichnungen und fehlendem Vergleichsmaterial befasst und im Hinblick hierauf die Herabsetzung des Wahrscheinlichkeitsgrades der Gutachtenaussage berücksichtigt. Die Sachverständige hat vergleichend ausgeführt, dass die Stimmhöhe der E1 geringfügig tiefer sei als die Stimmhöhe der S8, jedoch höher als diejenige der C9. Dies belege die Stimmbandgrundfrequenz, also das akustische Korrelat der Stimmhöhe, welche instrumentalphonetisch gemessen werden kann und deren Mittelwert und Grenzen von anatomischen und situativen Faktoren abhängen. Für die E1 zuzuordnenden Stimmproben liege die Frequenz bei 200 bis 233 Hz, für die S8 zuzuordnenden Stimmproben bei 238 bis 266 Hz und für die beiden C9 zuzuordnenden Stimmproben bei 184 und 192 Hz. Auch die Grade der im Kehlkopf wirkenden Kräfte (laryngeales Setting) wichen voneinander ab: die Stimmqualität sei bei den Frau C9 zuzuordnenden Aufzeichnungen höher als bei denjenigen, die Frau E1 zuzuordnen seien. In Gesprächen der Frau C9 finde sich die Stimmqualität der Rauheit nicht. Gefundene sprachlich-lautliche Übereinstimmungen zwischen den Sprachproben seien nicht hochgradig sprecheridentifizierend. In Bezug auf habituelle Floskeln, die ein potentes sprecheridentifizierendes Merkmal seien, ließen sich innerhalb der Gruppierungen – E1, S8 und C9 – deutliche Übereinstimmungen finden, zwischen diesen deutliche Abweichungen, insbesondere im Hinblick auf die Reihenfolge der Begrüßungsinformationen und die Verabschiedung, aber auch im Hinblick auf Füllungen von Pausen des Redeflusses (Häsitationsphänomene). Das hörbare Atemverhalten der Frau E1 weiche in Häufigkeit und Ausprägung von den Frau S8 und Frau C9 zuzuordnenden 343

Aufzeichnungen ab.

gg) Die einzelnen im Tatkomplex A abgeurteilten Fälle 344

Die Feststellungen zu den einzelnen im Tatkomplex A abgeurteilten Fällen beruhen insbesondere auf den detailreichen, sachlichen und plausibel nachvollziehbaren Aussagen der vernommenen Bankkunden zu den im Tatkomplex abgeurteilten Fällen, soweit diese hierzu aufgrund eigener Wahrnehmung eigene Angaben machen konnten, ferner auf den jeweils verlesenen bzw. in Augenschein genommenen Dokumenten. Hierzu zählen insbesondere Ausdrucke von Phishingmails, Kontenauszüge und Umsatzanzeigen für Einzelumsätze, die jeweils den Empfänger, die Empfänger-IBAN, den Zeitpunkt und die Höhe der Überweisungen, sowie verwendete TANs ausweisen, Schadensfallmeldungen der T1 und Geschäftsvorfallsdetails-Auskünfte der T1, Übersichten aus rückwirkenden Verbindungsdaten und Protokollen durchgeführter Telefonüberwachungsmaßnahmen, die Zeitpunkte, Dauer und Inhalte der Gespräche belegen. Diese Dokumente stützten und ergänzten die Bekundungen der Zeugen in Details und fügten sich zwanglos in das jeweils festgestellte Tatgeschehen. 345

Soweit einzelne Zeugen bekundet haben, keine Email erhalten, dem Link nicht gefolgt zu sein, ihre Daten auf der Phishingseite nicht eingegeben oder im Telefonat keine TAN herausgegeben zu haben oder insoweit keine Erinnerung zu haben, beruhen die Feststellungen auf der bereits dargelegten Überzeugung der Kammer hinsichtlich der identischen Vorgehensweise sowie dem noch darzulegenden Umstand, dass alle im Tatkomplex A abgeurteilten Fälle durch dieselbe Tätergruppe unter Einschluss des Angeklagten begangen wurden. 346

- Soweit der Zeuge N5 sich – ebenso wie die Zeugen I, I2, L7, H2 und T13 – an den Erhalt einer Email lediglich nicht sicher erinnern konnte, steht dies der Überzeugung der Kammer, dass auch diese Zeugen eine Email erhalten haben, nicht entgegen. Soweit die Zeugen X3, S2 und M1 sich nicht daran erinnern konnten, dem Link gefolgt zu sein bzw. ihre Daten auf der Phishingseite eingegeben zu haben, gilt dasselbe. Die teilweise fehlende Erinnerung der Zeugen führt nicht zu der Annahme, dass die jeweiligen Zeugen eine Email nicht erhalten hätten, dem Link nicht gefolgt wären oder ihre Daten nicht eingegeben hätten. Insoweit wird zur Vermeidung von Wiederholungen auf die obigen Ausführungen zu **aa)** verwiesen. 347 348

- Dass die Zeugen H1, C5, I, I2, L7, H2 und T13 ausgesagt haben, ihre persönlichen Daten nicht auf einer vermeintlich von der T1 stammenden Seite eingegeben zu haben, bzw. dass der Zeuge G1 ausgesagt hat, bereits keine Email bekommen zu haben, begründet ebenfalls keine durchgreifenden Zweifel der Kammer an den getroffenen Feststellungen. Abgesehen davon, dass, wie bereits dargelegt, anderenfalls nicht erklärlich wäre, wie die Tätergruppe sonst an die zwingend erforderlichen Kontenzugangsdaten der Zeugen gelangt sein sollte, steht zur Überzeugung der Kammer fest, dass alle vorliegend zum Tatkomplex A abgeurteilten Fälle von derselben Tätergruppe nach demselben modus operandi begangen wurden (vgl. dazu im Einzelnen unter **hh)**). 349 350

- 351 352

Entsprechendes gilt auch für die Aussage der Zeugin T13, die bekundet hat, der von ihr herausgegebene „Code“ habe sowohl Buchstaben als auch Zahlen enthalten, sowie die Aussagen der Zeuginnen H1 und L7, die angegeben haben, keine TAN oder sonstige Ziffernfolge herausgegeben zu haben. Die Kammer hat hierbei auch berücksichtigt, dass die Zeugin H1 – wie sie glaubhaft bekundet hat – nach Entdeckung der unberechtigten Überweisungen psychisch für einen Zeitraum von etwa drei Monaten beeinträchtigt war und die Zeugin L7, der Aussage des Zeugen L4 zufolge, zum Zeitpunkt der in Rede stehenden Anrufe gesundheitlich angeschlagen war, wobei sich dies auch auf ihre Konzentrationsfähigkeit auswirkte. Zudem hat der Zeuge L4 glaubhaft bekundet, seine Frau habe ihm gegenüber nach dem Telefonat sehr wohl angegeben, dass es um eine Aktualisierung und um TANs gegangen sei. Anhaltspunkte dafür, dass die erforderliche TAN seitens der Tätergruppe anders als durch die Herausgabe während des Telefonats erlangt wurde, hat die Beweisaufnahme demgegenüber nicht ergeben.

Die Feststellungen zu dem späteren Ersatz der abgebuchten Beträge aus einem internen Sicherungsfonds der T1 beruhen auf den diesbezüglichen Angaben der betroffenen Kunden sowie den Angaben des Zeugen T4. So haben die hierzu vernommenen Kunden übereinstimmend berichtet, die abgebuchten Beträge seien ihnen – in der Regel mehrere Wochen später – auf ihrem Konto wieder gutgeschrieben worden. Der Zeuge T16, Mitarbeiter der Abt. Electronic Banking Center der T15, hat hierzu bestätigt, dass für Schadensfälle u.a. infolge „Phishing“ ein überregionaler Sicherungsfonds der T1 eingerichtet ist, durch den betroffenen Bankkunden im bankseitigen Interesse des Vertrauens der Kunden in sichere elektronische Bankgeschäfte bis zur Grenze der vorsätzlichen Schadenszufügung im Kulanzwege entschädigt werden, ohne dass ein diesbezüglicher Rechtsanspruch bestehe. 353

hh) Begehung aller im Tatkomplex A abgeurteilter Fälle durch dieselbe Tätergruppe 354

Dass alle im Tatkomplex A abgeurteilten Fälle durch dieselbe Tätergruppe begangen wurden, steht zur Überzeugung der Kammer aufgrund der Zusammenhänge der einzelnen festgestellten Fälle fest. Abgesehen von den einerseits in den Fällen des SMS-TAN-Verfahrens, andererseits in den Fällen des Chip-TAN-Verfahrens jeweils von den zum Tatkomplex A vernommenen Bankkunden im Kern übereinstimmend bekundeten – in wesentlichen Teilen formalisiert wirkenden – Gesprächsabläufen in den unautorisierten Überweisungen vorangehenden Telefonanrufen, stehen alle zum Tatkomplex A abgeurteilten Fälle aufgrund verschiedener übereinstimmender Merkmale nach den getroffenen Feststellungen miteinander in Verbindung. 355

- So wurden die Zeugen G1 (**Fall 1**), I2 (**Fall 3**), T4 (**Fall 4**), X3 (**Fälle 5 und 6**), N5 (**Fall 7**), I3 (**Fälle 10 und 11**), H1 (**Fälle 12 bis 20**), L7 (**Fall 21**), H2 (**Fall 22**), C5 (**Fall 23**) und M1 (**Fall 24**) vor den nicht autorisierten Überweisungen jeweils von der Nummer **…** aus von einer vermeintlichen Mitarbeiterin der T1 angerufen. Von eben dieser Nummer aus erhielt auch die Zeugen I (**Fall 2**) einen Anruf, wenn dieser auch unbeantwortet blieb und diese Nummer bei dem folgenden Anruf nicht angezeigt wurde. Soweit die Zeugen T4 und N5 jeweils zudem einen Anruf von der Nummer … erhielten, handelt es sich bei dieser Nummer nach der entsprechenden Bekundung des Zeugen E4 sowie ausweislich des Aktenvermerks des Zeugen E4 vom 12.02.2015 um eine solche Nummer, die bei der Firma W1 für die Weiterleitung über die Nummer … hinterlegt war. 356 357

- 358 359

In den Fällen X3, I3 und H1 wurde täterseits die Empfängernummer für den Empfang von TANs per SMS jeweils hin zur Nummer **…** geändert.

- Im Fall T13 (**Fälle 26 und 27**) wurde eine Überweisung an „**N4**“ durchgeführt, wie auch im Fall X3. Die Empfängernummer für TANs per SMS wurde täterseits – wie auch in den Fällen E3 (**Fall 25**) und L5 (**Fälle 28 und 29**) – auf die Nummer **…** umgestellt. 360 361

- Von dem Konto des Zeugen S2 (**Fälle 8 und 9**) wurde eine Überweisung an „**B2**“ durchgeführt. Ein namensähnlicher Überweisungsempfänger wurde auch bei einer gestoppten Überweisung im Fall X3 (B) und bei einer Überweisung im Fall H1 (B3) angegeben. Im Fall H1 erfolgten weiterhin Überweisungen an eine **K** wie im Fall T4, an einen **D1** wie im Fall X3 und an **L3** wie im Fall I3. 362 363

- Dem Zeugen E3 stellte die Anruferin sich als „E1“ vor, ebenso wie eine Anruferin bei dem Zeugen G1 es unter Bezugnahme auf ein zuvor geführtes Telefonat in einem Anruf nach Durchführung der nicht autorisierten Überweisung tat. 364 365

ii) Beteiligung des Angeklagten an den verfahrensgegenständlichen Taten 366

Die Kammer ist aufgrund einer Gesamtschau aller bereits genannten sowie der folgenden Umstände zudem der sicheren Überzeugung, dass der Angeklagte als Mitglied der Tätergruppe auf die vorbeschriebene Art und Weise auch an den verfahrensgegenständlichen Taten beteiligt war: 367

- Hierfür sprach zunächst die bereits ausgeführte Verbindung des Angeklagten zu der gesondert Verfolgten H alias Q2 bzw. E1 sowie der Umstand, dass sich die Telefonistin in verfahrensgegenständlichen Anrufen auch als E1 vorstellte. Da – wie ebenfalls bereits ausgeführt – die Kammer davon überzeugt ist, dass sämtliche im Tatkomplex A abgeurteilten Fälle durch dieselbe Tätergruppe begangen wurden, lag schon von daher nahe, dass auch die übrigen zum Tatkomplex A begangenen Taten unter entsprechender Mitwirkung des Angeklagten begangen wurden. 368 369

- Darüber hinaus spricht für die Beteiligung des Angeklagten an den im Tatkomplex A abgeurteilten Fällen auch, dass die in der Funkzelle F4 – dem Wohnort der J2 und regelmäßigem Aufenthaltsort des Angeklagten - von L genutzte Mobilfunknummer … von der Tätergruppe als Empfängernummer für TANs in den Fällen E3, T13 und L5 (Fälle 25 bis 29) verwendet wurde. Unter Berücksichtigung der im Übrigen gegebenen Parallelen und Verbindungen unter den einzelnen Fällen sprach auch dieser Umstand für einen Bezug des Angeklagten zu den verfahrensgegenständlichen Taten. Auch insoweit wird zur Vermeidung von Wiederholungen ergänzend auf die obigen Ausführungen verwiesen. 370 371

- Die Rufnummer **…**, von der aus die Zeugin L5 (**Fälle 28 und 29**) – wie sich aus den insoweit verlesenen Dokumenten ergibt – angerufen wurde, ist nach dem Vermerk des Zeugen E4 vom 28.05.2015, dessen Inhalt durch bestätigt wurde, eine solche des Anbieters W1, für die unter anderem die niederländische Telefonnummer … hinterlegt 372 373

wurde. Von dieser niederländischen Nummer aus erfolgte am 05.05.2015 nach dem Ergebnis der Telekommunikationsüberwachung ein Anruf auf die dem Angeklagten zuzuordnende Mobilfunknummer ….

- Die Bankverbindung des Empfängerkontos für die unberechtigte Überweisung im Fall G1 (**Fall 1**) wurde von L an Q2 mitgeteilt, wie sich aus der Auswertung der Asservate aus der Wohnung des Angeklagten ergibt. Der Chat, in welchem die Mitteilung erfolgte, war auf dem sichergestellten USB Stick … 16 GB abgespeichert. 374 375

- Ebenso war dort ein Chat, in welchem L gegenüber Q2 die Kontoverbindung eines P mitteilte, die auch als Empfängerkonto im Fall I (**Fall 2**) verwendet wurde, gespeichert. 376 377

- Die persönlichen und Zugangsdaten der Zeugin I waren zudem in der Datei „gin woman info.txt“ auf dem in der Wohnung des Angeklagten in S1 sichergestellten USB Stick … 16 GB, wie sich aus der Verschriftung dieser Datei ergibt, abgespeichert. 378 379

In der Gesamtschau ergaben sich damit konkrete Bezüge des Angeklagten zu Taten sowohl zu Beginn als auch zum Ende des Tatkomplexes A. Unter Berücksichtigung dieser sowie aller weiteren genannten Umstände verblieben bei der gebotenen Gesamtschau keine begründeten Zweifel, dass der Angeklagte als Teil der Tätergruppe an sämtlichen Taten aus Tatkomplex A in der festgestellten Art und Weise beteiligt war. 380

jj) Begehung der im Tatkomplex B abgeurteilten Taten durch den Angeklagten 381

Dass der Angeklagte die im Tatkomplex B festgestellten Emails massenhaft versandte, ergibt sich insbesondere aus den Ergebnissen der durchgeführten TKÜ-Maßnahmen, der Auswertung der Asservate, sowie den glaubhaften Aussagen der Zeugen E4 und B4. 382

(1) S 383

Dass der Angeklagte in den **Fällen 30 bis 32** massenhaft Phishingmails betreffend die S versandte, ergibt sich zur Überzeugung der Kammer aus den Ergebnissen der Telekommunikationsüberwachung zur – dem Angeklagten zuzuordnenden – Rufnummer …, wie sie in den Aktenvermerken des Zeugen E4 vom 27.02.2015 und vom 02.03.2015 ausgeführt sind. Deren Inhalte hat der Zeuge E4 in seiner Aussage zudem bestätigt. Danach versandte der Angeklagte über die vorbenannte Rufnummer zwischen dem 27.02.2015 und dem 01.03.2015 massenhaft Phishingmails der S, in welchen auf ein angebliches Sicherheitsupdate hingewiesen wurde und dessen Link zu einer entsprechenden Phishingseite führte. 384

Die Zeitpunkte der Versendungen sowie die jeweilige Anzahl der versandten Emails hat die Kammer – so auch hinsichtlich der Fälle 33 bis 42 – anhand der plausiblen, sich inhaltlich deckenden und zwanglos ergänzenden Aussagen der Zeugen E4 und B4 im Hauptverhandlungstermin am 17.01.2017 festgestellt. Diese haben übereinstimmend, detailliert und ohne ersichtliche Widersprüche sowohl den Auszähl- und Auswertungsvorgang der vorhandenen Netzwerkrohdaten, als auch die Ermittlung von Tatzeiten anhand von Zeitstempeln der smpt-Vorgänge im Sinne der getroffenen Feststellungen bekundet. Insbesondere haben sie im Einzelnen und schlüssig zur Extrahierung der Daten, deren Export in ein CSV-Programm und deren Begrenzung auf die für die angeklagten Fälle 385

relevanten Inhalte unter Berücksichtigung vom Server nicht weitergeleiteter Emails ausgesagt.

Soweit eine vorherige Auswertung zu abweichenden Emailanzahlen und Versendungszeiträumen – nämlich den der Anklage zugrunde gelegten – geführt hat, stellt dies die getroffenen Feststellungen nicht in Frage. Insoweit hat der Zeuge E4 schlüssig und detailliert bekundet, aus welchem Grund die erste Auswertung unzutreffend war und wie sich die Abweichungen zur zweiten Auswertung ergeben. So hat er ausgesagt, dass bei der ersten Auswertung lediglich Stichproben ausgewertet und Hochrechnungen erfolgt seien; eine tatsächliche Auszählung im Einzelnen sei – anders als im Rahmen der zweiten Auswertung – nicht erfolgt. Bei dieser Hochrechnung sei man zudem irrtümlich davon ausgegangen, dass die Detailinformationen zu den versandten Emails jeweils lediglich die Empfänger *einer* Email auswiesen. Eine Kontrolle im Rahmen der zweiten Auswertung habe jedoch ergeben, dass Empfänger mehrerer Emails dort ausgewiesen würden, was die erste Hochrechnung verfälscht habe und bei der zweiten Auswertung berücksichtigt worden sei. Vor dem Hintergrund der Berücksichtigung und Ausräumung von Fehlerquellen aus der ersten Auswertung im Rahmen der detaillierten zweiten Auswertung steht für die Kammer sicher fest, dass die in der zweiten Auswertung ausgewiesenen Emailanzahlen die Mindestanzahl der versendeten Phishingmails darstellen. 386

Verkürzungen des Versendungszeitraums im Rahmen der zweiten Auswertung konnte der Zeuge E4 plausibel dadurch erklären, dass bei der ersten Auswertung die Zeiten der gesamten Internetsitzung protokolliert worden seien. Im Rahmen der zweiten Auswertung sei hingegen eine konkretere Eingrenzung auf die Zeiten von smpt-Verbindungen erfolgte. Der sachverständige Zeuge B4 hat zudem nachvollziehbar bekundet, dass zeitliche Verschiebungen in den Versendungszeiträumen trotz gleicher Quelldaten vorkommen könnten. Solche könnten auch aus der Zugrundelegung unterschiedlicher Zeitstempel resultieren. 387

(2) Q1 und J 388

Auch die Überzeugungen der Kammer von der massenhaften Versendung von Phishingmails betreffend die Q1 in den **Fällen 33 bis 35** und von der massenhaften Versendung von Phishingmails der J Bank im **Fall 36** ergeben sich aus den Ergebnissen der Telekommunikationsüberwachung zur Rufnummer …. Diese sind insoweit im Aktenvermerk des Zeugen E4 vom 20.03.2015 ausgeführt und wurden von ihm in seiner Aussage bestätigt. Danach versandte der Angeklagte über die vorbenannte Rufnummer zwischen dem 16.03.2015 und dem 18.03.2015 massenhaft Phishingmails der Q1 und am 18.03.2015 der J Bank, die jeweils einen Link auf die entsprechende Phishingseite enthielten. 389

Die Feststellung, dass im **Fall 37** massenhaft durch den Angeklagten Phishingmails betreffend die Q1 versendet wurden, deren Link auf Phishingseiten führte, entspricht den Ergebnissen der Telekommunikationsüberwachung des – dem Angeklagten zuzuordnenden – Gerätes mit der auf -**…** endenden IMEI, wie sie im Aktenvermerk des Zeugen S6 vom 19.05.2015 niedergelegt ist und von dem Zeugen in seiner Aussage bestätigt wurde. 390

Dass der Angeklagte in den Fällen **38 bis 41** erneut massenhaft Phishingmails betreffend die Q1 mit dem in den Feststellungen wiedergegebenen Inhalt versandte, ergibt sich zur Überzeugung der Kammer aus den Ergebnissen der Telekommunikationsüberwachung des Gerätes mit der auf -**…** endenden IMEI ist, wie sie im Aktenvermerk des Zeugen E4 vom 26.05.2015 ausgeführt sind und von diesem bestätigt wurden. Danach versandte der Angeklagte über das vorbenannte Gerät zwischen dem 25.05.2015 und dem 27.05.2015 391

massenhaft Phishingmails der Schweizer Q1 in mindestens vier gesonderte „Wellen“, in welchen auf ein angebliches Sicherheitsupdate hingewiesen wurde und dessen Link zu einer entsprechenden Phishingseite führte.

Die Feststellung, dass im **Fall 42** massenhaft durch den Angeklagten Phishingmails betreffend die Q1 versendet wurden, entspricht den Ergebnissen der Telekommunikationsüberwachung des Gerätes mit der auf -**…** endenden IMEI, wie sie im Aktenvermerk des Zeugen S6 vom 29.05.2015 ausgeführt und entsprechend den Feststellungen durch den Zeugen S6 in seiner Vernehmung bekundet wurden. 392

Die Aussagen der Zeugen E4 und S6 sind glaubhaft und werden auch durch das übrige Ergebnis der Beweisaufnahme nicht in Zweifel gezogen. Überdies stützen auch die bereits ausgeführten Ergebnisse der Auswertung der in der Wohnung des Angeklagten sichergestellten Geräte – insbesondere das Vorhandensein von Phishingmails, Zugangsdaten zu smpt-Servern, die dem massenhaften Emailversandt dienen und der Programme … und … die Überzeugung der Kammer von einem massenhaften Emailversandt durch den Angeklagten in den festgestellten Fällen. 393

(3) Anzahl der Massenversendungen 394

Dass der Angeklagte in den im Tatkomplex B abgeurteilten Taten **mindestens 13 Mal** eine massenhafte Emailversendung anstieß, folgt aus den zeitlichen Zusammenhängen sowie dem weiteren Beweisergebnis. Auch wenn der Angeklagte die Emails massenhaft etwa unter Verwendung des Programms … versandte, spricht nichts dafür, dass die Versendungen während der 13 verschiedenen Tatzeiträume allein auf einen die Versendung „anstoßenden“ Akt des Angeklagten zurückzuführen wären. 395

Hiergegen spricht bereits der von Ende Februar bis Ende Mai 2015 reichende Tatzeitraum. Gerade angesichts des Umstands, dass die Phishingseiten, auf die in den Emails enthaltene Links leiteten, sich auf fremden Servern befanden, wäre eine Platzierung einer Phishingseite im Februar für erst im Mai versandte Emails aus Tätersicht mit einem unnötigen Entdeckungs- bzw. Fehlerrisiko behaftet. 396

Abgesehen von dem Umstand, dass die Emails drei verschiedene Aussteller erkennen lassen und unterschiedliche Inhalte aufweisen, unterscheiden sich die „URLs“ der Phishingseiten, die über den in den Emails enthaltenen Link erreicht wurden, zwischen den Einzelnen „Versendungswellen“. Dies hat der Zeuge E4 auf der Grundlage seiner umfangreichen Ermittlungen und Auswertungen glaubhaft bekundet. Seine Bekundungen werden zudem gestützt durch seine die unterschiedlichen URLs der in den Emails enthaltenen Links im Einzelnen aufführenden Aktenvermerke vom 20.03.2015 und 26.05.2015, die er im Rahmen seiner Vernehmung inhaltlich bestätigt hat. Auch dies lässt darauf schließen, dass jede Massenversendung aufgrund der Abweichung zur vorherigen einzeln in Gang gesetzt wurde. 397

Überdies ergibt sich die Überzeugung der Kammer von mindestens 13 einzelnen Versendungshandlungen auch aus der glaubhaften, da detaillierten und sachlich fundierten Aussage des Zeugen B4. Dieser hat insoweit zwar bekundet, dass Versendungsprogramme wie das Programm … grundsätzlich nacheinander eine Liste von Empfängern „abarbeiten“. Emails mit verschiedenen „Bodies“ – also auch solche, die Links auf unterschiedliche Seiten enthalten – könnten gleichzeitig jedoch nur abgearbeitet werden, wenn das Programm entsprechend der Anzahl der unterschiedlichen Emailbodies mehrfach gestartet würde. 398

399

Die Feststellungen zu den einzelnen Banken – Q1, S und J – beruhen auf den jeweiligen, den Feststellungen entsprechenden öffentlich zugänglichen Informationen der Banken, wie sie in Form von Screenshots im Rahmen der Hauptverhandlung eingesehen wurden. Von niederländischen Inhalten hat die Kammer sich durch Übersetzung durch den Sprachsachverständigen I5 Kenntnis verschafft.

kk) Subjektiver Tatbestand und finanzieller Vorteil des Angeklagten 400

Dass der Angeklagte seine Tatbeiträge hinsichtlich des Tatkomplexes A auf der Grundlage eines gemeinsamen Tatplans und in Kenntnis bzw. mit dem Ziel der Verwendung der „abgephishten“ Daten zur Durchführung unautorisierter Überweisungen vornahm, folgt bereits aus den festgestellten objektiven Tatumständen. Insbesondere die Art der von ihm erbrachten Tatbeiträge, die Inhalte des Chat-Verkehrs mit den gesondert Verfolgten V und H sowie die weiteren Inhalte von ausgewerteten Daten auf den sichergestellten Asservaten lassen keinen begründeten Zweifel daran, dass der Angeklagte seine Tatbeiträge in Kenntnis und mit dem Ziel der „Abschöpfung“ der Konten im Sinne eines arbeitsteiligen Vorgehens der Gruppe einbrachte. 401

Dass auch der Angeklagte durch die Taten der Tätergruppe einen finanziellen Vorteil erstrebte und erhielt, folgt aus der Gesamtschau der gegebenen Umstände. Angesichts der Vielzahl der bei dem Angeklagten sichergestellten Geräte, die zur Ausführung seiner Tatbeiträge genutzt wurden, des insbesondere aus den durchgeführten Telekommunikationsmaßnahmen ersichtlichen immensen Zeitaufwandes des Angeklagten für die in Rede stehenden Taten und des Ergebnisses der Auswertungen der asservierten Geräte, das eine intensive Beschäftigung mit den Taten – etwa durch das Vorhandensein diverser gefälschter Phishingseiten nebst php-Skripten und diversen mit Anmerkungen versehenen Datensätzen betreffend Kontendaten – erkennen lässt, ist eine unentgeltliche Tätigkeit des Angeklagten aus Sicht der Kammer ausgeschlossen. Vielmehr ist bei lebensnaher Betrachtung unter Berücksichtigung auch des Entdeckungsrisikos und der drohenden strafrechtlichen Konsequenzen davon auszugehen, dass der Angeklagte diesen finanziellen, intellektuellen und zeitlichen Aufwand erbracht hat, um hieraus einen dauerhaften finanziellen Vorteil zu erhalten. 402

Dass der Angeklagte hinsichtlich der im Tatkomplex B abgeurteilten Taten in der Absicht handelte, die Empfänger der Phishingmails über deren tatsächlichen Aussteller zu täuschen und sie hierdurch zur Eingabe ihrer persönlichen und Zugangsdaten hinsichtlich ihres Online-Banking-Accounts zu veranlassen, steht zur Überzeugung der Kammer aufgrund der gegebenen Gesamtumstände fest. Allein eine solche Absicht erklärt den aus der Beweisaufnahme ersichtlichen enormen zeitlichen, geistigen und technischen Aufwand bei der Erstellung und Versendung der in Rede stehenden Emails, denen ihrem Inhalt nach keine andere Bedeutung, als die Erlangung von Daten durch Täuschung der Empfänger, beigemessen werden kann. 403

Das übrige Ergebnis der Beweisaufnahme steht den getroffenen Feststellungen nicht entgegen 404

IV. Rechtliche Würdigung 405

1. Tatkomplex A (Fälle 1-29) 406

Der Angeklagte hat sich nach den getroffenen Feststellungen des Computerbetruges in 29 tateinheitlich zusammentreffenden Fällen, wobei es in drei Fällen (Fälle 3, 23 und 25) beim 407

Versuch verblieb, strafbar gemacht (§§ 263a Abs. 1, Abs. 2, 263 Abs. 2, 22, 23 Abs. 1, 25 Abs. 2 StGB).

a) Durch das Zugreifen auf die Online-Banking-Accounts der in Rede stehenden Konteninhaber und die Ausführung von nicht autorisierten Überweisungen mittels der im Wege des Phishings erlangten geheimen Kontozugangsdaten und abgelisteter TANs, hat das jeweilige Zugriff nehmende und die Überweisung ausführende Mitglied der Tätergruppierung den objektiven Tatbestand des § 263a Abs. 1 StGB erfüllt. 408

Die Eingabe von Zugangscodes wie PIN und TAN gegen den Willen des Berechtigten, nachdem mit Methoden des Phishings geheime Zugangsdaten eines Kontoinhabers für den Kontozugriff im Online-Banking erlangt wurden, stellt eine unbefugte Verwendung von Daten im Sinne der betrugsspezifischen Auslegung des Begriffs der Unbefugtheit im Sinne des § 263a Abs. 1 StGB dar (vgl. Fischer, StGB, 64. Auflage, § 263a, Rn. 11 f., 16). 409

Durch die Eingabe der abgelisteten oder nach Umstellung der Empfängernummer generierten TANs zur Durchführung der vorbereiteten Überweisungen, wurde jeweils unmittelbar eine vermögensrelevante Disposition des Computers – nämlich die Belastung des jeweiligen Kontos mit dem Überweisungsbetrag – verursacht und damit das Ergebnis eines Datenverarbeitungsvorgangs beeinflusst (Fischer, aaO., Rn. 20). Hierdurch trat als unmittelbare Folge des beeinflussten Ergebnisses des Datenverarbeitungsvorgangs ein Vermögensschaden bei dem jeweiligen Kunden bzw. – bei Vorliegen der zivilrechtlichen Voraussetzungen eines Berichtigungsanspruchs mangels wirksamen Überweisungsauftrags - bei der kontoführenden Bank ein (vgl. Fischer, 64. Auflage, § 263a, Rn. 22; Goeckenjan, wistra 4/2008, 128, 132). Das etwaige Auseinanderfallen von Verfügendem und geschädigtem Vermögensinhaber steht der Strafbarkeit wegen Computerbetruges aufgrund des besonderen Näheverhältnisses zwischen Bank und Kunden nicht entgegen. 410

Diejenigen Fälle, in denen ein Überweisungsrückruf erfolgreich war (Fälle 3, 23 und 25), hat die Kammer mangels Schadenseintritts rechtlich als Versuch gewertet. 411

In den übrigen Fällen ist die Kammer von (tatbestandlichen) Schäden in Höhe der festgestellten, nicht zurückgebuchten, Überweisungsbeträge ausgegangen. Mithin hat die Kammer folgende (tatbestandlichen) Schadenshöhen angenommen: 412

Fall 1: 2.000,00 € 413

Fall 2: 1.479,00 € 414

Fall 4: 8.442,00 € 415

Fall 5: 10.000,00 € 416

Fall 6: 9.950,00 € 417

Fall 7: 9.687,00 € 418

Fall 8: 9.976,00 € 419

Fall 9: 9.987,00 € 420

Fall 10: 4.500,00 € 421

422

Fall 11:	230,00 €	
Fall 12:	12.130,00 €	423
Fall 13:	3.400,00 €	424
Fall 14:	3.200,00 €	425
Fall 15:	500,00 €	426
Fall 16:	900,00 €	427
Fall 17:	7.300,00 €	428
Fall 18:	2.500,00 €	429
Fall 19:	2.400,00 €	430
Fall 20:	5.000,00 €	431
Fall 21:	9.890,00 €	432
Fall 22:	1.420,00 €	433
Fall 24:	9.898,00 €	434
Fall 26:	9.950,00 €	435
Fall 27:	1.660,51 €	436
Fall 28:	9.300,00 €	437
Fall 29:	2.300,00 €	438

Dass überwiesene Gelder später aus einem internen Sicherungsfonds der T1 – kulanzweise – ersetzt wurden, steht der Annahme eines Schadenseintritts in der genannten Höhe mangels unmittelbarer Kompensation nicht entgegen. 439

b) Die Ausführungshandlungen sind dem Angeklagten nach der insoweit gebotenen wertenden Gesamtbetrachtung jeweils aufgrund einer mittäterschaftlichen Begehungsweise nach § 25 Abs. 2 StGB zuzurechnen. 440

Mittäterschaft ist gegeben, wenn ein Tatbeteiligter mit seinem Beitrag nicht bloß fremdes tatbestandsverwirklichendes Tun fördern will, sondern dieser Beitrag im Sinne arbeitsteiligen Vorgehens Teil einer gemeinschaftlichen Tätigkeit sein soll. Dabei muss der Beteiligte seinen Beitrag als Teil der Tätigkeit des anderen und umgekehrt dessen Tun als Ergänzung seines eigenen Tatanteils wollen. Der gemeinschaftliche Tatentschluss kann durch ausdrückliche oder auch durch konkludente Handlungen gefasst werden. Ob ein Beteiligter ein derart enges Verhältnis zur Tat hat, ist nach den gesamten Umständen, die von seiner Vorstellung umfasst sind, in wertender Betrachtung zu beurteilen. Wesentliche Anhaltspunkte für diese Beurteilung können der Grad des eigenen Interesses am Erfolg der Tat, der Umfang der Tatbeteiligung und die Tatherrschaft oder wenigstens der Wille hierzu sein, so dass Durchführung und Ausgang der Tat maßgeblich auch vom Willen des Betreffenden abhängen (st. Rspr.; vgl. etwa BGH, Beschluss vom 21.05.2015, 3 StR 575/14 m.w.N.). Die Annahme 441

von Mittäterschaft erfordert nicht zwingend eine Mitwirkung am Kerngeschehen; es kann vielmehr auch ein Beitrag im Vorbereitungsstadium des unmittelbar tatbestandlichen Handelns und ein solcher im Stadium zwischen Vollendung und Beendigung der Tat genügen (BGH aaO., m.w.N.).

Dies zugrunde gelegt liegen die Voraussetzungen der mittäterschaftlichen Zurechnung gem. § 25 Abs. 2 StGB vor: 442

Der Angeklagte hat für das Gelingen der unautorisierten Online-Überweisungen wesentliche und gewichtige Tatbeiträge geleistet, indem er – entsprechend der Arbeitsteilung innerhalb der Tätergruppe – im Vorfeld das Internet nach potenziellen Phishingmail-Empfängeradressen durchsucht und massenhaft Phishingmails versendet hat. Hierdurch hat er maßgeblich zum späteren Gelingen der Taten beigetragen, da es erst so zur Erlangung der für den unautorisierten Zugriff auf die Online-Banking-Accounts erforderlichen Daten kam. Die hieraus erlangten Daten wurden für die letztlich den Zugriff und die Überweisung ausführenden Personen von ihm aufbereitet und in Datensätzen zusammengestellt weitergeleitet. Das spätere Gelingen hing damit maßgeblich von der Tätigkeit und dem Willen auch des Angeklagten ab. Auch wenn nicht festgestellt werden konnte, dass Überweisungen durch ihn (eigenhändig) freigegeben wurden, nahm er doch durch die erteilten Anweisungen und Entscheidungen steuernden Einfluss auf das eigentliche Tatgeschehen. Sowohl den Handlungen des Angeklagten als auch dem darauf aufbauenden Handeln der Telefonisten und Telefonistinnen bis hin zur Durchführung der Überweisungen lag ein gemeinsamer, auf Arbeitsteilung beruhender Tatplan zugrunde, wobei der Angeklagte seinen Beitrag als Teil der Tätigkeit der Anrufenden bzw. die Überweisungen Ausführenden und deren Beiträge als Ergänzung seines Tatanteils wollte. 443

Der Angeklagte kannte das weitere Vorgehen der Telefonisten /-innen der Tätergruppe und nahm eine Vermögensschädigung der Banken bzw. Bankkunden um des erstrebten eigenen finanziellen Vorteils willen zumindest billigend in Kauf. Er beabsichtigte, zunächst Dritten, mittelbar jedoch auch sich selbst durch die erfolgten Online-Überweisungen einen Vermögensvorteil zu verschaffen. 444

Da die mittäterschaftlichen Tatbeiträge im Vorfeld der eigentlichen Taten begangen wurden und nicht sicher aufgeklärt werden konnte, in wie vielen einzelnen Vorgängen er die aufbereiteten Daten weiterleitete, sind ihm die (rechtlich selbständigen) Taten der die unautorisierten Überweisungen ausführenden Mittäter als in gleichartiger Tateinheit (§ 52 StGB) begangen zuzurechnen (vgl. Fischer, StGB, 64. Auflage, Vor § 52, Rn. 35 m.w.N.). Die konkurrenzrechtliche Beurteilung ist bei mehreren Tatbeteiligten nach der Art eines jeden Tatbeitrags gesondert zu ermitteln (Fischer, aaO., Rn. 34). 445

2. Tatkomplex B 446

Indem der Angeklagte im Zeitraum zwischen dem 27.02.2015 und dem 28.05.2015 massenhaft vorgeblich von der S, der Q1 oder der J-Bank stammende Phishingmails in 13 voneinander getrennten Vorgängen versandte, hat er sich wegen Fälschung beweiserheblicher Daten gemäß § 269 Abs. 1 StGB in 13 Fällen strafbar gemacht. 447

Wären die den versandten Phishingmails zugrundeliegenden Daten unmittelbar verkörpert wahrnehmbar, läge – was der Angeklagte jeweils beabsichtigte – jeweils eine unechte Urkunde vor. 448

449

Die in Rede stehenden Emails weisen insbesondere einen rechtlich erheblichen Inhalt auf. Sie enthalten die Aufforderung - im Rahmen eines bestehenden Vertragsverhältnisses zwischen dem Konteninhaber und der Bank - eine Aktualisierung bzw. ein Sicherheitsupdate durchzuführen, mithin eine Aufforderung zu einer vertragsgemäßen Mitwirkung des Kunden (vgl. Goeckenjan, wistra 2008, 128 ff.). Die Emails lassen darüber hinaus jeweils einen anderen – nämlich die jeweilige Bank – als den tatsächlichen Aussteller – nämlich den Angeklagten – erkennen (vgl. Goeckenjan, wistra 2008, 128 ff.; vgl. Seidl/Fuchs, HRRS 2010, 85 ff.).

Ob dann nicht mehr von einer Urkunden-Vergleichbarkeit ausgegangen werden kann, wenn die Email derart fehlerhaft und schwerverständlich gefasst ist, dass sie nicht als ernsthafte Erklärung gelten kann (vgl. Goeckenjan, a.a.O.) kann vorliegend dahinstehen, da die verfahrensgegenständlichen Emails den insoweit gestellten Anforderungen genügen. Die in Rede stehenden, vorgeblich von der S, der Q1 bzw. der J stammenden Emails, sind sprachlich verständlich und auch orthographisch, grammatikalisch sowie von der Wortwahl her nicht derart fehlerhaft, dass sie nicht als ernsthafte Erklärungen angesehen werden könnten. Als Aussteller wird jeweils der Name einer im jeweiligen Land bekannten Bank benannt. 450

Durch das Versenden hat der Angeklagte die Tathandlung des Speicherns im Sinne von § 269 Abs. 1 StGB verwirklicht, zumal die Emails, die vom Server des Angeklagten weitergeleitet wurden, auf dem Mail-Server bzw. Rechner des Empfängers abgelegt wurden (vgl. Goeckenjan, aaO.). 451

Der Angeklagte handelte hierbei in der Absicht, die Empfänger der Phishingmails über deren tatsächlichen Aussteller zu täuschen und sie hierdurch zur Eingabe ihrer persönlichen und Zugangsdaten hinsichtlich ihres Online-Banking-Accounts zu veranlassen. 452

In konkurrenzrechtlicher Hinsicht liegen 13 eigenständige, in Tatmehrheit (§ 53 StGB) stehende Taten vor, da der Angeklagte zumindest 13 eigenständige Versendungsvorgänge angestoßen hat. Die Taten des Tatkomplexes B werden auch nicht durch § 263a Abs. 3 StGB verklammert. Die Beschaffung und Verwahrung verschiedener Programme, insbesondere die Verwendung des Programms … zur Versendung der Phishingmails erfolgte zwar zur *Vorbereitung* eines späteren Computerbetruges, nicht aber zu dessen *Begehung*, weshalb diese Programme bereits nicht dem Tatbestand des § 263a StGB unterfallen (vgl. Schönke/Schröder/Perron, StGB, 29. Auflage, § 263a, Rn. 33a). 453

V. Strafzumessung 454

1. Strafrahmen / Besonders schwerer Fall 455

Die Kammer ist sowohl hinsichtlich der Taten aus Tatkomplex A wie derjenigen aus Tatkomplex B jeweils von einem besonders schweren Fall des Computerbetruges gem. §§ 263a Abs. 2, 263 Abs. 3 S. 2 Nr. 1 Alt. 1 StGB bzw. der Fälschung beweiserheblicher Daten gemäß §§ 269 Abs. 3, 267 Abs. 3 S. 2 Nr. 1 Alt. 1 StGB ausgegangen. 456

Der Angeklagte handelte in allen Fällen gewerbsmäßig, da seine Absicht darauf gerichtet war, sich durch die letztlich von der Tätergruppierung ausgeführten unzulässigen Überweisungen – mittelbar – einen fortlaufenden, eigennützigen, finanziellen Vorteil zu verschaffen. 457

458

Die vorzunehmende Gesamtabwägung führt in keinem Fall dazu, dass die Indizwirkung des Regelbeispiels ausnahmsweise entfällt. Dies wäre anzunehmen, wenn außergewöhnliche Umstände gegeben wären, die das Unrecht oder die Schuld des Angeklagten deutlich vom Regelfall unterscheiden und deshalb im Einzelfall die Anhebung des Regelstrafrahmens nicht als gerechtfertigt erscheinen würde. Im Rahmen der vorzunehmenden Gesamtabwägung hat die Kammer alle Umstände und Aspekte herangezogen und gewürdigt, die für die Wertung der Tat und der Person des Angeklagten in Betracht kommen, gleichgültig, ob sie der Tat innewohnen, sie begleiten, ihr vorausgehen oder nachfolgen (vgl. BGH, NStZ 1982, 246). Danach entfällt die Indizwirkung des Regelbeispiels vorliegend – auch in den Fällen des Tatkomplexes B, in denen verhältnismäßig weniger Phishingmails versendet wurden – nicht, so dass eine Anhebung des Regelstrafrahmens nicht ausnahmsweise ausscheidet.

Die Kammer hat hierbei nicht verkannt, dass zu Gunsten des Angeklagten verschiedene strafmildernde Gesichtspunkte zu berücksichtigen waren: So ist der Angeklagte in Deutschland bislang lediglich geringfügig strafrechtlich in Erscheinung getreten. Aufgrund seiner fehlenden Sprachkenntnisse ist er zudem besonders haftempfindlich. Die Untersuchungshaft war für ihn aufgrund der angenommenen Umstände zudem mit erheblichen besonderen Erschwernissen verbunden. Zum Teil ist es hinsichtlich der Taten aus Tatkomplex B bei der Versendung einer verhältnismäßig geringen Anzahl von Phishingmails verblieben. Das Versenden der Phishingmails in Tatkomplex B erfolgte zudem unter polizeilicher „Beobachtung“. 459

Gegen ihn sprach demgegenüber die Einbindung in eine international organisierte, bandenmäßig strukturierte und konspirativ vorgehende Tätergruppe. Das Tatbild ist zudem geprägt durch ein mehrstufiges, aufeinander abgestimmtes professionelles Vorgehen, was ein erhebliches Maß an krimineller Energie zeigt und sich von anderen Fällen des gewerbsmäßigen Computerbetrugs bzw. der gewerbsmäßigen Fälschung beweiserheblicher Daten nach oben hin abhebt. Zu seinen Lasten waren im Tatkomplex A zudem die große Anzahl der betroffenen Bankkunden und die Höhe des insgesamt verursachten Schadens zu berücksichtigen. In diesem Zusammenhang hat die Kammer – insoweit zu seinen Gunsten – auch bedacht, dass den betroffenen Bankkunden letztlich kein finanzieller Schaden verblieben ist, da die überwiesenen Beträge aus einem internen Sicherungsfonds erstattet wurden. 460

Bei der gebotenen Gesamtwürdigung war die Kammer nach alledem der Ansicht, dass – auch unter zusätzlicher Berücksichtigung des vertypten Milderungsgrundes gem. §§ 23 Abs. 2, 49 Abs. 1 StGB in den Fällen 3, 23 und 25 – die Indizwirkung des Regelbeispiels in keinem der abgeurteilten Fälle entfällt. 461

Auszugehen war nach alledem im Tatkomplex A von dem Strafrahmen des § 263 Abs. 3 S. 1 StGB i.V.m. § 263a Abs. 2 StGB, der Freiheitsstrafe von 6 Monaten bis zu 10 Jahren vorsieht. Da insoweit ein Fall gleichartiger Tateinheit gegeben ist, war hinsichtlich Tatkomplex A auf eine Strafe zu erkennen (§ 52 Abs. 1 StGB). Hinsichtlich der im Tatkomplex B festgestellten Taten war jeweils der Strafrahmen des § 267 Abs. 3 S. 1 StGB i.V.m. § 269 Abs. 3 StGB, der ebenfalls jeweils Freiheitsstrafe von 6 Monaten bis zu 10 Jahren vorsieht, zu Grunde zu legen. 462

2. Konkrete Strafzumessung 463

Innerhalb des damit jeweils anzuwendenden Strafrahmens hat die Kammer bei der konkreten Straffindung die bereits bei der Strafrahmenbestimmung genannten be- und entlastenden Umstände – auf die insoweit Bezug genommen wird – erneut umfassend berücksichtigt. 464

Unter Abwägung aller für und gegen den Angeklagten sprechenden Umstände – hinsichtlich der im Tatkomplex B angeklagten Taten auch unter Berücksichtigung der jeweiligen Anzahl der versandten Phishingmails – hat die Kammer folgende Einzelstrafen für tat- und schuldangemessen erachtet: 465

aa) Tatkomplex A 466

(Fälle 1 bis 29) **3 Jahre und 6 Monate Freiheitsstrafe** 467

bb) Tatkomplex B 468

für Fall 30 **8 Monate Freiheitsstrafe** 469

für Fall 31 **1 Jahr Freiheitsstrafe** 470

für Fall 32 **10 Monate Freiheitsstrafe** 471

für Fall 33 **10 Monate Freiheitsstrafe** 472

für Fall 34 **8 Monate Freiheitsstrafe** 473

für Fall 35 **8 Monate Freiheitsstrafe** 474

für Fall 36 **10 Monate Freiheitsstrafe** 475

für Fall 37 **10 Monate Freiheitsstrafe** 476

für Fall 38 **1 Jahr Freiheitsstrafe** 477

für Fall 39 **1 Jahr und 3 Monate Freiheitsstrafe** 478

für Fall 40 **1 Jahr Freiheitsstrafe** 479

für Fall 41 **10 Monate Freiheitsstrafe** 480

für Fall 42 **8 Monate Freiheitsstrafe** 481

3. Gesamtstrafenbildung 482

Hieraus hat die Kammer unter nochmaliger Berücksichtigung aller für und gegen den Angeklagten sprechenden Umstände gemäß §§ 53, 54 Abs. 1 S. 2 StGB durch Erhöhung der höchsten verwirkten Einzelstrafe von 3 Jahren und 6 Monaten Freiheitsstrafe eine Gesamtfreiheitsstrafe von 483

4 Jahren und 6 Monaten 484

gebildet und dabei insbesondere auch den engen zeitlichen und kriminologischen Zusammenhang zwischen den Taten berücksichtigt. 485

4. Anrechnung der Auslieferungshaft 486

Die in niederländischer Auslieferungshaft verbrachte Haftzeit war im Verhältnis 1:1 anzurechnen, § 51 Abs. 4 S. 2, Abs. 3 S. 2, Abs. 1 S. 1 StGB. 487

VI. Kostenentscheidung 488