*Jan Marcel Stammkötter**

# Ist die Zahlung eines „Lösegeldes“ bei Ransomware strafbar?

## A. Einleitung

Die Technisierung und Digitalisierung des alltäglichen Lebens schreiten schnellen Fußes voran. Angefangen im privaten Bereich erstreckt sich dieser Wandel nun auch immer weiter auf die Berufswelt – doch neben den immensen Vorteilen, die dieser Wandel hin zu einer digitalen Gesellschaft mit sich bringt, gilt es insbesondere auch, die Augen nicht vor den Schattenseiten der steigenden Technisierung zu verschließen: Im Laufe der letzten Jahre ist ein starker Anstieg der Fallzahlen im Bereich der Cyberkriminalität feststellbar.

Eine Schlüsselrolle innerhalb der Cyberkriminalität nimmt der Phänomenbereich der sog. Ransomware ein. Hierbei werden Datenbestände bzw. Datensysteme der Betroffenen durch einen meist gezielten Angriff kompromittiert und verschlüsselt. Ziel der Angreifer ist es, den Betroffenen für die Freigabe bzw. Entschlüsselung der Datenbestände zu einer Lösegeldzahlung zu motivieren. Im Rahmen eines solchen Ransomware-Angriffes und einer damit einhergehenden Verschlüsselung der Daten und Dateisysteme stellt sich den Betroffenen somit die Frage, ob sie der Forderung der Täter, ein in der Höhe näher bestimmtes Lösegeld zur Freigabe der Daten und Dateisysteme zu zahlen, Folge leisten sollen. Mag dieser Gedanke aus unternehmerischer bzw. betriebswirtschaftlicher Sicht durchaus seine Berechtigung haben, so stellt sich auf juristischer Ebene unmittelbar die Frage, ob eine Zahlung des geforderten Lösegeldes eine strafrechtlich relevante Handlung darstellt.

Ziel der nachfolgenden Arbeit ist es, mögliche Strafbarkeitsrisiken bei der Zahlung eines Lösegeldes im Falle eines Ransomware-Angriffes aufzuzeigen und eine Hilfestellung zur Minimierung des möglichen Strafbarkeitsrisikos zu geben. Hierzu werden in einem ersten Teil zunächst der Phänomenbereich Cybercrime bzw. Ransomware vorgestellt, mögliche Angriffsvektoren aufgezeigt und die aktuelle Bedrohungslage erörtert. Im zweiten Teil der Arbeit erfolgt eine Analyse der in Betracht kommenden Straftatbestände. Der Schwerpunkt dieser Erörterung wird auf der Prüfung einer Strafbarkeit wegen Unterstützung einer kriminellen

Vereinigung, strafbar gem. § 129 Abs. 1 S. 2 StGB und weiteren Tatbeständen des Strafgesetzbuches, mithin dem Kernstrafrecht, liegen. Daneben werden auch Strafbarkeitsrisiken im Bereich des Finanz- und Steuerstrafrechts erörtert.

## B. Cybercrime

### I. Cybercrime, Ransomware und Angriffsvektoren

Längst haben sich Straftaten im digitalen Raum etabliert. Bei diesen Straftaten wird zwischen der Cyberkriminalität im engeren Sinne und Cyberkriminalität im weiteren Sinne differenziert. Während letzterer Begriff all die Straftaten beschreibt, die mithilfe des Tatmittels Internet begangen werden, beschreibt erstgenannter Begriff der Cyberkriminalität im engeren Sinne all die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten.[1] Letztgenanntem Deliktsfeld unterfällt auch der Phänomenbereich Ransomware.

Der Begriff Ransomware, zusammengesetzt aus den englischen Worten „ransom“ und „malware“, beschreibt eine Unterkategorie von Schadsoftware. Ziel der hinter einem Ransomware-Angriff stehenden Cyberkriminellen ist es allgemein, die Datensysteme der Betroffenen zu verschlüsseln und für die Freigabe der Daten ein Lösegeld zu erpressen.[2] Im Falle der Nichtzahlung des Lösegeldes wird regelmäßig die Veröffentlichung der Daten angedroht. Bei dieser Form eines Ransomware-Angriffes handelt es sich um eine sog. „Double Extortion“. Daneben existieren – mit untergeordneter Relevanz - die Modi Operandi der Triple Extortion, bei der zusätzlich die Durchführung von DDoS-Attacken auf die IT-Systeme der Betroffenen angedroht wird, wodurch die betroffenen Systeme durch diverse Anfragen überlastet und somit vorübergehend nicht verfügbar sind[3], sowie die Fälle sog. Second Stage Extortion, bei der zusätzlich zum eigentlichen Betroffenen

---

* „Der Verfasser ist Rechtsreferendar am Landgericht Bielefeld. Bei dem Beitrag handelt es sich um eine Studienarbeit aus dem LL.M.-Studiengang „IT und Recht“, welche im Sommersemester 2022 im Seminar „KI, Legal Tech und das IT-Strafrecht“ bei Herrn Prof. Dr. Dominik Brodowski, LL.M. (UPenn) verfasst wurde. Das Seminar wurde mit 15 Punkten bewertet. Die Veröffentlichungsfassung wurde um bis September 2023 veröffentlichte Literatur ergänzt.“

1 *Dreißigacker* et al. in Cyberkriminologie, S. 320.

2 *Vogelgesang* / *Möllers*, jM 2016, 381, 381.

3 *Schröder/Lantwin*, ZD 2021, 614, 615.

auch die Kunden selbiger mit der Veröffentlichung der erlangten Daten im Falle der Nichtzahlung des Lösegeldes erpresst werden.[4]

Eine Infizierung mit Ransomware kann über verschiedenste Wege erfolgen: Häufigstes Einfallstor sind Spam- und Phishing-Nachrichten, die durch Social-Engineering, dem bewussten Ausnutzen menschlicher Eigenschaften wie Vertrauen, Hilfsbereitschaft oder Angst mit dem Ziel der Manipulation des Gegenübers[5], immer weiter professionalisiert und von zumeist unbedarften IT-Anwendern geöffnet werden. Die Schadsoftware befindet sich sodann zumeist als Downloader in beigefügten Dokumenten, die als Geschäftsunterlagen getarnt werden und im allgemeinen Betriebsablauf unverdächtig erscheinen. Wird der Anhang geöffnet, so wird im Hintergrund die eigentliche Schadsoftware heruntergeladen und ausgeführt.[6] Weiterhin möglich sind Infektionen der IT-Systeme durch sog. Drive-By-Downloads, bei der die Schadsoftware automatisch bei Besuch einer infizierten Webseite heruntergeladen wird,[7] sowie eine Ransomware-Infektion durch nicht ausreichend abgesicherte (Heim-) Server[8] und Fernzugänge sowie Schwachstellen in IT-Anwendungen[9]. Immer häufiger gehen die Ransomware-Angreifer dazu über, die Verschlüsselung der Daten erst einige Zeit nach dem unentdeckten Eindringen in das Netzwerk vorzunehmen. Dies führt dazu, dass der Betroffene aufgrund von Beschränkungen bei der Versionierung von Backups nicht ohne Weiteres ein älteres, noch nicht mit der Schadsoftware infiziertes Backup einspielen und der Datenverschlüsselung so entgehen kann.[10]

## II. Aktuelle Bedrohungslage

In der Vorstellung des Bundeslagebildes Cybercrime für das Jahr 2021 am 09.05.2022 beschreibt die Vize-Präsidentin des Bundeskriminalamts Martina Link die Bedrohungslage durch Ransomware als „immens“ und „als die Erscheinung von

4 *BKA*, BLB Cybercrime 2021, S. 2.
5 *Müller*, NZWiSt 2020, 96, 97.
6 *Maihold* in Hdb. BankR, § 33 Rn. 57.
7 *Borges*, NJW 2012, 2385, 2386; *Moos* in Taeger/Gabel, TTDSG, § 19 Rn. 32; *Schmidt/Pruß* in Hdb. IT- u. DSR, Teil A § 3 Rn. 266.
8 *Beukelmann*, NJW-Spez. 2017, 376, 376.
9 S. hierzu z.B. die Schwachstellen log4j (CVE-2021-44228) und Microsoft Exchange (CVE-2021-26855; 26857).
10 *Kölmel*, Digitale Welt 01/2022, 44, 45.

Cyberkriminalität mit dem höchsten Schadpotential“[11]: Die Zahl an Straftaten im Bereich der Cyberkriminalität im engeren Sinne ist erneut um 12% im Vergleich zum Vorjahr angestiegen, die Aufklärungsquote beträgt inzwischen nur noch weniger als 30%. Während allgemein die Anzahl an Straftaten leicht rückläufig ist, nimmt die Zahl an Cyberstraftaten entgegen diesem Trend stark zu.[12] Der finanzielle Schaden durch Ransomware im Berichtsjahr 2021 beläuft sich auf ca. 24,3 Milliarden Euro, sodass sich dieser innerhalb von zwei Jahren in etwa verfünffacht hat.[13] Das durchschnittlich geforderte Lösegeld pro Ransomware-Fall beläuft sich hierbei auf rund 204.695 US-Dollar.[14]

Ebenfalls alarmierend sind die kürzlich veröffentlichten Zahlen des Virenschutzherstellers Sophos: Hiernach waren 66% der befragten Unternehmen im vergangenen Jahr von Ransomware-Angriffen betroffen, 65% der Angriffe resultierten in einer erfolgreichen Verschlüsselung von Daten. Unter anderem aus Angst vor einem vollständigen Datenverlust wurde in 46% der Fälle das geforderte Lösegeld gezahlt, allerdings konnten nur rund 61% der verschlüsselten Daten nach erfolgter Lösegeldzahlung entschlüsselt werden. Lediglich 4% der Unternehmen, die ein Lösegeld zahlten, erhielten die Daten vollständig zurück.[15]

Die Auswirkungen für Betroffene eines Ransomware-Angriffes können enorm sein und weit über bloße Unannehmlichkeiten hinausgehen – angefangen bei der Verschlüsselung privater Daten wie Unterlagen und Fotos auf Heimservern über die Verschlüsselung von Waren- und Wirtschaftssystemen über die Verschlüsselung ganzer kommunaler Datenbestände und -systeme bis hin zur Verschlüsselung ganzer medizinischer Fachsysteme können die Auswirkungen existenz- bzw. gar lebensbedrohlich werden. Neben den Behörden, die eindringlich vor einer Lösegeldzahlung warnen und eine solche auch nicht unterstützen, haben sich nunmehr auch aufgrund dieser dramatischen Auswirkungen, die mit einer Ransomware-Verschlüsselung einhergehen können, diverse IT-Sicherheitsforscher und Netzaktivisten in einem offenen Brief an die Bundesregierung gewandt[16] und u.a. den Erlass wirksamer Maßnahmen zur Unterbindung von Lösegeldzahlungen bei

11 *BKA*, PK-BLB Cybercrime 2021, Min. 07:31.
12 *BKA*, PK-BLB Cybercrime 2021, Min. 02:43.
13 *BitKom e.V./BfV*, Wirtschaftsschutz 2021, Folie 10.
14 *BKA*, BLB Cybercrime 2021, S. 2.
15 Sophos, State of Ransomware 2022, S. 3, 4.
16 *Bodden,* Ransomletter, zul. abgerufen am 28.06.2022.

Ransomware-Erpressungen sowie die Abschaffung der steuerlichen Absetzbarkeit von Lösegeldzahlungen nach § 33 EstG gefordert.

## C. Strafbarkeitsrisiken bei Zahlung des Lösegeldes

Fraglich ist somit, ob die Zahlung eines Lösegeldes im Rahmen eines Ransomware-Angriffes strafrechtlich relevant ist. Strafbarkeitsrisiken des Lösegeldzahlenden ergeben sich hierbei aus dem Kernstrafrecht sowie dem Nebenstrafrecht in Form des Außenwirtschaftsgesetzes sowie der Abgabenordnung.

### I. Strafbarkeit wegen Unterstützung einer kriminellen Vereinigung gem. § 129 Abs. 1 S. 2 StGB

Zunächst könnte sich der Betroffene durch die Zahlung des Lösegeldes gem. § 129 Abs. 1 S. 2 StGB wegen Unterstützung einer kriminellen Vereinigung strafbar machen. Hierzu müsste der Betroffene den Tatbestand rechtswidrig und schuldhaft verwirklichen.

Mit der Strafbarkeit wegen Unterstützung einer kriminellen Vereinigung verfolgt der Gesetzgeber das Ziel, möglichst viele Erscheinungen organisierter Kriminalität von Beginn an und somit bereits in ihren Wurzeln zu bekämpfen.[17] Aus diesem Ansatz des Gesetzgebers ergibt sich auch die besondere rechtspolitische Relevanz der Vorschrift, denn durch die weitgefasste Formulierung dieser Strafvorschrift können bereits viele (teilweise auch nur vorbereitende) Fälle und Handlungen erfasst und sanktioniert werden.[18] Diese weite Fassung der Strafvorschrift stößt insbesondere in der Literatur vielfach auf Kritik[19], denn bereits die Einleitung eines entsprechenden Ermittlungsverfahrens eröffnet den Strafverfolgungsbehörden die Möglichkeit, auf weitreichende strafprozessuale Zwangsmaßnahmen zurückzugreifen: Nach § 100a Abs. 1 S. 1, Abs. 2 S. 1 lit. d) StPO wäre im Rahmen eines Ermittlungsverfahrens die Anordnung einer Telekommunikationsüberwachung je nach Einzelfall statthaft, weiterhin könnten die Instrumente der Onlinedurchsuchung gem. § 100b Abs. 1, 2 S. 1 lit. c) StPO, der akustischen Wohnraumüberwachung gem. § 100c Abs. 1 StPO sowie der Verkehrsdatenüberwachung nach § 100g Abs. 2 S. 1 lit. c) StPO Anwendung

17 *Schäfer/Anstötz* in MüKO-StGB, § 129 Rn. 1, 2.
18 *Sinn/Iden/Pörtner*, ZIS-online 7-8/2021, 435, 441.
19 *Kuhli* in Matt/Renzikowski, StGB, § 129 Rn. 4; m.w.N. § 129a Rn. 6.

finden. Zudem wäre – soweit Anklage erhoben bzw. ein Haftbefehl gegen den Beschuldigten erlassen wird – eine Vermögensbeschlagnahme iSd. § 443 Abs. 1 S. 1 Nr. 1 StPO statthaft. Neben erheblichen strafprozessualen Risiken und Maßnahmen würde eine spätere Verurteilung des Lösegeldzahlenden auf wirtschaftlicher Ebene – sofern dieser als Unternehmer am öffentlichen Wirtschaftsleben beteiligt ist – gar dazu führen, dass der Lösegeldzahlende bzw. dessen Unternehmen gem. § 42 Abs. 1 VgV iVm. § 123 Abs. 1 Nr. 1, Abs. 3 GwB zwingend von öffentlich-rechtlichen Vergabeverfahren auszuschließen ist.[20] Es ist somit insbesondere aufgrund der vorgenannten weitreichenden Ermittlungsbefugnisse der Strafverfolgungsbehörden mehr als fraglich, ob der Verhältnismäßigkeitsgrundsatz noch gewahrt ist, wenn im Falle einer Lösegeldzahlung gegen den Zahlenden nach § 129 Abs. 1 S. 2 StGB vorgegangen wird.

### 1. Tatbestandsmäßigkeit

Tatbestandlich setzt § 129 Abs. 1 S. 2 StGB das vorsätzliche Unterstützen einer kriminellen Vereinigung voraus.

#### a) Kriminelle Vereinigung

Es müsste somit zunächst eine kriminelle Vereinigung als Begünstigte der Lösegeldzahlung vorliegen, derer der Lösegeldzahlende nicht als Mitglied angehört.

Waren die Voraussetzungen über das Vorliegen einer Vereinigung iSd. § 129 Abs. 1 S. 2 StGB bis 2017 in Rechtsprechung und Literatur noch umstritten, so sorgt die durch das 54. StrÄndG vom 17.07.2017 als § 129 Abs. 2 StGB eingefügte Legaldefinition[21] nunmehr für Klarheit über die tatbestandlichen Voraussetzungen: Hiernach ist unter einer Vereinigung „ein auf längere Dauer angelegter, von einer Festlegung von Rollen der Mitglieder, der Kontinuität der Mitgliedschaft und der Ausprägung der Struktur unabhängiger organisierter Zusammenschluss von mehr als zwei Personen zur Verfolgung eines übergeordneten gemeinsamen Interesses“ zu verstehen. Dieser Vereinigungsbegriff ist somit durch ein zeitliches, ein organisatorisches, ein personelles sowie ein voluntatives Element geprägt.[22] Während sich hinsichtlich der Anforderungen an das personelle und zeitliche Element des früheren, rechtsprechungsgeprägten Vereinigungsbegriffs keine Änderungen ergeben haben,[23] so sind

[20] *Opitz* in Burgi/Dreher/Opitz, BK-VergR, § 123 GWB Rn. 21.
[21] BGBl. I, S. 2440: Die Einfügung der Legaldefinition diente der Umsetzung des EU-Rahmenbeschlusses 2008/841/JI.
[22] *Gazeas* in Leipold/Tsambikakis/Zöller, AnwKO StGB, § 129 Rn. 12.
[23] *Schäfer/Anstötz* in MüKO StGB, § 129 Rn. 14a.

tiefgreifende Änderungen bzgl. der Anforderungen an das organisatorische und das voluntative Element feststellbar: Auf organisatorischer Ebene wird nunmehr lediglich ein von „[…] der Struktur unabhängiger organisierter Zusammenschluss […]“ erfordert, sodass der Vereinigungsbegriff nun deutlich mehr Organisationsformen umfasst. Waren vormals ausschließlich Organisationen umfasst, die durch eine klare Aufgabenverteilung, durch Gruppenregeln und somit durch eine feste Struktur gekennzeichnet waren, so werden nunmehr auch Gruppierungen als tatbestandlich relevante Vereinigung erfasst, die über eine grundlegende Organisationsstruktur verfügbar und lediglich in ihren Grundzügen koordiniert werden.[24] Hinsichtlich des voluntativen Elements hat sich der Gesetzgeber im reformierten Vereinigungsbegriff nunmehr vom Merkmal der Verfolgung eines „übergeordneten Gesamtwillens“ verabschiedet.[25] Verlangt wird somit lediglich die Verfolgung eines gemeinsamen Interesses, welches in der Verfolgung von politischen, ideologischen, religiösen oder rein wirtschaftlichen Zielen aufgrund dahingehend geteilter Überzeugungen liegen kann.[26]

Problematisch ist vorliegend jedoch, dass die Täterstrukturen im Bereich Cybercrime nicht vollständig ausermittelt sind. Zwar hob das Bundeskriminalamt auch im aktuellen Bundeslagebericht Cybercrime 2021 hervor, dass eine Entwicklung vom Einzeltäter (sog. „Script-Kiddies“) hin zur hochprofessionellen, möglicherweise gar arbeitsteilig agierenden Ransomware-Gang[27] erkennbar sei, jedoch ist es nach wie vor nicht ausgeschlossen, dass im konkreten Einzelfall ein einzelner Täter handelt. Auch gilt hinsichtlich des zeitlichen Elements des Vereinigungsbegriffes, dass ein Zusammenschluss zwecks einer einmaligen Tatbegehung den Anforderungen an eine Vereinigung nicht genügt.[28] Dies erscheint insbesondere im Falle des arbeitsteiligen Zusammenwirkens problematisch, denn hier sind je nach Angriffsziel unterschiedliche Fachkenntnisse erforderlich, die einen regelmäßigen Wechsel der Beteiligten auf Täterseite erfordern. Es muss mithin prozessual sicher nachweisbar eine Vereinigung im o.g. Sinne vorliegen. Mangelt es an einer solchen Vereinigung oder kann eine solche nicht sicher nachgewiesen werden, so ist eine Strafbarkeit zu verneinen.

---

24 *Selzer*, KriPoZ 04/2018, 224,

25 *Sinn/Iden/Pörtner*, ZIS-online 7-8/2021, 435, 443.

26 *Gazeas* in Leipold/Tsambikakis/Zöller, AnwKO StGB, § 129 Rn. 18; *Schäfer/Anstötz* in MüKO StGB, § 129 Rn. 22.

27 Bei diesen arbeitsteilig agierenden Ransomware-Gruppierungen handelt es sich aus kriminologischer Sicht um den Phänomenbereich des sog. „Cybercrime-as-a-Service“, kurz CaaS, s. hierzu *Manske*, Kriminalistik 2020, 235.

28 *Gazeas* in Leipold/Tsambikakis/Zöller, AnwKO StGB, § 129 Rn. 16.

Kriminell ist die Vereinigung sodann, wenn deren Zweck bzw. Tätigkeit auf die Begehung von Straftaten gerichtet ist, die im Höchstmaß mit Freiheitsstrafe von mindestens zwei Jahren bedroht sind. Die Begehung solcher Straftaten muss mithin der verbindlich festgelegte Zweck sein, zu dessen Erreichen sich die Mitglieder verpflichtet haben.[29] Im Falle eines Ransomware-Angriffes werden seitens der Angreifer zunächst regelmäßig durch das Eindringen in und das Verschlüsseln der Dateien und Datensysteme die Tatbestände der Datenveränderung und Computersabotage, strafbar gem. §§ 30aa Abs. 1, 303b Abs. 1 Nr. 1, 3 StGB, verwirklicht. In Betracht kommt zudem, je nach Einzelfall, die Verwirklichung des Regelbeispiels aus § 303b Abs. 2 StGB, nämlich dann, wenn die Datenverarbeitung für den Betroffenen von wesentlicher Bedeutung ist.[30] Hieran anknüpfend wird sodann regelmäßig durch Forderung des Lösegeldes zur Freigabe der verschlüsselten Datensysteme der Straftatbestand der (zumindest versuchten) Erpressung, strafbar gem. § 253 Abs. 1 (, 3) StGB, verwirklicht.[31] Für den Fall einer Veröffentlichung erlangter Daten im Rahmen der sog. „Double Extortion“ kommt eine Strafbarkeit gem. § 202d Abs. 1 Var.1 StGB in Betracht.[32] Vorgenannte Straftaten sind im Höchstmaß mit Freiheitsstrafe von drei bzw. fünf Jahren bedroht, sodass in aller Regel die in § 129 Abs. 1 S. 1 StGB geforderte Erheblichkeitsschwelle überschritten wird. Zu beachten ist indes, dass ein bloßes Vorbehalten der Begehung von nicht näher definierten Straftaten nicht ausreichend ist[33], sodass insgesamt eine hinreichende Konkretisierung auf die Begehung vorgenannter Straftaten erforderlich ist.

### b) Tathandlung: Unterstützen

Weiterhin ist eine Unterstützungshandlung erforderlich. Eine taugliche Unterstützungshandlung liegt vor, wenn der Lösegeldzahlende als Nichtmitglied der kriminellen Vereinigung den Fortbestand oder die Verwirklichung der Ziele der Vereinigung fördert.[34] Hiervon umfasst sind somit alle der kriminellen Vereinigung objektiv nützlichen Handlungen[35], während der vom Unterstützungstäter beabsichtigte Erfolg nicht eintreten muss.[36] Im Falle einer Lösegeldzahlung an die

29 *Schäfer/Anstötz* in MüKO-StGB, § 129 Rn. 48.
30 Kriterien, nach denen sich die Bestimmung der Wesentlichkeit der Daten-verarbeitung richten kann, finden sich in § 303b Abs. 4 StGB.
31 *Eisele* in Hilgendorf/Kudlich/Valerius, Hdb. StrafR (Bd. 6), Rn. 142.
32 *Gercke*, ZUM 2021, 921, 930.
33 *Schäfer/Anstötz* in MüKO-StGB, § 129 Rn. 49.
34 BGH, NJW 1980, 64, 64.
35 *Fischer*, KO-StGB, § 129 Rn. 40.
36 *Fischer*, KO-StGB, § 129 Rn. 40a.

Ransomware-Angreifer, welche den Angreifern erwünscht und objektiv nützlich ist, ist eine Unterstützungshandlung somit regelmäßig gegeben.

**c) Kein Ausschluss nach Absatz 3**

Weiterhin darf kein Tatbestandsausschluss nach § 129 Abs. 3 StGB einschlägig sein. Ein solcher Ausschluss wird im Regelfalle eines Ransomware-Angriffes nicht einschlägig sein, insbesondere greift der Tatbestandsausschluss aus § 129 Abs. 3 Nr. 2 StGB üblicherweise nicht, denn die Begehung von Straftaten ist regelmäßig der einzig verfolgte Zweck der Vereinigung und somit selbstredend nicht von untergeordneter Relevanz. Dennoch gilt es, den jeweiligen Einzelfall genau zu betrachten.

**d) Subjektiver Tatbestand: Vorsatz**

Auf subjektiver Tatbestandsebene setzt eine Strafbarkeit gem. § 129 Abs. 1 Nr. 2 StGB vorsätzliches Handeln iSd. § 15 StGB voraus, wobei jedoch das Vorliegen von dolus eventualis genügt. Vorsatz meint hierbei den Willen zur Verwirklichung des Straftatbestandes in Kenntnis all seiner objektiven Tatumstände. Der Lösegeldzahlende muss somit den Eintritt des tatbestandlichen Erfolgs ernsthaft für möglich halten und diesen zumindest billigend in Kauf nehmen.

Regelmäßig wird ein durchschnittlich informierter Betroffener im Falle eines Ransomware-Angriffes, bedingt durch die steigende mediale Berichterstattung über Bedrohungen im digitalen Raum, es für möglich halten, dass seine Zahlung an eine kriminelle Vereinigung fließen wird und er somit eine kriminelle Vereinigung unterstützt. Durch die Zahlung des Lösegeldes in der Hoffnung, dass die Daten und Dateisysteme wieder freigegeben werden, nimmt der Betroffene den Erfolgseintritt überdies zumindest billigend in Kauf, auch wenn ihm dieser nicht erwünscht ist. Eine Unterstützungsabsicht oder ein sicheres Wissen über den Empfänger der Zahlung ist ausdrücklich nicht erforderlich, sodass der subjektive Tatbestand in aller Regel verwirklicht wird, wenngleich jeweils der konkrete Einzelfall zu betrachten ist.

### e) Ergebnis Tatbestandsmäßigkeit

In den üblichen Fallkonstellationen einer Lösegeldzahlung im Rahmen eines Ransomware-Angriffes erfüllt der Betroffene mit der Zahlung des Lösegeldes regelmäßig den Tatbestand des § 129 Abs. 1 S. 2 StGB.

## 2. Rechtswidrigkeit

Fraglich ist somit, ob die Handlung gerechtfertigt werden kann. Dies ist der Fall, wenn dem Zahlenden ein Rechtfertigungsgrund zur Verfügung steht. In Betracht kommt eine Rechtfertigung der Tat wegen eines rechtfertigenden Notstandes gem. § 34 StGB.

Im Fall eines Ransomware-Angriffes wird der Betroffene des Angriffes dazu genötigt, eine Zahlung an den Angreifer zu leisten, welche als unterstützende Handlung den Tatbestand des § 129 Abs. 1 S. 2 StGB erfüllt. Die Notstandslage beruht somit auf der Nötigung durch einen Dritten, durch die der Betroffene dazu veranlasst wird, in die Allgemeinrechtsgüter der öffentlichen Sicherheit und der staatlichen Ordnung einzugreifen. Mithin liegt ein Nötigungsnotstand[37] vor. Fraglich und streitig ist, wie dieser in Fällen einer Ransomware-Erpressung rechtlich zu bewerten ist.

Nach einer Ansicht scheide vorliegend eine Rechtfertigung gem. § 34 StGB aus, es könne allenfalls eine Entschuldigung gem. § 35 StGB einschlägig sein. Die Vertreter dieser Ansicht führen an, dass der Notstandstäter bewusst auf die Seite des Unrechts trete und somit zum Werkzeug eines rechtswidrig handelnden Dritten werde. Als solches habe der Notstandstäter keine Solidarität durch die Rechtsgemeinschaft zu erwarten, mithin trete diese hinter dem Rechtsbewährungsinteresse der Allgemeinheit zurück.[38] Zudem wird angeführt, dass dem unbeteiligten Dritten bei pauschaler Billigung eines Notstandsrechts aus § 34 StGB das eigene Notwehrrecht genommen würde, denn die Tat des Notstandstäters wäre bereits nicht rechtswidrig. Problematisch ist vorliegend jedoch, dass § 35 StGB bei Zahlung eines Lösegeldes mangels Notstandsfähigkeit des Rechtsguts Eigentum in aller Regel nicht

37 *Kühl* in Lackner/Kühl, StGB, § 34 Rn. 2.
38 *Perron* in Schönke/Schröder, StGB, § 34 Rn.41b.

einschlägig sein wird,[39] denn von der Vorschrift geschützt werden ausschließlich die Rechtsgüter Leib, Leben und Freiheit in Form der Fortbewegungsfreiheit. Schlussendlich wären nach dieser Ansicht in den üblichen Ransomware-Fällen sowohl eine Rechtfertigung der Zahlung als auch eine Entschuldigung der Zahlung ausgeschlossen.

Nach anderer Ansicht wird vertreten, dass der Notstandstäter bei Vorliegen aller weiteren Voraussetzungen nach § 34 StGB gerechtfertigt sein könne. Hierzu wird angeführt, dass auch der Notstandstäter aufgrund des Vorliegens einer Gefahrensituation die Solidarität der Rechtsgemeinschaft verdiene, wenn dies zum Schutz überwiegender Interessen erforderlich sei. Das Vertrauen in die Rechtsordnung werde hierdurch nicht tangiert, sondern stelle einen Ausfluss der allgemeinen Solidaritätsverpflichtung eines jeden Bürgers dar.[40] Zudem enthalte § 34 StGB keine Beschränkung hinsichtlich der Gefahrenquelle, sodass der Rechtfertigungsgrund nicht über seinen Wortlaut hinaus eingeschränkt werden dürfe, Art. 103 Abs. 2 GG.[41] Maßgeblich für die Bewertung, ob die Tat nach § 34 StGB gerechtfertigt werden kann, sei somit die Interessenabwägung.

Ein pauschaler Ausschluss der Möglichkeit einer Rechtfertigung der Tat erscheint bei einer Lösegeldzahlung im Rahmen eines Ransom-Angriffes nicht sachgerecht, denn dies würde dazu führen, dass die Tat allenfalls über § 35 StGB entschuldigt werden kann. Mangels Notstandsfähigkeit des verletzten Rechtsguts Eigentum wäre jedoch regelmäßig auch eine Entschuldigung der Tat unmöglich. Eine Versagung des Notwehrrechts unbeteiligter Dritter in Fällen, in denen die Zahlung nach § 34 StGB gerechtfertigt wäre, kann – wie von den Vertretern erstgenannter Ansicht herangezogen – in Fällen einer Ransomware-Erpressung indes nicht als Argumentationsgrundlage dienen, denn betroffen wären vorliegend

---

39 In bestimmten Sonderfällen eines Ransomware-Angriffes wäre eine Entschuldigung der Zahlung durch § 35 StGB indes möglich, genannt seien an dieser Stelle Fälle, in denen es zu einer akuten Gefährdung von Menschenleben durch Verschlüsselung medizinischer, möglicherweise lebenserhaltender Infrastruktur kommt. Ein solcher Angriff lag im Jahr 2020 am Universitätsklinikum Düsseldorf vor (s. hierzu Heise, UK Düsseldorf: Ermittlungen nach Tod einer Frau, Beitrag v. 17.09.2020). Das von der zuständigen Staatsanwaltschaft eingeleitete Todesermittlungsverfahren wegen des Verdachts der fahrlässigen Tötung gg. Unbekannt wurde inzwischen eingestellt.

40 *Engländer* in Matt/Renzikowski, StGB, § 34 Rn. 41; *Erb* in MüKO StGB (1), § 34 Rn. 194; *Hauck* in Leipold/Tsambikakis/Zöller, AnwKO StGB, § 35 Rn. 4; *Momsen/Savic* in BeckOK StGB, § 34 Rn.17.

41 *Schmitz* in MüKO StGB (1), § 1 Rn. 16, 18.

Allgemeinrechtsgüter, gegenüber denen ein Notwehrrecht gar nicht besteht[42], nicht hingegen Individualrechtsgüter.

Vorzugswürdig erscheint in Fällen einer Ransomware-Erpressung mithin letztgenannte Ansicht, nach der eine Lösegeldzahlung unter gewissen Voraussetzungen gem. § 34 StGB gerechtfertigt sein kann. Dies folgt insbesondere aus dem Umstand, dass § 34 StGB aufgrund seiner offenen Definition der Notstandslage hinsichtlich des eingeschlossenen Personenkreises sowie der geschützten Rechtsgüter deutlich weiter gefasst ist als § 35 StGB. Maßgebliches Kriterium im Rahmen der rechtlichen Bewertung ist folglich die Interessenabwägung und somit die Frage, ob das schützenswerte Interesse des Zahlenden unter Berücksichtigung des Handelns mit Unrechtsgehalt die Interessen der Allgemeinheit deutlich überwiegt. In vorliegenden Fallkonstellationen hat mithin eine Abwägung der Rechtsgüter der Allgemeinheit in Form der öffentlichen Sicherheit und der staatlichen Ordnung mit den Rechtsgütern des Betroffenen in Form des Eigentums an dessen Daten und Datensystemen zu erfolgen, wobei der jeweilige Einzelfall maßgeblich ist: Bei einer Ransomware-Erpressung einer Verwaltungsbehörde bzw. eines Gerichts treten zu dem geschützten Interesse des vorab genannten Eigentums auch die ebenfalls geschützten Interessen an der Funktionsfähigkeit der öffentlichen Verwaltung bzw. Justiz / Rechtspflege hinzu, was die Interessenabwägung zugunsten der Lösegeldzahlenden beeinflussen könnte. Weiterhin muss die Höhe des geforderten Lösegeldes in die Interessenabwägung miteinbezogen werden. Während bei einer vergleichsweise geringen Lösegeldforderung eher angenommen werden kann, dass das Eigentumsinteresse des Betroffenen den Interessen der Allgemeinheit vorgeht, so wird diese Annahme mit steigender Höhe der Lösegeldforderung umso schwieriger zu halten sein. Angesichts der derzeit geforderten Lösegelder, die in ihrer Höhe stets ansteigen,[43] wird dieser Umstand zunehmend problematischer.

Insgesamt ist somit nach hier vertretener Ansicht eine Rechtfertigung der Lösegeldzahlung nach § 34 StGB grundsätzlich möglich, wenngleich hohe Anforderungen an sie gestellt werden. Ob eine Lösegeldzahlung gerechtfertigt werden kann, ist einzelfallabhängig und lässt sich mithin nicht pauschal beurteilen.

42 *Momsen/Savic* in BeckOK StGB, § 32 Rn. 20.
43 *BKA*, BLB Cybercrime 2021, S. 2.

### 3. Schuld

Ferner dürften dem Lösegeldzahlenden keine Entschuldigungsgründe zur Verfügung stehen.

Wie vorab beschrieben scheidet eine Entschuldigung der Lösegeldzahlung gem. § 35 StGB aus, denn ein einschlägiger Nötigungsnotstand richtet sich im Falle einer Ransomware-Erpressung nach hier vertretener Ansicht nach § 34 StGB. Mithin stehen keine Entschuldigungsgründe zur Verfügung.

### 4. Persönliche Strafaufhebungsgründe

Zuletzt dürften dem Lösegeldzahlenden keine persönlichen Strafmilderungs- bzw. Strafaufhebungsgründe zur Verfügung stehen.

#### a) Mitläuferklausel, § 129 Abs. 6 StGB

In Betracht kommt hierbei zunächst ein fakultatives Absehen von Strafe gemäß der sog. Mitläuferklausel, § 129 Abs. 6 StGB. Voraussetzung hierfür ist kumulativ, dass die Schuld des Lösegeldzahlenden als gering anzusehen ist und die Tathandlung in Form des Unterstützens eine untergeordnete Rolle für die Gesamtgefährlichkeit der kriminellen Vereinigung darstellt.[44] Im Falle einer Lösegeldzahlung im Rahmen einer Ransomware-Erpressung besteht hinsichtlich der Zahlung eine Zwangslage für den Betroffenen, sodass dessen Schuld regelmäßig als gering iSd. § 129 Abs. 6 StGB anzusehen sein wird. Auch hat die Zahlung eines Vermögenswertes einen allenfalls unbedeutenden Einfluss auf die Gesamtgefährlichkeit der Vereinigung, sodass die Voraussetzungen der Mitläuferklausel regelmäßig gegeben sind. Zu beachten ist hierbei jedoch, dass lediglich die Rechtsfolge auf den Schuldspruch beschränkt wird und insbesondere eine Kostentragungspflicht des Angeklagten gem. § 465 Abs. 1 S. 1 StPO bestehen bleibt.[45] Ebenfalls wird durch die Mitläuferklausel ein Absehen von der Verfolgung gem. § 153b StPO ermöglicht.[46]

---

44 *Fischer*, KO-StGB, § 129 Rn. 61.
45 *Stein/Greco* in Wolter, SK-StGB, § 129 Rn. 62.
46 *Beukelmann* in Graf, BeckOK StPO, § 153b Rn. 1, 1.1.

### b) Tätige Reue, § 129 Abs. 7 Nr. 2 StGB

In Betracht kommt weiterhin die Anwendung der Tätige-Reue-Klausel gem. § 129 Abs. 7 Nr. 2 StGB mit der Folge einer fakultativen Strafmilderung gem. § 49 Abs. 2 StGB. Dies setzt voraus, dass durch Offenbarung des Wissens des Lösegeldzahlenden gegenüber den Strafverfolgungsbehörden bereits geplante und diesem bekannte Straftaten verhindert werden können. Im Falle einer Ransomware-Erpressung wäre dies möglich im Rahmen einer Kooperation mit den Strafverfolgungsbehörden dergestalt, dass die Behörden frühzeitig in die Ermittlungen eingebunden werden und der Betroffene den Behörden sämtliche Dateien, beispielsweise in Form eines forensischen Snapshots des betroffenen PCs / Servers oder einer Kopie der kompromittierten E-Mail oder Webseite, weiterleitet, sodass hierüber gegebenenfalls die kompromittierte Webseite oder aber die E-Mail-Server des Angreifers abgeschaltet bzw. gestört werden können, sodass eine Weiterverbreitung der Schadsoftware nicht mehr erfolgen kann. In der Praxis wird es jedoch aufgrund vieler einander tangierender Zuständigkeiten sowie der steigenden technischen Komplexität regelmäßig Schwierigkeiten bereiten, den konkret kompromittierten Server ausfindig zu machen und die Weiterverbreitung der Schadsoftware zu verhindern, sodass die Tätige-Reue-Klausel nach § 129 Abs. 7 Nr. 2 StGB von eher untergeordneter Relevanz ist.

## 5. Anwendbarkeit auf internationale Fälle

Immer häufiger werden Ransomware-Angriffe durch international agierende Ransomware-Gangs, die nicht auf deutschem Hoheitsgebiet beheimatet sind, verübt. Auch in diesem Fall kann sich derjenige, der ein Lösegeld an eine solche ausländische kriminelle Vereinigung zahlt, gem. § 129b Abs. 1 iVm. § 129 Abs. 1 S. 2 StGB strafbar machen.[47,48]

## 6. Ergebnis zu § 129 Abs. 1 S. 2 StGB

Bei Zahlung eines Lösegeldes im Rahmen eines Ransomware-Angriffes kommt eine Strafbarkeit gem. § 129 Abs. 1 S. 2 StGB wegen Unterstützung einer

47 *Altvater*, NStZ 2003, 179, 181; BeckOK StGB, § 129b Rn. 6, 7.

48 § 129b Abs. 1 StGB regelt – neben §§ 3ff. StGB – die Anwendbarkeit deutschen Rechts auf Auslandstaten. Eine ausführlichere Erörterung hierzu findet sich in *Salomon*, MMR 2016, 575, 578.

kriminellen Vereinigung grundsätzlich in Betracht. Insbesondere aufgrund der weitreichenden Ermittlungsbefugnisse der Strafverfolgungsbehörden bei Einleitung eines Ermittlungsverfahrens ist die Anwendbarkeit der Norm auf Lösegeldzahlungen in derartigen Fällen zu kritisieren, allerdings bieten sich regelmäßig zahlreiche Ausstiegsstellen für die Strafverteidigung, um eine Strafbarkeit des Lösegeldzahlenden letztlich zu vermeiden. Zusammenfassend erscheint eine Sanktionierung des Lösegeldzahlenden nicht sachgerecht, denn über die Bußgeld- und Schadensersatzvorschriften der Art. 82 Abs. 1, 83 Abs. 4 lit. a), Abs. 5 lit. a) DSGVO bestehen bereits außerhalb des Strafrechts ausreichende Sanktionierungsmöglichkeiten bezüglich einer mangelhaften Absicherung von IT-Systemen.

## II. Strafbarkeit wegen Terrorismusfinanzierung gem. § 89c Abs. 1 Nr. 3 StGB

Durch die Zahlung eines Lösegeldes könnte sich der Zahlende weiterhin wegen Terrorismusfinanzierung gem. § 89c Abs. 1 Nr. 3 StGB wegen des Bereitstellens von Vermögenswerten zur Begehung einer der dort genannten Straftaten strafbar machen.

Ziel des Gesetzgebers war es bei Einführung der aktuellen Gesetzesfassung ausweislich der Gesetzesbegründung, den Anwendungsbereich der Vorschriften über die Terrorismusfinanzierung auszuweiten, sodass nunmehr sämtliche Formen der Finanzierung terroristischer Vereinigungen strafbewehrt sind. Hierdurch wird beabsichtigt, terroristischen Organisationen unter ausdrücklicher Bezugnahme auf Organisationen wie dem sog. „Islamischen Staat“ bzw. der Terrororganisation „Al-Qaida“, die für den Terroranschlag vom 11.09.2001 auf das World Trade Center in den Vereinigten Staaten verantwortlich ist, die wirtschaftliche Handlungsfähigkeit zu nehmen.[49]

Hinsichtlich Telos und Wortlaut der Norm erscheint es fraglich, ob eine Strafbarkeit wegen Terrorismusfinanzierung bei Zahlung eines Lösegeldes im Rahmen eines Ransomware-Angriffs einschlägig sein kann. Dem Telos der Norm nach dient der Straftatbestand der Terrorismusfinanzierung dazu, Terrororganisationen die wirtschaftliche Handlungsfähigkeit zu nehmen. Zwar wird in § 89c Abs. 1 Nr. 3

[49] BT-Drs. 18/4087, S. 7, 8, 11f.

StGB ausdrücklich die Straftat der Computersabotage iSd. § 303b StGB aufgeführt, die im Regelfall im Rahmen einer Verschlüsselung von Datensystemen und somit im Falle eines Ransomware-Angriffs täterseitig erfüllt wird. Allerdings fällt die Straftat der Computersabotage in den Bereich der mittleren Kriminalität, wohingegen terroristische Straftaten in den Bereich der staatsgefährdenden Schwerstkriminalität fallen, sodass eine Identität der Qualität der Straftaten nicht gegeben ist. Insoweit bestehen erhebliche verfassungsrechtliche Bedenken, zuvorderst an der Bestimmtheit der Vorschrift iSd. Art. 103 Abs. 2 GG sowie an der Verhältnismäßigkeit, ob eine Zahlung eines Lösegeldes bei einem Ransomware-Angriff, die an eine möglicherweise terroristische Vereinigung geleistet wird, dem Tatbestand der Terrorismusfinanzierung unterfallen kann. Es ist ernstlich zu bezweifeln, ob sich der Gesetzgeber im Rahmen der zuletzt erfolgten Anpassung der Norm dieses Spannungsverhältnisses bewusst gewesen ist.

Weiterhin würde eine Zahlung des Lösegeldes mit dem Ziel, die Freigabe der verschlüsselten Daten und Dateisystemen zu erreichen bzw. um die Veröffentlichung der Dateien durch die Angreifer zu unterbinden, erfolgen. Im Falle eines Ransomware-Angriffes wäre es mithin nicht Ziel des Zahlenden, die Begehung weiterer Straftaten gem. § 303b StGB zu finanzieren bzw. allgemein zu fördern. Weiterhin fehlt dem Zahlenden im Regelfalle eines Ransomware-Angriffes ein Einblick in die Struktur der Organisation und somit das Wissen über die weitere Verwendung des Lösegeldes.

Somit stehen der Telos und der Wortlaut der Norm, wobei letzterer insbesondere auf subjektiver Tatbestandsebene das sichere Wissen bzw. die Absicht des Zahlenden verlangt, dass die bereitgestellten Vermögenswerte zur Begehung weiterer, in den Nummern 1 bis 8 näher bezeichneten Straftaten, eingesetzt wird, einer Strafbarkeit des Lösegeldzahlenden gem. § 89c Abs. 1 Nr. 3 StGB wegen Terrorismusfinanzierung entgegen. Obgleich der geäußerten erheblichen verfassungsrechtlichen Bedenken hinsichtlich der Anwendbarkeit der Strafnorm auf die Fälle einer Lösegeldzahlung scheidet eine Strafbarkeit wegen Terrorismusfinanzierung im Fall der Zahlung eines Lösegeldes bei einem Ransomware-Angriff mithin regelmäßig spätestens auf subjektiver Tatbestandsebene aus.

## III. Strafbarkeit wegen Verstoßes gegen ein Bereitstellungsverbot gem. § 18 Abs. 1 Nr. 1 lit. a) AWG

Durch Zahlung des Lösegeldes könnte sich der Betroffene weiterhin wegen eines Verstoßes gegen ein Bereitstellungsverbot, strafbar gem. § 18 Abs. 1 Nr. 1 lit. a) AWG, strafbar machen. Dies setzt voraus, dass der Lösegeldzahlende den Tatbestand rechtswidrig und schuldhaft verwirklicht.

### 1. Tatbestand

Tatbestandlich setzt eine Strafbarkeit gem. § 18 Abs. 1 AWG das vorsätzliche Bereitstellen von Vermögenswerten an von mit staatlichen Sanktionsmaßnahmen belegte Personen oder Organisationen[50] voraus.

#### a) Tathandlung: Bereitstellung

Die Zahlung des Lösegeldes müsste somit zunächst ein tatbestandlich relevantes Bereitstellen von Vermögenswerten darstellen. Die Tatmodalität des Bereitstellens ist im Außenwirtschaftsgesetz nicht definiert.[51] Man versteht hierunter jedes Zur-Verfügung-Stellen von Geldern oder wirtschaftlichen Ressourcen[52], das Tatbestandsmerkmal ist mithin weit[53] gefasst. Durch Zahlung des Lösegeldes stellt der Zahlende den Ransomware-Erpressern unmittelbar Gelder zur Verfügung. Ergo liegt mit der Zahlung des Lösegeldes grds. ein Bereitstellen von Vermögenswerten vor. Diese Bereitstellung muss dem Lösegeldzahlenden jedoch im Strafverfahren sicher und zweifelsfrei nachgewiesen werden können. Probleme können sich an dieser Stelle in der Praxis aus einer Lösegeldzahlung über Kryptowährungen ergeben. Lässt sich dem Betroffenen die Lösegeldzahlung somit prozessual nicht nachweisen, steht dies einer Verurteilung entgegen.

---

50 *Wagner* in MüKO StGB, § 18 AWG Rn. 33.

51 *Nestler* in Esser/Rübenstahl/Saliger/Tsambikakis, WiStR, § 18 AWG Rn. 13.

52 Rückert, GwuR 03/2021, 103, 104; *Wagner* in MüKO StGB, § 18 AWG Rn. 32.

53 Stark kritisiert wird die weite Fassung des Tatbestandsmerkmals von *Hoffmann* in Wabnitz/Janovsky/Schmitt, HdB-WiStStR, § 18 AWG Rn. 79 als „einen bis an die Konturlosigkeit heranreichenden Anwendungsbereich“. Diese Kritik verdient Zuspruch.

### b) Verstoß gegen EU-Rechtsakt

Die Vermögenswerte müssten einer Person oder Organisation, die kraft eines EU-Rechtsakts mit einer wirtschaftlichen Sanktionsmaßnahme belegt ist, bereitgestellt werden.

Unter einem EU-Rechtsakt ist hierbei jede EU-Verordnung, die Finanztransaktionen an bestimmte Länder, Organisationen oder Einzelpersonen zur Durchsetzung beschlossener Sanktionen untersagt, zu verstehen.[54] Ransomware-Angriffe gehen vielfach auf ausländische Tätergruppierungen zurück.[55] Es ist somit im konkreten Einzelfall zu prüfen, ob der Zahlungsempfänger mit einer wirtschaftlichen Sanktionsmaßnahme der EU belegt ist. Von besonderer Relevanz sind hierbei die Zahlungsverbote, mithin EU-Rechtsakte, gegen Nordkorea, gegen den Iran, gegen Russland sowie gegen bekannte Cyberkriminelle.[56]

### c) Vorsatz

Auf subjektiver Tatbestandsebene wird zumindest bedingt vorsätzliches Handeln gefordert.[57] Dies setzt voraus, dass der Lösegeldzahlende den Erfolgseintritt in Form der Bereitstellung von Vermögenswerten an Personen, Länder oder Organisationen, die mit einer wirtschaftlichen Sanktionsmaßnahme der EU belegt sind, ernstlich für möglich hält und diesen billigend in Kauf nimmt.

Aufgrund des Umstandes, dass die Täterstrukturen bei Cyberstraftaten nicht vollständig ausermittelt sind, kann die Identität der Lösegeldfordernden im Einzelfall unklar sein. Insoweit kommt ein vorsatzausschließender Tatbestandsirrtum iSd. § 16 Abs. 1 StGB, der mangels Fahrlässigkeitsstrafbarkeit eine Strafbarkeit nach dem Außenwirtschaftsgesetz entfallen ließe, in Betracht. Ein solcher vorsatzausschließender Tatbestandsirrtum ist indes in Fällen, in denen über Fachmedien hinaus in allgemein zugänglichen Print- und Onlinemedien über konkrete Cyberangriffe einer konkreten Gruppierung nach einem konkreten Muster berichtet wird, ausgeschlossen. Ergo ist im Einzelfall zu ermitteln, ob dem

54 *Stein/von Rummel* in Rüsken, ZollR, § 18 AWG Rn. 6, 8.
55 *BKA*, BLB Cybercrime 2021, S. 32f.
56 S. für Nordkorea Art. 21 VO-EU 2017/1509, für den Iran s. Art. 23 Abs. 3 VO-EU 267/2012, für Russland s. Art. 2 Abs. 2 VO-EU 269/2014, für die bekannten Cyberkriminellen s. Art. 3 Abs. 2 VO-EU 2019/796.
57 *Wagner* in MüKO StGB, § 18 AWG Rn. 12.

Lösegeldzahlenden die Identität der empfangenden Tätergruppierung bekannt ist oder bekannt sein müsste.

#### d) Zwischenergebnis

Der Tatbestand des § 18 Abs. 1 Nr. 1 lit. a) AWG kann im konkreten Einzelfall erfüllt sein.

### 2. Rechtswidrigkeit / Schuld

Der Lösegeldzahlende müsste den Tatbestand rechtswidrig und schuldhaft verwirklichen. Diesem dürften somit keine Rechtfertigungs- oder Entschuldigungsgründe zur Verfügung stehen.

Die Zahlung des Lösegeldes kann jedoch im konkret zu beurteilenden Fall nach hier vertretener Ansicht – unter den vorab unter Punkt C. I. genannten Voraussetzungen – im Rahmen des Nötigungsnotstandes nach § 34 StGB gerechtfertigt sein. Eine Entschuldigung der Tat gem. § 35 StGB scheidet indes nach hier vertretener Ansicht aus.

### 3. Ergebnis zu § 18 Abs. 1 Nr. 1 lit. a) AWG

Eine Strafbarkeit gem. § 18 Aabs.1 Nr. 1 lit. a) AWG ist dem Grunde nach möglich. Es bieten sich jedoch bereits auf Tatbestandsebene mehrere Ausstiegsstellen für die Strafverteidigung, insbesondere hinsichtlich der Nachweisbarkeit der Zahlung sowie hinsichtlich des Vorsatzes. Ebenso wie im Rahmen der Strafbarkeit wegen Unterstützung einer kriminellen Vereinigung ist nach hier vertretener Ansicht eine Rechtfertigung der Lösegeldzahlung nach § 34 StGB möglich.

## IV. Strafbarkeit wegen Geldwäsche gem. § 261 Abs. 1 Nr. 3 StGB

Indem der Betroffene eine Lösegeldzahlung tätigt, könnte er sich weiterhin wegen Geldwäsche gem. § 261 Abs. 1 Nr. 3 StGB strafbar machen.

Eine solche Strafbarkeit setzt jedoch auf tatbestandlicher Ebene voraus, dass der Gegenstand, mithin jeder Vermögenswert[58], welcher dem Dritten verschafft wird, aus einer rechtswidrigen Vortat stammt. Dies wird regelmäßig im Falle einer

[58] *Ruhmannseder* in BeckOK StGB, § 261 Rn. 9.

Zahlung eines Lösegeldes an den Erpresser zwecks Freigabe der verschlüsselten Daten nicht der Fall sein. Mithin scheidet eine Strafbarkeit des Lösegeldzahlenden wegen Geldwäsche gem. § 261 Abs. 1 Nr. 3 StGB im Regelfall aus.

## V. Strafbarkeit wegen Begünstigung gem. § 257 Abs. 1 StGB

Soweit der Ransomware-Erpresser der deutschen Einkommenssteuerpflicht unterliegt, kommt weiterhin eine Strafbarkeit des Lösegeldzahlenden gem. § 257 Abs. 1 StGB wegen Begünstigung einer Steuerhinterziehung in Betracht, welche nach § 369 Abs. 1 Nr. 4 AO als Steuerstraftat einzustufen ist.

### 1. Tatbestandsmäßigkeit

Hierzu müsste dieser zunächst den Tatbestand des § 257 Abs. 1 StGB verwirklichen.

#### a) Rechtswidrige Vortat eines anderen

Dies setzt zunächst das Vorliegen einer rechtswidrigen Vortat, die durch einen anderen begangen wurde, voraus. In Betracht kommt hierbei eine Strafbarkeit wegen Steuerhinterziehung durch Unterlassen, strafbar gem. § 370 Abs. 1 Nr. 2 AO.

Im Falle eines Ransomware-Angriffes wird der Erpresser die getätigte Lösegeldzahlung aus Sorge vor Strafverfolgung[59] regelmäßig nicht in seiner Einkommenssteuerklärung als solches deklarieren. Durch dieses pflichtwidrige Unterlassen der Angabe steuerlich erheblicher Tatsachen in Form von gewerblichen Einkünften nach § 15 EstG gegenüber der zuständigen Finanzbehörde macht sich der Erpresser somit – soweit er der inländischen Einkommenssteuerpflicht unterliegt – einer Steuerhinterziehung durch Unterlassen gem. § 370 Abs. 1 Nr. 2 AO strafbar.[60] Unerheblich ist hierbei gem. § 40 AO der Grund der geleisteten Zahlung, mithin die zugrundeliegende Erpressung. Ergo liegt eine rechtswidrige Vortat eines anderen vor.

---

59 § 116 AO statuiert eine Mitteilungspflicht der Ermittlungsbehörden an das Bundeszentralamt für Steuern bzw. die zuständige Finanzbehörde, soweit ein Anfangsverdacht hinsichtlich der Begehung einer Steuerstraftat vorliegt.

60 *Trinks*, NStZ 2016, 263, 264.

### b) Durch die Vortat erlangter, noch vorhandener Vorteil

Weiterhin muss der Vortäter unmittelbar aus der Tat einen Vorteil materieller Art erlangt haben, der zum Zeitpunkt der Begünstigungshandlung noch vorhanden ist. Unter einem Vorteil ist hierbei jede Verbesserung der rechtlichen, wirtschaftlichen oder tatsächlichen Situation des Vortäters zu verstehen, welche unmittelbar aus der Vortat resultiert.[61] Der Vorteil einer Steuerhinterziehung ist aufgrund der zu niedrigen Steuerfestsetzung durch die sachbearbeitende Finanzbehörde in einer Ersparnis von Abgaben zu sehen.[62] Diese Ersparnis von Steuerzahlungen stellt mithin einen wirtschaftlichen Vorteil dar. Allerdings ist dieser Vorteil zum Zeitpunkt der Begünstigungshandlung, somit bei Zahlung des Lösegeldes, noch nicht vorhanden, denn die zu entrichtenden Steuern werden erst nach Abgabe der Einkommenssteuererklärung festgesetzt. Ein durch die Vortat erlangter Vorteil ist mithin noch nicht vorhanden.

### 2. Zwischenergebnis

Der Tatbestand der Begünstigung ist nicht erfüllt. Eine Strafbarkeit gem. § 257 Abs. 1 StGB scheidet vorliegend aus.

## VI. Strafbarkeit wegen Beihilfe zur Steuerhinterziehung gem. §§ 370 Abs. 1 Nr. 2 AO, 27 StGB

Zuletzt könnte sich der Betroffene durch Zahlung des geforderten Lösegeldes wegen Beihilfe zur Steuerhinterziehung durch Unterlassen, strafbar gem. §§ 370 Abs. 1 Nr. 2 AO, 27 StGB, strafbar machen. Einer näheren Erörterung bedarf zunächst jedoch die Frage, ob eine Beihilfestrafbarkeit zu einer Steuerhinterziehung durch Unterlassen in vorliegender Fallkonstellation überhaupt möglich ist.

Zahlt der Betroffene eines Ransomware-Angriffes das geforderte Lösegeld, so tut er dies, um die Freigabe der verschlüsselten Dateien und Datensysteme zu erwirken bzw. um eine Veröffentlichung der Daten abzuwenden. Das so erwirkte Lösegeld wird der Erpresser aus vorgenannten Gründen regelmäßig nicht in der später abzugebenden Einkommenssteuererklärung als Einkommen aus gewerblicher Tätigkeit iSd. § 15 EstG deklarieren und begeht so eine Steuerhinterziehung

61 *Mückenberger* in Esser/Rübenstahl/Saliger/Tsambikakis, WiStR, § 257 StGB, Rn. 10, 13.
62 *Tsambikakis* in Leipold/Tsambikakis/Zöller, AnwKO StGB, § 257 Rn. 11.

durch Unterlassen. Diese vom Erpresser verwirklichte Straftat stellt aus Sicht des Lösegeldzahlenden, der lediglich die Freigabe der vorab verschlüsselten Daten erwirken möchte, eine unbeabsichtigte Nebenfolge, die durch die Zahlung des Lösegeldes ermöglicht wird, dar. Eine Bestrafung des Lösegeldzahlenden erscheint allerdings, da dieser auf das spätere Handeln des Erpressers keinen Einfluss hat, nicht sachgerecht. Für den konkreten Fall einer Lösegeldzahlung im Rahmen eines Ransomware-Angriffes wurde die Frage einer Strafbarkeit des Lösegeldzahlenden wegen Steuerhinterziehung durch Unterlassen – soweit ersichtlich – gerichtlich noch nicht geklärt. In einer dem Grunde nach vergleichbaren Situation, dem Eingehen des Auftraggebers auf ein Angebot des Werkunternehmers, das in Auftrag gegebene Werk „ohne Rechnung“ mit dem Ziel, die Einnahmen aus dem Rechtsgeschäft nicht zu versteuern, zu erstellen, entschied der 5. Strafsenat des Bundesgerichtshofs[63] dass der Tatvorwurf der Beihilfe zur Steuerhinterziehung - soweit diese nicht das einzige Motiv für den Vertragsabschluss ist - nicht ausschließlich an das Entstehen lassen eines verkürzten Steueranspruches anknüpfen könne und verneinte so eine Strafbarkeit des Auftraggebers wegen Beihilfe zur Steuerhinterziehung durch Unterlassen. Bezieht man diese Entscheidung des BGH auf die vorliegende Fallkonstellation, so ist erkennbar, dass auch bei der Zahlung des Lösegeldes im Rahmen der Ransomware-Erpressung nicht primär bezweckt wird, die Einnahmen aus dem Erpressungsdelikt nicht zu versteuern, sondern eine Freigabe der Daten und Datensysteme erwirkt werden soll. Hinzu tritt, dass die Zahlung des Lösegeldes – entgegen der dem Urteil zugrundeliegenden Sachlage – nicht freiwillig erfolgt, sondern durch den Ransomware-Angriff erzwungen wird. Mithin ist nach hier vertretener Ansicht eine Strafbarkeit des Lösegeldzahlenden wegen Beihilfe zur Steuerhinterziehung durch Unterlassen erst recht zu verneinen.

## D. Resumée und Ausblick

Die vorliegende Arbeit hat gezeigt, dass bei Zahlung eines Lösegeldes im Falle eines Ransomware-Angriffes im konkreten Einzelfall eine Strafbarkeit des Lösegeldzahlenden gegeben sein kann. Den Verantwortlichen in den Unternehmen sowie denjenigen Privaten, die eigene Datensysteme betreiben, ist somit eindringlich zu empfehlen, sich präventiv möglichst zeitnah und umfassend mit dieser Thematik auseinanderzusetzen. Hierbei gilt es auch, bestehende IT-Sicherheitsmechanismen

63 BGH, Urt. v. 23.06.1992, Az.: 5 StR 75/92.

zu evaluieren sowie Reaktionspläne zu entwerfen und an die aktuelle Situation anzupassen.

Eine Strafbarkeit droht insbesondere wegen der Unterstützung einer kriminellen Vereinigung, strafbar gem. § 129 Abs. 1 S. 2 StGB[64] sowie wegen eines Verstoßes gegen ein Bereitstellungsverbot, strafbar gem. § 18 Abs. 1 Nr. 1 lit. a) AWG. Beide Strafbarkeiten haben gemeinsam, dass sich im Rahmen der Strafverteidigung diverse Ausstiegsstellen darbieten, die eine Strafbarkeit im konkreten Einzelfall entfallen lassen können. Allerdings kann bereits die Einleitung eines Ermittlungsverfahrens durch die zuständigen Strafverfolgungsbehörden aufgrund der Statthaftigkeit umfangreicher strafprozessualer Zwangsmaßnahmen erhebliche Eingriffe in den Geschäftsablauf bzw. das Privatleben bedeuten. Diese Gefahr besteht insbesondere hinsichtlich der Strafbarkeit wegen Unterstützung einer kriminellen Vereinigung, dessen Anwendbarkeit auf Lösegeldzahlungen im Falle einer Ransomware-Erpressung zu kritisieren ist. Betonen die Sicherheits- und Strafverfolgungsbehörden zwar regelmäßig die Relevanz einer vertrauensvollen Kooperation zwischen dem Betroffenen und den Behörden, so lässt sich diese unter dem Gesichtspunkt einer drohenden Strafbarkeit und somit mit einer Kriminalisierung des eigentlichen Opfers kaum realisieren. Erforderlich wäre somit zunächst eine Anpassung des § 129 Abs. 1 S. 2 StGB dergestalt, dass sinnvollerweise eine sog. „Safe-Harbor-Lösung“[65] in § 129 StGB eingefügt wird, durch die eine Strafbarkeit unter der Voraussetzung, dass die Zahlung des Lösegeldes behördlich begleitet und somit zumindest eine Verfolgung der Ransomware-Erpresser durch die involvierten Strafverfolgungsbehörden ermöglicht wird, auf Tatbestandsebene ausgenommen wird.[66]

---

64 Dass eine Strafbarkeit gem. § 129 Abs. 1 S. 2 StGB grds. möglich, eine Verurteilung jedoch vergleichsweise unwahrscheinlich ist, bestätigen auch die Zahlen der Strafverfolgungsstatistik: Im Jahre 2018 kam es zu lediglich 25 Verurteilungen, welche sich allesamt nicht auf Ransomware-Lösegeldzahlungen beziehen (*von Hentschel-Heinegg* in BeckOK StGB, § 129 Rn. 33).

65 Insoweit zustimmend *Brodowski* und *Hartmann*, Ransomware-Zahlungen“, WisteV, Düsseldorf 2022.

66 Weiterhin denkbar wäre insbesondere eine Verfahrenseinstellung gem. der §§ 153ff. StPO – diese führen allerdings nicht zur Vermeidung der vorab kritisierten Ermittlungsmaßnahmen und hinterlassen wegen der Feststellung einer „geringen Schuld“ zumindest einen ugs. „negativen Beigeschmack“.

Dass eine wie vorab beschriebene Kriminalisierung des eigentlichen Tatopfers nicht sachdienlich erscheint und eine solche die Kooperationsbereitschaft der Betroffenen hemmt, haben inzwischen auch die Strafverfolgungsbehörden erkannt und setzen zunehmend auf niederschwellige Informationsangebote mit teils humorvollen Elementen[67], um auf die Wichtigkeit strafrechtlicher Ermittlungen hinzuweisen und Vorurteile hinsichtlich der durch Ermittlungsmaßnahmen befürchteter Einschnitte im betrieblichen Umfeld abzubauen.[68]

Abschließend empfiehlt es sich für den Fall, dass ein Ransomware-Angriff bereits erfolgreich durchgeführt wurde, bereits frühzeitig, möglichst ab Kenntnisnahme von dem Cyberangriff, einen auf IT-Straftaten spezialisierten Strafverteidiger zu konsultieren. Dieser kann im Rahmen einer Kooperation mit den Behörden auf eine geräuschlose Abwicklung des Sachverhalts hinwirken und im optimalen Falle die Einleitung eines Ermittlungsverfahrens vermeiden. Jedenfalls kann dieser, sollte ein Ermittlungsverfahren dennoch eingeleitet werden, über die diversen sich darbietenden Ausstiegsstellen im Regelfalle eine Verurteilung des Lösegeldzahlenden verhindern. Präventiv hingegen sollten die Verantwortlichen den Bereich der IT-Sicherheit insgesamt stärker fokussieren, denn auch bei fehlenden technischen oder organisatorischen Sicherheitsmaßnahmen drohen empfindliche Bußgelder gemäß den Vorschriften der DSGVO.[69] Hierbei sind insbesondere Awareness-Maßnahmen in Form von regelmäßigen Mitarbeiter-Schulungen durchzuführen, weiterhin ist die Implementierung grundlegender Sicherheitsstandards[70] erforderlich. Vergegenwärtigen sollten sich die Verantwortlichen auch stets die Kosten, die mit einer erfolgreichen Verschlüsselung von Datensystemen einhergehen, denn einschließlich des Reputationsschadens, der Neuanschaffungskosten von Hardware, den Kosten für den Einsatz von spezialisierten IT-Forensikern und den eigenen Personalausfällen übersteigen diese die Kosten der Implementierung grundlegender IT-Sicherheitsmechanismen regelmäßig um ein Vielfaches.

---

67 *Meywirth*, Mithilfe Verfolgung Cybercrime (zuletzt abgerufen am 26.07.2022).

68 *BKA*, Handreichung Cyberattacken Unternehmen, S. 2, 3; *Ringwald,* Lagebild der Vorbehalte (zuletzt abgerufen am 27.07.2022).

69 Gemeint sind an dieser Stelle die Bußgeldvorschriften aus Art. 83 Abs. 4 lit. a) sowie des Art. 83 Abs. 5 lit. a) DSGVO.

70 Eine sinnvolle Orientierungshilfe bieten die BSI-Standards sowie die jeweils konkret relevanten Bausteine des IT-Grundschutzes des BSI, s. hierzu: *BSI,* IT-GrSchK 2022, Bst. CON.3; OPS.1.1.4; OPS.1.1.7; APP.3.3; APP.5.3; SYS.1.6.