Musterklausur Cyberstrafrecht: „Wenn der [Ph]isch erst einmal angebissen hat…“

Prof. Dr. Sascha Kische, LL.M.[1],
HSPV NRW

Viele der von den Kriminalämtern unter ‚Straftaten mit dem Tatmittel Internet‘ erfassten Delikte gehören zum Pflichtstoff im Polizeistudium in Bund und Ländern. Allein wegen der umfänglichen Fülle von Lehr- und Lerninhalten in den hochschulischen Curricula geraten die polizeipraktisch bedeutsamen und vor allem cyberstrafrechtlich einschlägigen Vorschriften zu kurz. Auch deshalb hat bspw. die Landesregierung NRW entschieden, für nordrhein-westfälische Polizeibeamtinnen und -beamte ein auf die Erfordernisse der Polizeipraxis zugeschnittenes, weiteres Bachelorstudium „Cyberkriminalistik“ (mit Abschluss B.Sc.) am Cyber Campus NRW einzurichten (Erlass seitens des Innenministeriums NRW vom 14.12.2022 – Az. 421-27.17). Mit dieser Musterklausur sollen eher methodische Einblicke in die strafrechtliche Begutachtung eines „Phishing“-Szenarios für Studierende, Lehrende und auch Praktiker gewährt werden. Zugunsten eines besseren Leseverständnisses wird auf Nachweise und Fußnotenapparat gänzlich verzichtet – bewusst in den Mittelpunkt gestellt werden die Gesetzesanwendung und die stets studentisch schwerfallende Subsumtion unter die Vorschriften.

Sachverhalt:

Hacker H hat erfolgreich sein Studium der Informatik absolviert. Auf der Suche nach einer passenden Tätigkeit ist er weder von den derzeitigen Angeboten der freien Wirtschaft noch des öffentlichen Dienstes wirklich überzeugt. Sein Vorbild war lange Zeit der Nachbar N, der als Manager bei einem örtlich ansässigen Industrie-Unternehmen (U) in der Führungsebene tätig ist. Gespannt, aber auch mittlerweile genervt hört er von den wöchentlichen Flügen des N über die ganze Welt, die N stets selbst mit seiner Kreditkarte bucht und dann auch noch Flugmeilen für private Flüge mit der Familie sammelt. Überdies prahlt N immer damit, sämtliche private und berufliche Geschäfte mit Leichtigkeit nur noch über das Internet abzuwickeln – und zwar mithilfe des immer gleichen Benutzernamen und Kennwortes, denn so gerate nichts in Vergessenheit und mache keine Sorgen.

Um an diese Informationen zu gelangen und damit dem N die Schwächen seiner Vorgehensweisen aufzuzeigen, heckt H folgenden Plan aus und führt diesen folgendermaßen durch: Weil N, wie H weiß, stets beim gleichen Flugunternehmen Lufthansa bucht, gestaltet er mithilfe einer bereits zu Studienzwecken angeschafften speziellen Software eine E-Mail mit folgender Aufmachung:

Von: Miles & More

Wichtig: Registrieren Sie sich jetzt für den neuen Sicherheitsstandard 3-D Secure für Online-Zahlungen

Sehr geehrter Kunde,
Heute möchten wir Sie über eine bevorstehende Änderung bei Online-Zahlungen informieren:
Visa Secure und Mastercard® Identity Check TM sind eine Weiterentwicklung von Verified by Visa und Mastercard® SecureCode TM. Mit den Namen ändern sich auch die Logos. Am 5.1.2023 tritt die 2. Zahlungsdiensterichtlinie der Europäischen Union (Payment Service Directive 2 – PSD2) in Kraft. Stellen Sie sicher, dass Sie auch in Zukunft bequem online einkaufen können. Registrieren Sie sich jetzt in wenigen Schritten für die neuen Sicherheitsverfahren Visa Secure und Mastercard® Identity CheckTM.

Mit freundlichen Grüßen
Miles and More Lufthansa KartenService

Diese E-Mail sendet H an die ihm bekannte Email-Adresse des N. Dieser denkt sich nach Erhalt nichts Schlimmes und gibt Benutzername und Passwort ein, worauf er nicht auf die Internetseiten des Flugunternehmens, sondern auf eine von H ebenfalls per Software gestaltete Webseite geleitet wird, auf der nach erfolgter Eingabe durch N lediglich mitgeteilt wird, dass der Bearbeitungsvorgang gestartet ist und eine Rückmeldung nach Fertigstellung erfolgt.

Nunmehr in Kenntnis von den Zugangsdaten weiß A auch, dass auf den Internetseiten von U ein Login-Bereich für die Mitarbeiter mit Zugriff auf das Firmenintranet vorgehalten ist. Nach Eingabe von Benutzername und Passwort kann H neben der Einsicht in das Email-Postfach auch auf verschiedenste persönliche Mitarbeiterinformationen, persönliche Daten von Führungspersonal sowie Nutzer- und Angestellten-Informationen zugreifen. Sein spezielles Augenmerk gilt jedoch den durch den Zugang des M als Führungsperson einsehbaren sensiblen Informationen von Kundendaten anderer Unternehmen weltweit. Diese Informationen lädt sich H herunter und speichert diese auf seinem USB-Stick ab. A überlegt noch, die Dateien auf Unternehmensseite zu sperren oder gar zu löschen, verwirft diesen Gedanken aber ganz schnell wieder, um keine Spur zu hinterlassen.

Einige Tage später kommt dem H angesichts der sensiblen Unternehmensdaten eine neue Idee: Aus studentischen Zeiten erinnert er sich an die vielfältigen Möglichkeiten des Darknets und der dortigen finanziellen Gewinnmöglichkeiten. So erstellt er eine auszugsweise Liste über die erbeuteten Daten und stellt diese anonym und unter wahrheitsgemäßer Darstellung der Herkunft ein verbunden mit einer zielgerichteten Nachricht an U, dass sämtliche gespeicherten Dateien für 1.000.000 € zum Kauf angeboten werden, wenn U nicht seinerseits 500.000 € in bar an einem speziell noch zu vereinbarenden Ort hinterlegt, um dem Verkauf zuvorzukommen.

Nach Kenntnis von der Nachricht weigert sich U und schaltet die Polizei ein, die im Verlaufe weniger Tage auf die Aktivitäten des H aufmerksam wird und diesen schließlich festnimmt.

Aufgabe:

Prüfen Sie gutachterlich mögliche einschlägige Straftatbestände nach dem StGB.

Lösung:
Erster Handlungsabschnitt: Anfertigen von Email und Website sowie Versenden der E-Mail

I. § 263 Abs. 1 StGB, Betrug zu Lasten des N

H könnte sich wegen Betruges zulasten des N gemäß § 263 Abs. 1 StGB strafbar gemacht haben, indem er diesem die E-Mail von einem vermeintlichen Absender ‚Miles & More' zukommen ließ und vorgab, zwecks Registrierung des N würden Benutzername und Kennwort benötigt, um die bisherigen Käufe mittels Kreditkarte fortzuführen.

1. Objektiver Tatbestand

a) Täuschung über Tatsachen

H müsste über Tatsachen getäuscht haben.

Tatsachen sind konkrete Ereignisse oder Zustände der Gegenwart oder Vergangenheit, die dem Beweis zugänglich sind. Die Eigenschaft des Mailversenders, die Notwendigkeit einer neuen Registrierung auf der Unternehmenswebsite sowie die Feststellung, die neue Zahlungsdiensterichtlinie der EU trete am 5. Januar 2022 in Kraft und bedinge diese aktuelle Abfrage, sind gegenwärtig und dem Beweis zugänglich und fallen damit unter den Tatsachenbegriff.

Täuschung bedeutet die Einwirkung auf das Vorstellungsbild eines anderen durch eine wahrheitswidrige Behauptung oder ein sonstiges Verhalten mit Erklärungswert mit dem Ziel der Irreführung. Die vorbezeichneten Tatsachen werden ausweislich des Email-Textes durch H behauptet, obwohl sie tatsächlich nicht gegeben sind. Die Erklärung zielt darauf ab, den N über die wahren Motive des H in die Irre zu leiten. Eine Täuschung ist damit ebenfalls zu bejahen.

b) Irrtum

Es müsste ein auf der Täuschung beruhender Irrtum des N vorliegen. Dies verlangt ein unrichtige Vorstellung des Getäuschten über Tatsachen. N hegt überhaupt keinen Zweifel an der Richtigkeit der Inhalte der E-Mail und folgt den Anweisungen, wobei er gar nichts Schlimmes befürchtet. Eine Irrtumserregung ist auch zu bejahen.

c) Vermögensverfügung

Mit der Eingabe von Benutzernamen und Kennwort müsste N eine Vermögensverfügung vorgenommen haben (was bekanntlich als „ungeschriebenes Tatbestandsmerkmal" beim Betrug gilt). Eine Vermögensverfügung ist jedes willentliche Tun, Dulden oder Unterlassen mit unmittelbar vermögensmindernder Wirkung. Die Preisgabe beider sicherheitsrelevanter Informationen geschah zunächst willentlich. Zur Bedeutung der Unmittelbarkeit können zweierlei Aspekte vorgebracht werden: Zum einen mag nur eine mittelbare Vermögensminderung darin zu erblicken sein, dass erst noch ein eigenmächtiger deliktischer Akt des H erforderlich sei und durch die Verschaffung lediglich die Voraussetzungen für seinen Zugriff geschaffen werden. Zum anderen kann bereits auf den Zeitpunkt der Eingabe von Benutzername und Kennwort abgestellt werden, da – insbesondere unter Berücksichtigung der Angaben im Sachverhalt – dem H hiernach bereits eine jederzeitige Zugriffsmöglichkeit auf den Vermögensbereich des N besteht. Geht man von einer Unmittelbarkeit der Verfügung aus (a.A. vertretbar), liegt eine tatbestandliche Vermögensverfügung vor.

d) Vermögensschaden

Fraglich ist, ob ein unmittelbarer Vermögensschaden ein. Grundsätzlich bestimmt sich dieser Vermögensschaden nach der Betrachtung eines sog. negativen Saldos bei Vergleich der Vermögenswerte vor und nach der Vermögensverfügung.

Durch die bloße Herausgabe von Benutzername und Kennwort ist ein eigener Vermögenswert und mithin ein Negativsaldo noch nicht festzustellen. Daher richtet die h.M. auch den Blick auf eine sog. „schadensgleiche Vermögensgefährdung" und betrachtet im Einzelfall die hinreichende Wahrscheinlichkeit eines alsbaldigen, unmittelbaren und endgültigen Vermögensverlustes des Opfers. Bereits im Zeitpunkt der Überlassung von Zugangsdaten ist ein jederzeitiger Kontenzugriff möglich. Hinzu kommt, dass im vorliegenden Sachverhalt ein unmittelbarer und endgültiger Vermögensverlustes gerade deshalb wahrscheinlicher ist, weil N sämtliche geldlichen Geschäftsaktivitäten mit identischen Zugangsdatenkennungen vornimmt. Der Zugriff darauf liegt bereits alleine in der Hand des H, der so bspw. ein neues Passwort vergeben und damit dem N sogar den Zugriff vollständig entziehen kann. Eine schadensgleiche Gefährdung des Vermögens des N und mithin eine tatbestandlich vollendete Schädigung im Sinne des § 263 Abs. 1 StGB liegt vor.

2. Subjektiver Tatbestand

a) Vorsatz

Mit dem Erhalt von Benutzername und Kennwort war für H klar, dass er den N täuschungs- und irrtumsbedingt zur Preisgabe insbesondere seiner vermögensrelevanten Zugangsdaten bewegte und damit dem alleinigen Einflussbereich des N entzog, was dessen Vermögen bereits schadensgleich gefährdete. Genauso wollte H es auch. Er handelte demnach vorsätzlich gemäß § 15 StGB.

b) Absicht rechtswidriger Bereicherung

Zudem müsste H in der Absicht rechtswidriger Bereicherung gehandelt haben. Sozusagen „spiegelbildlich" müsste H danach den Vermögensnachteil bei N (hier die Vermögensgefährdung durch Verlust der Kontrolle über die Zugangsdaten) als Vermögensvorteil für sich oder einen Dritten erstrebt haben. Daran lässt sich zunächst zweifeln, weil H dem N anfangs nur eines Besseren belehren wollte und ihn mit einer Lektion für dessen Prahlerei erteilen wollte. Die Verschaffung dieser Zugangsdaten führt allerdings zu einem Besitzvorteil bei H, der bereits als Vermögensvorteil gilt, da diesen Daten ein wirtschaftlich messbarer Wert zukommt und geradewegs Gebrauchsvorteile durch die Ermöglichung des Zugangs zu vermögensbeinhaltenden Accounts (Bankkonten, soziale Netzwerke etc.) beinhaltet. Darauf kam es H auch zielgerichtet an, wie sich insbesondere auch seinem anschließenden Verhalten offenbart. Auf diese Zugangsdaten hatte H auch keinen Anspruch, so dass die Absicht rechtswidriger Bereicherung gegeben ist.

3. Rechtswidrigkeit und Schuld

Jeweilige Ausschlussgründe sind nicht ersichtlich.

4. Besonders schwerer Fall nach § 263 Abs. 3 StGB

Anhaltspunkte für das Vorliegen strafzumessungserschwerender Gründe nach § 263 Abs. 3 StGB sind ebenso wenig ersichtlich.

5. Ergebnis

H hat sich wegen Betruges zulasten des N gemäß § 263 Abs. 1 StGB strafbar gemacht.

II. § 269 StGB, Fälschung beweiserheblicher Daten

Indem H eigens die E-Mail für N vorbereitet und ihm zur Kenntnis brachte, könnte er sich wegen Fälschung beweiserheblicher Daten gemäß § 269 Abs. 1 StGB strafbar gemacht haben.

1. Objektiver Tatbestand

a) Daten

Tatobjekt des § 269 StGB sind beweiserhebliche Daten. Zum Datenbegriff kann auf die Legaldefinition in § 202a Abs. 2 StGB Rückgriff genommen werden: Daten sind solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Bei einer E-Mail handelt es sich um informationsenthaltene Daten.

b) Hypothetischer Vergleich mit § 267 StGB

Für § 269 Abs. 1 StGB ist hypothetisch zu prüfen, ob die Voraussetzungen des § 267 StGB bei einer visuellen Wahrnehmbarkeit i. Se. „Computerausdrucks und In-den-Händen-halten" verwirklicht sind. Neben dem hypothetischen zugedachten Erklärungsinhalt (sog. Perpetuierungsfunktion) müssten zudem die Beweis- und Garantiefunktion als urkundliche Voraussetzungen vorliegen.

Bei einer E-Mail handelt es sich um eine menschlich verkörperte Gedankenerklärung, da Inhalt und Intention durch eine menschliche Erklärung beigebracht worden sind.

Darüber hinaus müssen die enthaltenen Erklärungen geeignet und bestimmt sein, für ein Rechtsverhältnis Beweis zu erbringen. Beides kann der E-Mail heutzutage nicht mehr abgesprochen werden: Sie taugen gegenüber Behörden und Gerichten als Beweismittel, die Inhalte sind geeignet und vom Erklärenden bestimmt, für einen Vorgang einen verschriftlichten Nachweis zu schaffen.

Die Garantiefunktion erfordert bekanntermaßen, dass eine Urkunde einen Aussteller erkennen lässt. So wird derjenige als erkennbarer Aussteller angesehen, dem die Inhalte ihren Erklärungsgehalt nach (geistig) zugerechnet werden können. Die Ausstellereigenschaft kann sich hierbei nicht nur aus der verwendeten E-Mail-Adresse, sondern auch aus dem Namen, nach der Grußformel oder den Kontaktdaten am Ende der E-Mail ergeben. Hier geht ‚Miles & More' eindeutig als Aussteller hervor.

Bei der Wahrnehmung der Daten (s. oben) müsste also gemäß § 269 Abs. 1 StGB nunmehr eine unechte Urkunde vorliegen. Unecht ist eine Urkunde, wenn sie nicht von denjenigen stammt, der aus ihr hervorgeht. Die E-Mail stammt tatsächlich von H und nicht vom scheinbaren Aussteller des Flugunternehmens. Nicht nur Namens-, sondern geradezu identitätstäuschend wird ein Aussteller vorgegeben, der tatsächlich nicht hinter diesen Erklärung steht.

c) Tathandlung

Durch das Abschicken der E-Mail wird eine Speicherung der Daten sowohl auf dem Rechner von H als auch dem dem Rechner des N bewirkt, sodass hierdurch § 269 Abs. 1 Var. 1 StGB verwirklicht wird. Ebenso kommt in dem Versenden der E-Mail auch die Tathandlungsvariante des Gebrauchens nach Var. 3 in Betracht, da dem N als Empfänger die Möglichkeit der Kenntnisnahme gegeben wird.

2. Subjektiver Tatbestand

Der Täter muss vorsätzlich und deliktsspezifisch(!) zur Täuschung im Rechtsverkehr handeln. H schickte die E-Mail gerade zur Verstärkung der Täuschung, dass Inhalte und Anweisungen von der Flugfirma stammten und für den zukünftigen Geschäftsverkehr notwendig seien; das war sein Ziel.

3. Rechtswidrigkeit und Schuld

H handelt rechtswidrig und schuldhaft.

4. Ergebnis

H hat sich gemäß § 269 Abs. 1 Var. 1 und 3 StGB strafbar gemacht.

III. § 263 Abs. 1 (, § 25 Abs. 1 Alt. 2) StGB, Computerbetrug (in mittelbarer Täterschaft),

H könnte sich wegen Computerbetruges gemäß § 263a Abs. 1 StGB strafbar gemacht haben. In Betracht kommt hier eine verwirklichte Tathandlung der unbefugten Verwendung von Daten nach Var. 3, und zwar in mittelbarer Täterschaft begangen „durch den N" (§ 25 Abs. 1 Alt. 2 StGB), in dem dieser nach Erhalt der E-Mail auf der eigens von H präparierten Webseite seinen Benutzernamen und Kennwort eingab.

1. Objektiver Tatbestand

Mittels Eingabe von zutreffenden Benutzernamen und Kennwort verwendet N echte und damit richtige Daten. Als Tathandlung der „unbefugten" Verwendung ist nicht nur die eigenhändige Eingabe erfasst, sondern auch eine mittelbare Eingabe in den Datenverarbeitungsvorgang, bei der sich der Täter einer andere, selbst tatbestandslos oder auch vorsatzlos handelnden Person (des jeweiligen Dateninhabers) bedient. Die Streitfrage, was genau unter dem Merkmal „unbefugt" zu verstehen sei, kann hier zugunsten des eindeutige Umstandes noch dahinstehen, da es dem (bloßen) Eintrag der beiden Daten bereits an einer Beeinflussung eines Datenverarbeitungsvorgangs fehlt – denn es wird nur vorgeblich ein nicht existierender Bearbeitungsvorgang mit Worten suggeriert und eine spätere Rückäußerung angekündigt, jedoch das Ergebnis des Dateneingabevorgangs gerade nicht beeinflusst.

2. Ergebnis

H macht sich bei Eingabe der Daten durch N auf der von ihm erstellten Webseite nicht wegen Computerbetruges in mittelbarer Täterschaft strafbar.

IV. §§ 263a Abs. 2, 22, 23 Abs. 1 StGB, versuchter Computerbetrug

Allerdings könnte sich H durch dieselbe Verhaltensweise wegen versuchten Computerbetruges strafbar gemacht haben.

0. Vorprüfung

Die Vollendung liegt nicht vor (s. zuvor); der Versuch ist strafbar (§§ 263a Abs. 2, 263 Abs. 2, 23 Abs. 1, 12 Abs. 2 StGB).

1. Tatentschluss

Spiegelbildlich zum vollendeten Computerbetrug ist aber nach dem Vorstellungsbild des H der § 263a Abs. 1 StGB auch nicht erfüllt: Sein Vorsatz ist zwar auf die Erlangung von Benutzernamen und Kennwort des N gerichtet. Dessen Eingabe nach Erhalt E-Mail auf den eigens präparierten Webseite bewirkt allerdings keine Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs, sondern ist unbeeinflusstes Ergebnis eines ordnungsgemäßen Dateneingabevorgangs, was er auch weiß.

2. Iediglich hilfsweise: unmittelbares Ansetzen, § 22 StGB

Die Erlangung von Benutzernamen und Kennwort ist überdies auch noch nicht als „unmittelbares" Ansetzen gemäß § 22 StGB anzusehen, da die für einen späteren Zeitpunkt geplante Eingabe der erlangten Daten erst noch weitere deliktische Handlungen des H hinzukommen müssen.

3. Ergebnis

Auch eine Strafbarkeit wegen versuchten Computerbetruges scheidet aus.

V. § 263a Abs. 3 StGB, Vorbereitung eines Computerbetruges

Durch die Einrichtung der Website könnte sich H wegen Vorbereitung eines Computerbetruges gemäß § 263a Abs. 3 StGB strafbar gemacht haben.

1. Objektiver Tatbestand

In Betracht kommt zunächst das Herstellen eines Computerprogrammes, dessen Zweck die Begehung „einer solchen Tat" (des Computerbetrugs) ist. Als Computerprogramme gelten aber nur lauffähige Applikationen mit einer Befehlsfolge an einen Computer und Produzierens eines eigenen Arbeitsergebnisses. Soweit hiernach die Website mit der Entgegennahme von Benutzername und Passwort mittels selbsttätigen Ablaufes ein Arbeitsergebnis zum Vorschein bringt, scheitert die Strafbarkeit am Wortlaut der Norm, weil mittels der Website (noch)

keine solche Tat des Computerbetruges begangen wird und werden soll (s. oben).

2. Ergebnis
H hat sich auch nicht wegen Vorbereitung eines Computerbetruges strafbar gemacht.

VI. § 202a Abs. 1 StGB, Ausspähen von Daten zu Lasten des N
H könnte sich wegen Ausspähens von Daten nach § 202a Abs. 1 StGB strafbar gemacht haben, in dem er dem N die E-Mail zukommen ließ, mithilfe dieser seine Zugangsdaten auf einer von A vorbereiteten Website eingegeben hat.

1. Objektiver Tatbestand.
Die durch N eingegebenen Benutzernamen und Kennwort sind Daten im Sinne des § 202a Abs. 2 StGB. Dieser hat sich H in strafbarer Weise und mithin unbefugt verschafft.

Fraglich ist hier aber, ob die beiden Daten mit einer besonderen Zugangssicherung versehen waren. Denn das Verschaffen durch H hätte gerade unter Überwindung einer solchen Zugangssicherung erfolgen müssen. Hier veranlasst der H den N aber selbst dazu, die in Rede stehenden Daten an seinem Rechner einzugeben und an das dahinterstehende System zu übersenden. Insoweit muss also H gar keine Sicherung gegen unberechtigten Zugang überwinden, sie gelangen vielmehr durch willentliche Eingabe des N an ihn selbst. Mangels der Überwindung einer besonderen Sicherung scheidet eine taugliche Tatbegehung nach § 202a Abs. 1 StGB aus.

2. Ergebnis
H hat sich nicht wegen § 202a Abs. 1 StGB strafbar gemacht.

VII. § 202b StGB, Abfangen von Daten
Bereits nach dem Gesetzeswortlaut scheidet eine Strafbarkeit offensichtlich aus, weil sich H nicht in eine existierende Datenübermittlung zwischen dem N und dem Flugunternehmen schaltet, sondern die Datenübermittlung gezielt und von Anfang an nur zwischen N und dem H als Initiator der umgeleiteten Internetseite stattfindet.

VIII. § 202c StGB, Vorbereitung des Ausspähens und Abfangens von Daten
In Ermangelung der Einschlägigkeit von Straftaten des Ausspähen (§ 202a StGB) und Abfangens (§ 202b StGB) von Daten scheidet auch eine Strafbarkeit gemäß § 202c offensichtlich aus. Im Übrigen gilt das für die Straftat der Vorbereitung des Computerbetrugs zuvor Gesagte entsprechend: Die Herstellung der Website als durchaus taugliches Computerprogramm diente nicht dem Zweck der Begehung einer solchen Tat nach § 202a StGB, sondern dem Erhalt der Daten ohne Überwindung einer etwaigen Zugangssicherung durch Übermittlung durch N.

Zweiter Handlungsabschnitt: Datenverwendung auf Unternehmensseite und Dateiendownload

I. § 202a StGB, Ausspähen von Daten zu Lasten U
Indem sich H Zugang zu dem mit besonderer Zugangssicherung versehenen Login-Bereich des Us durch Eingabe von Benutzername und Kennwort des N verschafft und im dortigen Intranet vielfältige Unternehmensdateien heruntergeladen hat, verschaffte er sich Zugriff auf Daten im Sinne von § 202a StGB, die nicht für ihn bestimmt sind, unter Überwindung einer besonderen (mit personalisierter Kennung geschützten) Zugangssicherung. H handelte zudem vorsätzlich, rechtswidrig und schuldhaft. Für eine Strafverfolgung ist ein Strafantrag nach § 205 Abs. 1 S. 2 StGB, anderenfalls die (hier befürwortende) Bejahung eines besonderen öffentlichen Interesses an der Strafverfolgung für ein gebotenes Einschreiten von Amts wegen vonnöten.

H hat sich hinsichtlich der Datenverwendung nach § 202a Abs. 1 StGB strafbar gemacht.

II. § 263a Abs. 1 StGB, Computerbetrug zu Lasten U
Indem H nach Eingabe von Benutzernamen und Kennwort aus dem Intranet eine Vielzahl von Unternehmensdateien auf seinen USB-Stick heruntergeladen hat, könnte er sich wegen Computerbetruges gemäß § 263a Abs. 1 Var. 3 StGB zu Lasten U strafbar gemacht haben.

1. Objektiver Tatbestand
a) Beeinflussung des Ergebnisses eines Datenverarbeitungsvorganges durch unbefugte Verwendung von Daten
H müsste durch (aa) eine unbefugte Verwendung von Daten (bb) das Ergebnis eines Datenverarbeitungssystems beeinflusst haben.
(aa) Nach welchem Maßstab sich zunächst der Begriff der Befugnis der (hier in Benutzernamen und Kennwort unzweifelhaft verwendeten) Daten bemisst, wird kontrovers beurteilt.

Nach einer subjektivierten Auffassung ist jede Datenverwendung unbefugt, die dem wirklichen oder mutmaßlichen Willen des Datenberechtigten widerspricht. U gestattet in seinem Login-Bereich nur seinen berufsmäßig Beschäftigten den Zugang, sodass es dem Willen der Unternehmensverantwortlichen widerspricht, dass H die Zugangsdaten eines Mitarbeiters benutzt, obwohl er gar nicht in dem Unternehmen beschäftigt ist. H handelte insoweit ohne Befugnis.

Die eine computerspezifische Auslegung favorisierende Auffassung verlangt, dass sich der der Datenverwendung entgegenstehende Wille des Betreibers im Computerprogramm niederschlagen muss. Das soll umgekehrt bedeuten, dass sich derjenige nicht unbefugt verhält, wer den Computer an sich ordnungsgemäß bedient. H hat mittels richtigen Daten nicht auf die Funktionsweise des Datenverarbeitungsprozesses eingewirkt, sodass hiernach kein unbefugtes Handeln vorliege.

Die überwiegende Auffassung nimmt eine betrugsspezifische Auslegung vor und bemisst die Befugnis danach, ob eine Täuschung eines Menschen vorliegen würde, stünde anstelle des Computers ein Mensch. H benutzte Zugangsdaten des N, die nur letzterer im unternehmerischen Geschäftsverkehr zu führen berechtigt war. Dadurch täuschte H dem System aber vor, Mitarbeiter des Unternehmens zu sein und damit zugleich berechtigter Inhaber dieser Zugangsdaten zu sein.

Nur die computerspezifische Auslegung kommt hier zu einem die Strafbarkeit ausschließenden Ergebnis, ist jedoch nach großem Dafürhalten mit den Motiven des Gesetzgebers nicht in Einklang zu bringen, wonach die Vorschrift des Computerbetruges gerade deshalb eingefügt worden war, um Lücken im Vermögensschutz zu schließen. Angesichts der stets fortschreitenden Digitalisierung sollen neue Manipulationsformen bekämpft werden, wonach nicht notwendigerweise ein Mensch, sondern zunehmend Datenverarbeitungssysteme täuschungsbedingt überwunden werden (müssen).
(bb) H hat folglich durch die Eingabe der Zugangsdaten und auch das Herunterladen der Dateien das Ergebnis eines Datenverarbeitungsvorganges dermaßen beeinflusst, dass als systemisches Arbeitsergebnis dem Zugang des angeblichen Mitarbeiters H vertraut und der Dateidownload willentlich und unmittelbar freigegeben wurde.

b) Vermögensschaden
Infolge dieser Beeinflussung des Ergebnisses des Datenverarbeitungsvorganges müsste U einen Vermögensschaden erlitten haben. Ein solcher ist grundsätzlich zu bejahen, wenn ein Vergleich der Vermögenslagen vor und nach der Verfügung ergibt, dass die Vermögensminderung nicht unmittelbar durch ein vermögenswertes Äquivalent ausgeglichen wurde. Hier

ergibt sich die Besonderheit, dass H dem Unternehmen nur Datenkopien entzogen hat, während die Originaldateien weiter bei diesem verbleiben. Ausnahmsweise ist unter normativer Betrachtung jedoch auch der subjektive Wert von Vermögensverschiebungen für die individuellen wirtschaftlichen Verhältnisse des Opfers zu berücksichtigen. Hierfür sind drei Fallgruppen anerkannt:

- dem Opfer werden infolge der täuschungsbedingten Verfügung Mittel entzogen, die für die ordnungsgemäße Erfüllung seiner sonstigen Verbindlichkeiten sowie für eine angemessene Wirtschafts- und Lebensführung unerlässlich sind;
- das Opfer wird durch die täuschungsbedingte Verfügung zu weiteren vermögensschädigenden Maßnahmen genötigt oder
- das Opfer kann die Gegenleistung nicht oder nicht in vollem Umfang zu dem vertraglich vorausgesetzten Zweck oder in anderer zumutbarer Weise verwenden.

Diese für den Betrugstatbestand gemäß § 263 StGB entwickelten Grundsätze eines sog. ‚individuellen Schadenseinschlags' können auch bei § 263a StGB Berücksichtigung finden. Der Verlust der sensiblen Kundeninformationen und Dateien sind für die Wirtschaftsführung von U von überragender Bedeutung und schwerwiegend, weil durch den Datenklau die Unternehmensfortführung konkret und ganz erheblich gefährdet erscheint. Zudem muss U mit diesem Datenverlust erheblich weitere (ggf. auch ggü. den betroffenen Kunden und Unternehmen) vermögensschädigende Maßnahmen vornehmen, um weiteres Übel für den Bestand und auch die Fortführung des Unternehmens abzuwenden. Ein Vermögensschaden ist unter individueller Berücksichtigung in normativer Hinsicht zu bejahen.

2. Subjektiver Tatbestand

H wusste und wollte auch, dass mit seiner Eingabe der nicht für ihn berechtigten Zugangsdaten das Datenverarbeitungssystem mittels unbefugter Verwendung von Daten beeinflusst und durch das Herunterladen der Kundendateien U ein vermögensnachteiliger Schaden zugefügt wird. Zudem wollte H gezielt die Unternehmensdateien als Vorteil herunterladen, handelte also mit der geforderten Bereicherungsabsicht. Der subjektive Tatbestand ist erfüllt.

3. Rechtswidrigkeit und Schuld

H handelte rechtswidrig und schuldhaft.

4. Ergebnis

H hat sich wegen Computerbetruges gemäß § 263a Abs. 1 Var. 3 StGB zu Lasten U strafbar gemacht.

III. §§ 269, 270 StGB, Fälschen beweiserheblicher Daten

Mit der Eingabe der Zugangsdaten des N auf der Unternehmenswebsite und dem Herunterladen der ausgewählten Dateien könnte sich H wegen Fälschung beweiserheblicher Daten gemäß § 269 StGB strafbar gemacht haben.

1. Objektiver Tatbestand

Mit der Eingabe der Zugangsdaten und der Betätigung des Downloads und Sicherung auf dem USB-Stick speichert H Daten gemäß § 202 Abs. 2 StGB (s. oben) in der Weise, dass bei hypothetischer Überführung bei ihrer Wahrnehmung folgendes gilt: Erklärungsinhalt ist die Notwendigkeit des Dateiendownloads offenbar für geschäftliche Zwecke. Durch die Verwendung von Benutzername und Kennwort erklärt der H, entsprechend Mitarbeiter und Verfügungsberechtigter über das Benutzerkonto zu sein und ist damit auch als Aussteller zu erkennen. Indem über diesen Vorgang einen Datensatz im System abgebildet und gespeichert wird, handelt es sich schließlich um beweiserhebliche Daten, sodass bei ihrer Wahrnehmung eine unechte Urkunde vorliegen würde.

2. Subjektiver Tatbestand

H handelte vorsätzlich. Auch handelte H im Zeitpunkt der Tat mit dem Willen, die beweiserheblichen Daten, wenn auch nicht zur Täuschung im Rechtsverkehr, so doch zur nach § 270 StGB gleichgestellten fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr, um an die Dateien aus dem Unternehmensbereich überhaupt zu gelangen und herunterzuladen.

3. Rechtswidrigkeit und Schuld

Ausschlussgründe sind nicht ersichtlich.

4. Ergebnis

H hat sich ebenfalls wegen Fälschens beweiserheblicher Daten gemäß §§ 269, 270 StGB strafbar gemacht.

IV. § 303 Abs. 1 StGB, Datenveränderung

Mit dem Herunterladen der Vielzahl von Dateien hat H weder Daten im Sinne von § 202a Abs. 2 StGB weder gelöscht noch unbrauchbar gemacht oder verändert. Auch ein Unterdrücken scheidet aus, weil durch den Dateidownload lediglich Kopien hergestellt und durch H abgezogen werden, während die Originaldateien im Unternehmensbereich verbleiben und ungehindert weiter zugänglich sind. Eine Strafbarkeit nach § 303a Abs. 1 StGB scheidet aus.

V. § 303b StGB, Computersabotage

Indem H nach Zugangsverschaffung lediglich die ihn interessierenden Dateien auf seinen USB-Stick herunterlädt, scheidet der Tatbestand der Computersabotage gemäß § 303b Abs. 1 StGB gleich aus mehrfachen Gründen aus: Weder wird nach Nr. 1 eine Tat nach § 303a Abs. 1 begangen (s. oben), noch werden durch H gemäß Nr. 2 etwaige Daten eingegeben oder übermittelt, sondern lediglich durch Download abgezogen, und schließlich scheidet nach Nr. 3 auch eine Zerstörung, Beschädigung, Unbrauchbarmachung, Beseitigung oder Veränderung der Datenverarbeitungsanlage des Unternehmens angesichts einer technisch einwandfreien Bedienung aus. Mangels Vorliegen dieser tatbestandlichen Varianten kommt es ebenso wenig auf die Frage nach einer erheblichen Störung an.

Dritter Handlungsabschnitt: Hochladen ins Darknet und Zahlungsaufforderung

I. §§ 253 Abs. 3, 22, 23 Abs. 1 StGB, versuchte Erpressung zu Lasten U

H könnte sich der versuchten Erpressung strafbar gemacht haben, indem er die Dateien im Darknet hochgeladen hat verbunden mit der Aufforderung, U könne mit einer Zahlung in Höhe von 500.000 € dem angedrohten teureren Verkauf an Dritte zuvorkommen.

0. Vorprüfung

Der Erpressungserfolg ist nicht eingetreten, da das Unternehmen nicht zahlte und damit weder durch Tun, Dulden oder Unterlassen noch eine von der Literatur gegensätzlich als „ungeschriebenes Tatbestandsmerkmal" geforderte Vermögensverfügung zeigte. Der Versuch einer Erpressung ist strafbar gemäß § 253 Abs. 3, 23 Abs. 1, 12 Abs. 2 StGB.

1. Tatentschluss

Tatentschluss ist gleich zu verstehen mit Vorsatz (§ 15 StGB), verlangter Maßen also der Wille zur Straftatsverwirklichung in Kenntnis aller objektiven Tatumstände.

Der Tatentschluss des H könnte sich hier auf ein empfindliches Übel bezogen haben. Die angekündigte Weitergabe und

der Verkauf der sensiblen Unternehmensdaten ist grundsätzlich geeignet, einen besonnenen Menschen in der Lage des Betroffenen zur Zahlung des Geldes zu bewegen. Maßgeblich ist hier auf die Opferperspektive abzustellen, das Unternehmen soll das Übel zweifelsohne als nachteilig empfinden. Nach seiner Vorstellung stellt sich H gleichermaßen eine Zahlung als Tun (Rspr.) wie auch eine mit Willen gefasste Transferierung der Geldsumme als Vermögensverfügung (Lit.) vor. Auch nimmt er eine Schadensvertiefung notwendig mit in sein Bewusstsein auf, denn das Unternehmen solle für den Rückerhalt von Daten draufzahlen, über die es bereits selbst verfügt. Auch soweit H keine Datensperrung oder Datenlöschung vor Augen hat, genügt dies nach seinen Vorstellungen für einen Vermögensschaden.

Diese rechtsgrundlose Zahlung durch das Unternehmen erstrebt er zudem spiegelbildlich als Vermögensvorteil, sodass auch die Absicht der rechtswidrigen Bereicherung zu bejahen ist.

2. Unmittelbares ansetzen, § 22 StGB

Ein unmittelbares Ansetzen gemäß § 22 StGB liegt nach der vorherrschenden gemischt subjektiv-objektiven Theorie vor, wenn der Täter die Schwelle zum „Jetzt geht's los!" überschritten und und bereits solche Verhaltensweisen vorgenommen hat, die ohne weitere wesentliche Zwischenakte in die Tatbestandsvollendung einmünden. Der Versuch einer Erpressung beginnt bereits mit dem unmittelbaren Ansetzen zur Nötigungshandlung (und hier Drohung mit empfindlichen Übel). Diese Schwelle hat A mit dem Dateiupload und hieran ankündigender Zahlungsaufforderung bei gleichzeitiger Androhung der Konsequenzen überschritten, sodass er damit sämtlich notwendiges Geschehen aus seiner Hand gegeben hat und keine Zwischenschritte mehr bedurfte.

3. Rechtswidrigkeit

Rechtfertigungsgründe für das Verhalten von H sind nicht ersichtlich. Besonders zu berücksichtigen gilt die sog. Verwerflichkeitsklausel in § 253 Abs. 2 StGB, die aber auch hier einschlägig ist, weil das angedrohte Übel (Weiterverkauf sensibler Unternehmensdaten an den Meistbietenden) und angestrebter Zweck (die eigene Bereicherung) keinen auch nur geringstenfalls sozial anerkannten Zusammenhang aufweisen und daher als evident sozial unerträglich und verwerflich anzusehen ist.

4. Schuld und besonders schwerer Fall nach § 253 Abs. 4 StGB

Entschuldigungsgründe wie auch strafzumessungsrelevante Erschwerungsgründe nach § 253 Abs. 4 StGB sind nicht ersichtlich.

5. Ergebnis

H hat sich wegen versuchter Erpressung gemäß §§ 253 Abs. 3, 22, 23 Abs. 1 StGB strafbar gemacht.

II. §§ 240 Abs. 3, 22, 23 Abs. 1 StGB, versuchte Nötigung

In der zuvor geprüften versuchten Erpressung (§§ 253 Abs. 3, 22, 23 Abs. 1 StGB) ist die versuchte Nötigung vollumfänglich enthalten und mitverwirklicht und bedarf keiner gesonderten Erörterung.

III. §§ 263 Abs. 2, 22, 23 Abs. 2 StGB, versuchter Betrug zu Lasten potenzieller Käufer im Darknet

Eine diesbezügliche Versuchsstrafbarkeit an potenziellen Käufern scheidet offenkundig aus, da H den Umstand der zuvor auf illegitime Weise erlangen Dateien wahrheitsgemäß geäußert hat und damit kein täuschungsbeabsichtigtes Verhalten von ihm intendiert ist.

IV. §§ 202d, 22, 23 Abs. 1 StGB, versuchte Datenhehlerei(?)

Eine solche Strafbarkeit ist vom Gesetzgeber angesichts des Deliktscharakters als Vergehen (vgl. § 12 Abs. 2 StGB) nicht mit ausdrücklicher Versuchsstrafe (vgl. § 23 Abs. 1 StGB) – und demnach anders als bei der (Sach-)Hehlerei gemäß § 259 Abs. 3 StGB(!) – belegt.

1 Der Autor ist Professor für Strafrecht, Staatsrecht und Europarecht am Studienort Hagen der Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen und zudem Lehrbeauftragter für Cyberkriminalität und Strafrecht am Cyber Campus NRW.