www.betriebs-berater.de

Betriebs Berater

BB

38|2025

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

15.9.2025 | 80. Jg.
Seiten 2113–2176

DIE ERSTE SEITE

Alexander R. Zumkeller, MBA, RA
Anpassungen im Arbeitsrecht: Auf was wartet die Politik?

WIRTSCHAFTSRECHT

Tabitha Schulze-Bünte, RAin, und **Dr. Patrick Grosmann**, M.A., RA
Ransomware-Angriffe auf Unternehmen: Drohende Strafbarkeitsrisiken im Rahmen von Lösegeldzahlungen | 2115

Dr. Astrid Schnabel, LL.M. (Emory), RAin/FAinArbR, **Ekkehard Hübel**, RA, und **Darja Chabalewski**
Dekarbonisierung und Transformation: Rechtliche Rahmenbedingungen der Bundesförderung Industrie und Klimaschutz (BIK) | 2120

STEUERRECHT

Prof. Dr. Monika Jachmann-Michel, Vors. RiBFH
BB-Rechtsprechungsreport zur Besteuerung der Kapitaleinkünfte 2025 – Teil I | 2135

BILANZRECHT UND BETRIEBSWIRTSCHAFT

Dr. Jens Freiberg, WP
Nur Theater mit der Abgrenzung von Eigen- und Fremdkapital nach IFRS | 2155

ARBEITSRECHT

Isabell Flöter, RAin/FAinArbR, und **Dr. Till Heimann**, RA/FAArbR
Lösungsvorschläge zur Umsetzung der Entgelttransparenzrichtlinie für den deutschen Gesetzgeber | 2164

BB-Rechtsprechungsreport zur Besteuerung der Kapitaleinkünfte 2025 – Teil I

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Tabitha Schulze-Bünte, RAin, und Dr. Patrick Grosmann, M.A., RA

Ransomware-Angriffe auf Unternehmen: Drohende Strafbarkeitsrisiken im Rahmen von Lösegeldzahlungen

Ransomware-Angriffe bedrohen Unternehmen zunehmend und können mit hohen Lösegeldforderungen verbunden sein. Dieser Beitrag analysiert mögliche Strafbarkeitsrisiken von Unternehmensverantwortlichen im Zusammenhang mit Lösegeldzahlungen. Beleuchtet werden dabei neben den in Betracht kommenden Straftatbeständen auch praxisrelevante Rechtfertigungs- und Schuldausschließungsgründe. Der Aufsatz richtet sich insbesondere an alle Unternehmensverantwortlichen, Compliance-Beauftragten und Berater, die sich nach einem Cyberangriff Lösegeldforderungen ausgesetzt sehen.

I. Einleitung

Der Bericht zur IT-Sicherheit in Deutschland für das Jahr 2024[1] bewertet die Lage der IT-Sicherheit in Deutschland als „angespannt" und „besorgniserregend".[2] Dabei stellen Ransomware-Angriffe bereits seit Jahren die größte Bedrohung im Bereich der Cyberkriminalität dar.[3]

Der Begriff der Ransomware bezeichnet Schadprogramme, die dazu dienen, Computersysteme zu blockieren und/oder Betriebs- und Nutzerdaten zu verschlüsseln. Auf diese Weise wird der Zugriff auf Daten und Systeme eingeschränkt oder vollständig unterbunden. Für die Freigabe wird die Zahlung von Lösegeld (englisch: Ransom) gefordert.[4] Zahlen die Geschädigten nicht, wird regelmäßig mit einer Daten-Veröffentlichung gedroht.[5] Für den Fall einer Lösegeldzahlung werden eine Entschlüsselung der Daten sowie das Unterlassen ihrer Veröffentlichung, etwa im Darknet, in Aussicht gestellt (sog. „double extortion").[6] Um Unternehmen, die über wirksame Backups verfügen, ebenfalls zur Lösegeldzahlung zu veranlassen, greifen Cyberkriminelle immer wieder auch auf Backups zu und nehmen Verschlüsselungen vor.[7] In den Fällen der sog. „second stage extortion" setzen die Cyberkriminellen die erlangten Daten schließlich ein, um Kunden der zunächst angegriffenen Unternehmen zu attackieren oder zu erpressen.[8]

Es ist zu beobachten, dass die Cyberkriminellen zunehmend professionell und inzwischen auch arbeitsteilig vorgehen. Vom Zugang auf das betroffene Netzwerk, über Schadsoftware bis hin zur „Unterstützung" bei Lösegeldverhandlungen sind Hilfsmittel für alle „Arbeitsschritte" eines Ransomware-Angriffs quasi als Dienstleistungen verfügbar. So bietet beispielsweise die bekannte Hackergruppierung Lockbit ihre Schadsoftware als „Ransomware as a Service" („RaaS") an. Lockbit greift Unternehmen dabei nicht selbst an, sondern stellt ihre Schadsoftware zur Verfügung. RaaS ermöglicht es damit auch Einzeltätern, professionelle Angriffe durchzuführen. Gleichzeitig spezialisieren sich die Cyberkriminellen und können die von ihnen entwickelten Programme weiter verbessern. Darüber hinaus machen sie ihre Dienstleistungen schnell einem größeren Kreis eigentlicher Cyberkrimineller, sog. „Affiliates", zugänglich. Haben diese Lösegelder eingetrieben, zahlen sie an die Anbieter der von ihnen genutzten „Dienstleistungen" häufig eine Provision.[9]

Auf diese Weise sollen für den Berichtszeitraum 2024 weltweit Lösegelder in Höhe von 1,1 Mrd. USD vereinnahmt worden sein – die Dunkelziffer dürfte deutlich darüber liegen.[10] Die Angriffe kommen betroffene Unternehmen also teuer zu stehen. So gaben 57 % der Betroffenen im Rahmen einer Studie für das Jahr 2025 an, die Lösegeldforderung habe mindestens 1 Mio. USD betragen, 24 % der Forderungen lagen bei 5 Mio. USD oder darüber.[11] Die Angriffe betreffen umsatzstarke Großunternehmen ebenso wie kleine und mittlere Unternehmen (KMU), Kommunen, Universitäten und Forschungseinrichtungen sowie immer wieder auch IT-Dienstleister.[12] Die Auswirkungen von Angriffen in der Lieferkette stellen sich aufgrund der damit verbundenen multiplizierenden Wirkung häufig als besonders gravierend dar. So wurde 2024 ein Fall bekannt, der etwa 20 000 Arbeitsplätze in 72 Kommunen mit insgesamt rund 1,7 Mio. Einwohnern betraf.[13]

Dass sich diejenigen, die den Ransomware-Angriff verüben, hierdurch strafbar machen, dürfte auf der Hand liegen. Bei einem Eindringen in das fremde Computersystem droht eine Strafbarkeit wegen Ausspähens von Daten, § 202a Abs. 1 StGB.[14] In Betracht kommt zudem eine Strafbarkeit wegen Datenveränderung gemäß § 303a Abs. 1 StGB sowie wegen Computersabotage nach § 303b Abs. 1 StGB. Die im weiteren Verlauf gegenüber den Betroffenen ausgesprochene Aufforderung zur Zahlung kann ferner den Tatbestand der Erpressung gemäß § 253 Abs. 1 StGB erfüllen.[15] Haben die Cyberkriminellen von Anfang an vor, Daten und Systeme auch im Falle der Zahlung des Lösegeldes nicht freizugeben, kommt zudem eine Strafbarkeit wegen (versuchten) Betrugs gemäß § 263 Abs. 1, Abs. 2 StGB in Betracht.[16]

1 Berichtszeitraum: 1.7.2023 bis 30.6.2024.
2 Lagebericht zur IT-Sicherheit in Deutschland 2024, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html (Abruf: 2.9.2025), S. 8, 90 (nachfolgend: „Lagebericht zur IT-Sicherheit in Deutschland 2024").
3 BKA Bundeslagebild Cybercrime 2023, unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html (Abruf: 16.7.2025), S. 15.
4 Vgl. BSI: Ransomware – Vorsicht vor Erpressersoftware, unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html (Abruf: 2.9.2025).
5 *Gercke*, ZUM 2021, 921, 930.
6 *König*, NZWiSt 2023, 167, 167.
7 Lagebericht zur IT-Sicherheit in Deutschland 2024, S. 45.
8 *Brodowski u. a.*, NStZ 2023, 385, 386.
9 Lagebericht zur IT-Sicherheit in Deutschland 2023, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html (Abruf: 2.9.2025), S. 11.
10 Lagebericht zur IT-Sicherheit in Deutschland 2024, S. 90.
11 Sophos, Ransomware-Report 2025, unter https://www.sophos.com/en-us/content/state-of-ransomware (Abruf: 2.9.2025), S. 9.
12 Lagebericht zur IT-Sicherheit in Deutschland 2024, S. 9 f.
13 Lagebericht zur IT-Sicherheit in Deutschland 2024, S. 10.
14 *Gercke*, ZUM 2021, 921, 930.
15 BGH, 8.4.2021 – 1 StR 78/21, K&R 2021, 576.
16 *Götze/Bicker*, in: Krieger/Schneider, Handbuch Managerhaftung, 4. Aufl. 2023, Rn. 34.136.

Werden die erlangten Daten später tatsächlich veröffentlicht bzw. verkauft, kann den an der damit verbundenen Wertschöpfungskette Beteiligten zudem eine Strafbarkeit wegen Datenhehlerei gemäß § 202d Abs. 1 StGB drohen.[17] Bei einer wissentlichen Veröffentlichung nicht allgemein zugänglicher personenbezogener Daten einer großen Zahl von Personen kommt ferner eine Strafbarkeit gemäß § 42 Abs. 1 BDSG in Betracht.

Wenn auch paradox wirkend, ist die Frage nach den strafrechtlichen Risiken der handelnden Unternehmensbeschäftigten und -verantwortlichen,[18] die – um in jedenfalls versucht redlicher Weise größeren Schaden von ihrem Unternehmen abzuwenden – Lösegeldzahlungen vornehmen, für die Praxis ebenso relevant. Die Einzelheiten sind umstritten, Rechtsprechung hierzu gibt es – soweit ersichtlich – bisher nicht. Der vorliegende Beitrag befasst sich vor diesem Hintergrund mit den Strafbarkeitsrisiken, die Unternehmensverantwortlichen in Folge der Veranlassung entsprechender Zahlungen drohen.

II. Strafbarkeitsrisiken im Zusammenhang mit der Zahlung von Lösegeld

Auch wenn die Zahlung des Lösegeldes die Erpressung der Täter fördert, liegt darin keine strafbare Beihilfe zu einer Erpressung; es handelt sich vielmehr um einen Fall einer (straflosen) notwendigen Beteiligung. Da die Straftaten der Angreifer nicht von dem Katalog des § 140 StGB erfasst sind, ist in der Lösegeldzahlung auch keine Belohnung einer Straftat im Sinne der Norm zu sehen.[19] In Betracht kommen dagegen die im Folgenden dargestellten Delikte.

Bei allen dargestellten Delikten kann bei Vorliegen der entsprechenden Voraussetzungen eine Irrtumskonstellation oder ein Fall fehlender Rechtswidrigkeit bzw. Schuld gegeben sein. Aus Gründen der Darstellbarkeit wird hierauf jedoch lediglich im Zusammenhang mit § 129 StGB ausführlich eingegangen.

III. Unterstützen einer kriminellen Vereinigung

Praktisch relevant ist insbesondere das Strafbarkeitsrisiko wegen Unterstützens einer kriminellen Vereinigung gemäß § 129 Abs. 1 S. 2 StGB.

1. Objektiver Tatbestand

Dazu müsste eine „Tätergruppe", also eine Vereinigung im Sinne des § 129 Abs. 2 StGB, hinter den Cyberangriffen stehen. Eine Vereinigung ist ein auf längere Dauer angelegter, freiwilliger, organisatorischer Zusammenschluss von mindestens drei Personen mit einem übergeordneten gemeinsamen Interesse.[20] Umfassende und belastbare, allgemeine, kriminalistische oder wissenschaftliche Erhebungen zu Täterstrukturen bei Cyberangriffen liegen bisher nicht vor. Allgemein dürfte die zunehmende Anzahl von Hackerangriffen und die Professionalisierung der Angriffe dafürsprechen, dass sich Cyberkriminelle zu Vereinigungen in diesem Sinne zusammengeschlossen haben.

Eine kriminelle Vereinigung unterstützt, wer ihren Fortbestand oder die Verwirklichung ihrer Ziele fördert, ohne selbst Mitglied der Organisation zu sein.[21] Erforderlich, aber auch ausreichend ist es, wenn die Förderungshandlung an sich konkret wirksam, für die Organisation objektiv nützlich ist und dieser irgendeinen Vorteil bringt. Hierunter fällt insbesondere die finanzielle Unterstützung. Dies gilt unabhängig davon, ob die von der kriminellen Vereinigung erlangten Gelder für konkrete Straftaten zum Einsatz kommen.[22] Die Zahlung eines Lösegeldes ist somit im Grundsatz eine Unterstützungshandlung in diesem Sinne.

2. Subjektiver Tatbestand

Auf der subjektiven Tatseite genügt bedingter Vorsatz, bezogen darauf, dass es sich um eine Gruppierung handelt, die sich mit dem Ziel der Begehung von Straftaten zusammengeschlossen hat.[23] Der Unternehmensverantwortliche müsste es hierfür zumindest für möglich halten und billigend in Kauf nehmen, mit der Lösegeldzahlung eine kriminelle Vereinigung zu unterstützen.[24]

Extensiv wird teilweise vertreten, selbst im Falle lediglich bedingten Vorsatzes müsse der Unternehmensverantwortliche die konkreten Tatsachen, aus denen sich die Beteiligung einer kriminellen Vereinigung ergibt, zum Zeitpunkt der Lösegeldzahlung ebenso kennen, wie den kriminellen Zweck bzw. die kriminelle Tätigkeit der Vereinigung. Weiter müsse der Unternehmensverantwortliche die Unterstützung dieser konkreten Vereinigung billigen.[25] Diese Ansicht vernachlässigt, dass im Falle des Eventualvorsatzes gerade keine sichere Kenntnis von der Tatbestandsverwirklichung erforderlich ist. Ausreichend ist vielmehr, dass die Verwirklichung des Tatbestands für möglich erachtet wird.[26] Hierfür können neben steigenden Fallzahlen auch die zunehmende Professionalisierung der Cyberkriminellen sprechen. Auch die wachsende mediale Aufmerksamkeit kann ein Indiz dafür sein, dass der Unternehmensverantwortliche zumindest von der Möglichkeit eines Angriffs durch eine hierauf spezialisierte Vereinigung ausgeht.[27] Gleichzeitig erfolgen zunehmend Sensibilisierungsmaßnahmen zur IT-Sicherheit und zum Datenschutz, sodass häufig ein Bewusstsein für Risiken im Bereich der IT-Sicherheit und damit auch für Ransomware-Angriffe bestehen wird.[28]

Ist die Identität der Gruppierung von Cyberkriminellen durch Veröffentlichungen o. Ä. den Unternehmensverantwortlichen bekannt, wird regelmäßig jedenfalls ein Handeln mit Eventualvorsatz anzunehmen sein.[29] Ist diese unbekannt und gibt sich auch nicht zu erkennen, ist dagegen eine differenziertere Betrachtung angezeigt. Hier liegt es nahe, dass der Unternehmensverantwortliche nicht mit der Möglichkeit des Angriffs einer kriminellen Vereinigung rechnet.[30]

3. Irrtum über Tatumstände

In Betracht kommt zudem ein Irrtum über Tatumstände gemäß § 16 Abs. 1 StGB. Dies ist der Fall, wenn irrtümlich das Fehlen einzelner Tatumstände angenommen wird. In der vorliegenden Konstellation kommt ein Tatbestandsirrtum insbesondere dann in Betracht, wenn der Unternehmensverantwortliche fälschlicherweise davon ausgegangen ist, dass es sich bei dem Empfänger der Lösegeldzahlung um ei-

17 *Gercke*, ZUM 2021, 921, 930.
18 Im Folgenden zur sprachlichen Vereinfachung zusammengefasst als der bzw. die „Unternehmensverantwortliche(n)".
19 So auch *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 31.
20 *Fischer*, StGB, 72. Aufl. 2025, § 129 StGB, Rn. 7.
21 *Schäfer/Anstötz*, in: MüKo StGB, 5. Aufl. 2025, § 129 StGB, Rn. 107.
22 *König*, NZWiSt, 2023, 167, 168; *Schäfer/Anstötz*, in: MüKo StGB, 5. Aufl. 2025, § 129 StGB, Rn. 112.
23 *Schäfer/Anstötz*, in: MüKo StGB, 5. Aufl. 2025, § 129 StGB, Rn. 123; *Fischer*, StGB, 72. Aufl. 2025, § 129 StGB, Rn. 44; *Kulhanek*, in: BeckOK StGB, 63. Ed., Stand: 1.11.2024, § 129 StGB, Rn. 86.
24 Zum Eventualvorsatz *Heger*, in: Lackner/Kühl, StGB, 30. Aufl. 2023, § 15, Rn. 23 f.
25 *Makepeace*, StV 2022, 745, 755 f.; *Götze/Bicker/Skoupil*, in: Krieger/Schneider, Handbuch Managerhaftung, 4. Aufl. 2023, Rn. 34.140.
26 *König*, NZWiSt 2023, 167, 168; *Heger*, in: Lackner/Kühl, StGB, 30. Aufl. 2023, § 15, Rn. 23; *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 34.
27 *König*, NZWiSt 2023, 167, 169; hierzu auch *Kipker/Emmerich*, kes 2025, 66, 67; *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 34.
28 *König*, NZWiSt 2023, 167, 169.
29 *König*, NZWiSt 2023, 167, 169.
30 *König*, NZWiSt 2023, 167, 169, der in diesem Zusammenhang darauf hinweist, dass einem angegriffenen Unternehmen dann, wenn IT-Sicherheitsdienstleister involviert sind, möglicherweise durch diesen die Identität der Hacker als kriminelle Vereinigung bekannt wird; kritisch hierzu *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 34.

nen Einzeltäter handelt. In der Folge entfällt der Vorsatz, § 16 Abs. 1 StGB. Auf eine etwaige Vermeidbarkeit des Irrtums kommt es dabei, anders als im Falle eines Verbotsirrtums nach § 17 StGB, nicht an.[31]

4. Rechtswidrigkeit

Die Tat kann in der Praxis gerechtfertigt sein. Zwar scheidet ein Fall der Notwehr gemäß § 32 StGB aus, weil sich die Notwehrhandlung gegen den Cyberkriminellen, hier die den Ransomware-Angriff verübenden Täter, richten muss,[32] § 129 StGB jedoch die öffentliche Sicherheit und Ordnung schützt.[33] Die Tat des Unternehmensverantwortlichen kann dagegen als rechtfertigender Notstand gemäß § 34 StGB gerechtfertigt sein. Hierzu werden verschiedene Auffassungen vertreten:

In der hier vorliegenden Konstellation eines Nötigungsnotstands wird die Möglichkeit einer Rechtfertigung gemäß § 34 StGB rechtstheoretisch unterschiedlich bewertet. Ein Nötigungsnotstand liegt vor, wenn die Begehung einer Tat erfolgt, „*um einen Dritten von der Realisierung eines Übels abzuhalten, das dieser gerade deshalb angedroht hat, um die Begehung der Tat zu erzwingen*“.[34]

Von den Vertretern der sog. „Entschuldigungslösung“ wird die Möglichkeit einer Rechtfertigung in Fällen verneint, in denen der Täter zur Begehung einer Straftat genötigt wird. Straffreiheit erlange der im Nötigungsnotstand handelnde Täter allenfalls unter den Voraussetzungen des entschuldigenden Notstands gemäß § 35 StGB.[35] Die Vertreter dieser Auffassung stützten sich maßgeblich darauf, dass es das Recht nicht billigen dürfe, wenn sich ein Täter auf die Seite des Unrechts begebe.[36]

Sowohl nach der sog. „Rechtfertigungslösung“ als auch nach der sog. „vermittelnden Rechtfertigungslösung“ steht der Weg einer Rechtfertigung über § 34 StGB dagegen offen. Dabei soll § 34 StGB nach der „Rechtfertigungslösung“ in Fällen des Nötigungsnotstandes uneingeschränkt zur Anwendung kommen. Eine Einschränkung der Notstandsbefugnisse des Genötigten sei nur dann zu rechtfertigen, wenn diesem das Unrecht, das der Nötiger verwirkliche, zugerechnet werden könne. In der hier diskutierten Konstellation sei das Verhalten des Genötigten jedoch nicht frei, er begebe sich daher auch nicht auf die „Seite des Unrechts“. Auf dieser Seite stehe allein der Nötiger.[37]

Nach der „vermittelnden Rechtfertigungslösung“ kommt es dagegen auf eine Interessenabwägung im Einzelfall an. Eine Rechtfertigung der Nötigungsnotstandshandlung wird danach bejaht, wenn die geschützten Interessen die beeinträchtigten Interessen wesentlich überwiegen. Dies soll etwa in Betracht kommen, wenn der Genötigte Delikte „leichterer Kriminalität“ verwirkliche.[38] Dabei erscheint fraglich, dass die „vermittelnde Ansicht“ tatsächlich einen deutlichen Unterschied zur „Rechtfertigungslösung“ bedeutet, da § 34 StGB ohnehin ein wesentliches Überwiegen der geschützten Interessen gegenüber den beeinträchtigten Interessen in dem konkreten Einzelfall erfordert.[39]

Das Ergebnis der nach beiden Rechtfertigungslösungen vorzunehmenden Abwägung ist jedenfalls einzelfallabhängig und kann nicht letztgültig vorausgesagt werden. Sie wird im Zweifel durch die mit der Sache im konkreten Fall befasste Staatsanwaltschaft vorzunehmen sein, sollte diese über die Einleitung eines Ermittlungsverfahrens und später über die Anklageerhebung entscheiden müssen. Anklage kann sie dabei nur bei hinreichendem Tatverdacht, also nur dann erheben, wenn sie es für hinreichend wahrscheinlich erachtet, dass das Gericht den Angeklagten später auch verurteilt (§§ 170 Abs. 1, 203 StPO). Hierbei trifft sie eine eigene Prognoseentscheidung und hat sowohl die tatsächlichen Voraussetzungen als auch die rechtliche Bewertung der Tat zu berücksichtigen.[40] Eine entsprechende Annahme setzt damit auch voraus, dass die Abwägung im Rahmen des Notstandes mit hinreichender Wahrscheinlichkeit zu Lasten des Beschuldigten ausfiele. Indes sprechen gewichtige Argumente dafür, dass das Interesse an dem Schutz des unmittelbar gehackten Unternehmens sowie der Kunden, die mittelbar von dem Cyberangriff betroffen sind, das Interesse an der Vermeidung der Unterstützung einer kriminellen Vereinigung überwiegt. Neben den unmittelbaren finanziellen Auswirkungen kann hierbei auch der Schutz von Arbeitsplätzen zu berücksichtigen sein. Die von § 129 StGB geschützten Rechtsgüter der öffentlichen Sicherheit, der staatlichen Ordnung und des öffentlichen Friedens[41] dürften hierhinter regelmäßig zurücktreten.[42]

Die Auffassungen, die eine Rechtfertigung der Tat des von dem Nötigungsnotstand Betroffenen gemäß § 34 StGB für grundsätzlich möglich erachten, überzeugen. Denn die hier vorliegende Konstellation unterscheidet sich deutlich von den sonst unter der Rechtsfigur des Nötigungsnotstands diskutierten Fallgruppen: Einen durch die Notstandshandlung Betroffenen, der bei Anwendung des § 34 StGB wehrlos gestellt würde, kann es hier nicht geben. Denn § 129 StGB schützt die öffentliche Sicherheit und Ordnung.

Zu berücksichtigen ist zudem, dass eine Entschuldigung der Tat des Betroffenen gemäß § 35 StGB die Abwendung einer Gefahr von Leib, Leben oder Freiheit voraussetzen würde. Hieran wird es in Fällen eines Ransomware-Angriffs jedoch regelmäßig fehlen, mit der Folge, dass der die Lösegeldzahlung veranlassende Unternehmensverantwortliche nach der „Entschuldigungslösung“ in einer Vielzahl von Fällen weder gerechtfertigt noch entschuldigt wäre.[43] Es dürfte dem Vertrauen in die Rechtsordnung jedoch kaum zuträglich sein, wenn das Opfer eines Ransomware-Angriffs wehrlos gestellt und ihm ein „Sonderopfer zugunsten der Unverbrüchlichkeit der Rechtordnung“[44] aufgebürdet würde.

5. Erlaubnistatbestandsirrtum

Wenn der Unternehmensverantwortliche irrig von dem Vorliegen eines rechtfertigenden Notstands gemäß § 34 StGB ausgeht, ist ein Erlaubnistatbestandsirrtum möglich. Dieser liegt vor, wenn sich der Unternehmensverantwortliche irrig Umstände vorstellt, die – wenn sie vorlägen – einen anerkannten Rechtfertigungsgrund begründen würden.[45] Dies ist insbesondere in Konstellationen denkbar, in denen die Interessenabwägung im Rahmen der Prüfung eines rechtfertigenden Notstands (nach Auffassung eines später mit der Sache befassten Gerichts) fehlerhaft erfolgt ist. Dann werden die „*Voraussetzungen eines Rechtfertigungsgrundes im Vorstellungsbild des Täters tatsächlich erfüllt*“.[46] Zwar sind Rechtsfolgen des Erlaubnistatbestandsirrtums seit jeher umstritten. In der Rechtsprechung besteht jedoch Einigkeit darüber, dass der

31 *El-Ghazi*, JA 2020, 182, 183.
32 *Fischer*, StGB, 72. Aufl. 2025, § 32 StGB, Rn. 24.
33 *Heger*, in: Lackner/Kühl, StGB, 30. Aufl. 2023, § 129 StGB, Rn. 1.
34 *Erb*, in: MüKo-StGB, 5. Aufl. 2024, § 34 StGB, Rn. 191.
35 *Brand/Lenk*, JuS 2013, 883, 884; *Perron*, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 34 StGB, Rn. 41b.
36 *Perron*, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 34 StGB, Rn. 41b.
37 *Engländer*, in: Matt/Renzikowski, StGB, 2. Aufl. 2020, § 34 StGB, Rn. 41.
38 Vgl. *Bost*, NZG 2023, 1487, 1489; hierzu auch *Meyer/Biermann*, MMR 2022, 940, 942.
39 Hierzu auch *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 37.
40 *Gorf*, in: BeckOK StPO, 53. Ed., Stand: 1.4.2024, § 170 StPO, Rn. 2.
41 *Schäfer/Anstötz*, in: MüKo-StGB, 5. Aufl. 2025, § 129 StGB, Rn. 1.
42 Anders *Kipker/Emmerich*, kes 2025, 66, 68, die zu dem Schluss gelangen, dass die Abwägung angesichts der Höhe der inzwischen zu zahlenden Summen und der hiermit verbundenen unmittelbaren Förderung der kriminellen Vereinigung regelmäßig nicht mehr zu Gunsten des zahlenden Unternehmens ausfallen wird.
43 *Meyer/Biermann*, MMR 2022, 940, 942.
44 *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 37.
45 BGH, 25.5.2022 – 4 StR 36/22, NStZ 2023, 407.
46 BGH, 25.5.2022 – 4 StR 36/22, NStZ 2023, 407; BGH, 21.11.2019 – 4 StR 166/19, NStZ 2020, 725; hierzu auch *Joecks/Kulhanek*, in: MüKo StGB, 5. Aufl. 2024, § 16 StGB, Rn. 142.

Erlaubnistatbestandsirrtum eine Bestrafung wegen vorsätzlicher Tatbegehung ausschließt.[47]

6. „Mitläuferklausel"

§ 129 Abs. 6 StGB sieht mit der sog. „Mitläuferklausel" die Möglichkeit eines Absehens von der Strafe bei geringer Schuld und Unterstützungen von untergeordneter Bedeutung vor. Beide Tatbestandsvoraussetzungen müssen dabei kumulativ erfüllt sein.[48] Insbesondere muss das jeweilige Verhalten des Täters an der untersten Schwelle der tatbestandlich vorausgesetzten Wirkungsweise liegen.[49] Dies kommt etwa dann in Betracht, wenn nur ein geringer Betrag gezahlt wurde,[50] nicht dagegen, wenn die gezahlten Beträge im Millionenbereich liegen.[51] Es handelt sich insoweit um eine Ermessensvorschrift, die stets eine Betrachtung des Einzelfalls erfordert.[52]

7. Tätige Reue

Erfolgt eine ernsthafte und freiwillige Bemühung, das Fortbestehen der Vereinigung oder die Begehung einer ihren Zielen entsprechenden Straftat zu verhindern (§ 129 Abs. 7 Nr. 1 StGB) oder wird das Wissen bezüglich der Vereinigung offenbart, sodass geplante Straftaten verhindert werden können (§ 129 Abs. 7 Nr. 2 StGB), *kann* ein mit der Sache befasstes Gericht die Strafe zudem mildern oder ganz von ihr absehen. Unternehmensverantwortliche können das Risiko einer möglichen Strafbarkeit demnach vermeiden oder zumindest abmildern, indem sie die Polizei bzw. die Staatsanwaltschaft involvieren und die Übergabe der zu Tat und Tätern bekannten Informationen veranlassen. Da § 129 Abs. 7 StGB eine zwingende Nichtbestrafung lediglich in Fällen des Nichtfortbestehens der Vereinigung vorsieht, schafft die Regelung zur tätigen Reue für Unternehmensverantwortliche allerdings keine Rechtssicherheit.[53]

IV. Unterstützen einer ausländischen kriminellen Vereinigung

Für die Unterstützung einer ausländischen kriminellen Vereinigung verweist § 129b Abs. 1 S. 1 StGB u. a. auf § 129 StGB. Bezieht sich die Tat auf eine Vereinigung außerhalb der Mitgliedstaaten der Europäischen Union, gilt dies gemäß § 129b Abs. 1 S. 2 StGB indes nur, wenn diese durch eine im räumlichen Geltungsbereich des StGB ausgeübte Tätigkeit begangen wird oder wenn der Täter oder das Opfer Deutscher ist oder sich im Inland befindet.

V. Terrorismusfinanzierung

Der Tatbestand der Terrorismusfinanzierung gemäß § 89c Abs. 1 StGB wird regelmäßig in der Praxis nicht erfüllt sein.[54] Die Lösegeldzahlung müsste durch Unternehmensverantwortliche mindestens in dem Wissen erfolgen, dass die Cyberkriminellen das Geld für eine Katalogtat nach § 89c Abs. 1 Nr. 1-8 StGB verwenden werden.[55] In der Regel werden zum Zeitpunkt der Lösegeldzahlung jedoch keine Informationen über mögliche terroristische Aktivitäten der Cyberkriminellen vorliegen. Jedenfalls wird es regelmäßig an dem voluntativen Element des auf eine Terrorismusfinanzierung gerichteten Vorsatzes fehlen.

VI. Untreue

Insbesondere wenn Unternehmensverantwortliche eine Lösegeldzahlung veranlassen, dann jedoch keine Freigabe der Daten durch die Cyberkriminellen erfolgt, können sich Unternehmensverantwortliche in der Praxis dem Vorwurf einer Untreue gemäß § 266 Abs. 1 StGB ausgesetzt sehen. Gerade dann erscheint es möglich, dass unternehmensintern der Vorwurf einer strafbaren Untreue erhoben wird.[56]

Eine Untreue nach § 266 Abs. 1 StGB liegt vor, wenn eine eingeräumte Verfügungs- oder Verpflichtungsbefugnis über fremdes Vermögen missbraucht („Missbrauchstatbestand"), oder eine Treuepflicht, fremde Vermögensinteressen wahrzunehmen, verletzt wird („Treuebruchtatbestand"). In beiden Varianten muss hierdurch demjenigen, dessen Vermögensinteressen zu betreuen sind, ein Nachteil zugefügt werden.

Indes sind auch Fälle denkbar, in denen die Zahlung von Lösegeld innerhalb der rechtlichen Befugnisse des Unternehmensverantwortlichen erfolgt, sodass kein Raum für eine Erfüllung des Missbrauchstatbestands durch Überschreitung der Verfügungs- oder Verpflichtungsbefugnis bleibt. Erfolgt die Lösegeldzahlung etwa im ausdrücklichen Einverständnis der Gesellschafter einer GmbH, scheidet ein Missbrauch der Verfügungs- oder Verpflichtungsbefugnis – und damit auch eine Erfüllung des Missbrauchstatbestands – nach zutreffender Auffassung aus.[57]

Der zulässige Beurteilungsspielraum eines AG-Vorstandsmitglieds oder eines GmbH-Geschäftsführers ist dabei an den Business-Judgement-Rules zu messen.[58] Danach liegt eine Pflichtverletzung eines Vorstandsmitglieds einer AG nicht vor, *„wenn bei einer unternehmerischen Entscheidung vernünftigerweise angenommen werden durfte, auf der Grundlage angemessener Information zum Wohle des Unternehmens zu handeln und das unternehmerische Handeln frei von persönlichen Interessen und sachfremden Einflüssen ist"*.[59]

Jedenfalls dann, wenn bei einem Ransomware-Angriff kurzfristig keine andere Lösung in Betracht kommt, spricht Vieles dafür, dass Vorstandsmitglieder bzw. Geschäftsführer im Falle einer Zahlung zum Wohle des Unternehmens und frei von persönlichen Interessen und sachfremden Einflüssen agieren. Denn die Zahlung erfolgt regelmäßig, um finanzielle Schäden sowie Reputationsschäden und Schäden bei Mitarbeitenden sowie Kunden möglichst gering zu halten.[60]

VII. Geldwäsche

Ein Strafbarkeitsrisiko wegen Geldwäsche gemäß § 261 Abs. 1 S. 1 Nr. 3 StGB dürfte in der Praxis nicht drohen. Denn die Geldwäsche erfordert als Anschlussdelikt eine rechtswidrige Vortat.[61] Nach dem sog. „All-Crimes-Ansatz" könnte die Erpressung durch die Cyberkriminellen selbst zwar als Vortat im Sinne des § 261 StGB zu bewerten sein, aus der die Lösegeldzahlung dann kausal herrühren würde.[62]

47 Vgl. m. w. N. *Joecks/Kulhanek*, in: MüKo StGB, 5. Aufl. 2024, § 16 StGB, Rn. 154.
48 *König*, NZWiSt 2023, 167, 170; *Sternberg-Lieben/Schittenhelm*, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 129 StGB, Rn. 26.
49 *Kuhli*, in: Matt/Renzikowski, StGB, 2. Aufl. 2020, § 129 StGB, Rn. 46; *Sternberg-Lieben/Schittenhelm*, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 129 StGB, Rn. 26.
50 *Brodowski u. a.*, NStZ 2023, 385, 389; *Salomon*, MMR 2016, 575, 578.
51 *König*, NZWiSt 2023, 167, 170.
52 *König*, NZWiSt 2023, 167, 170.
53 *König*, NZWiSt 2023, 167, 170.
54 So auch *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 40.
55 *von Heintschel-Heinegg*, in: BeckOK StGB, 63. Ed., Stand: 1.11.2024, § 89c StGB, Rn. 12.
56 Hierzu auch *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 45 f.
57 *Dierlamm/Becker*, in: MüKo StGB, 4. Aufl. 2022, § 266 StGB, Rn. 161 ff.
58 BGH, 14.7.2008 – II ZR 202/07, NZG 2008, 751, BB 2008, 2370 Ls.; *Ziemons*, in: Michalski, GmbHG Kommentar, 4. Aufl. 2023, § 43 GmbHG, Rn. 134; zur Anwendbarkeit auf die Geschäftsführer einer GmbH sowie ausführlich zur Business Judgement Rule: *Willen*, Die Business Judgement Rule, 2019, S. 12; zum typenübergreifenden Institut: *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 46.
59 *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 46.
60 *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 46.
61 *Ruhmannseder*, in: BeckOK StGB, 63. Ed., Stand: 1.11.2024, § 261 StGB, Rn. 6.
62 *Makepeace*, StV 2022, 754, 756 f.

Dabei muss die Vortat nach der herrschenden Meinung gerade nicht vollendet oder beendet sein, das Vorliegen eines strafbaren Versuchs soll hier ausreichen.[63] Hiergegen wird jedoch zu Recht eingewandt, es gehe zu weit, bereits vor dem Stadium der Vollendung der Erpressung eine Geldwäsche anzunehmen, „weil der gezahlte Vermögensgegenstand aus einem Erpressungsversuch herrühre".[64]

Unabhängig hiervon erscheint es angesichts des Schutzzwecks des § 261 StGB wenig wahrscheinlich, dass mit einem solchen Fall befasste Strafverfolgungsbehörden die Regelung ausgerechnet auf Lösegeldzahlungen von Erpressungsopfern anwenden. Die Regelung soll den „staatliche[n] Zugriff auf illegale Vermögenswerte [sichern] und deren Einschleusen in den legalen Finanz- und Wirtschaftskreislauf verhinder[n]".[65] Illegale Kriminalität soll bekämpft werden,[66] indem ihr die finanzielle Grundlage entzogen wird.[67] Zwar kommen Lösegeldzahlungen den Cyberkriminellen zugute. Dennoch erscheint es wenig wahrscheinlich, dass § 261 StGB gerade gegen die von der Vortat des Cyberkriminellen unmittelbar Betroffenen zur Anwendung gebracht wird.[68]

VIII. Verstoß gegen EU-Sanktionsrecht

Eine Strafbarkeit nach § 18 Abs. 1 AWG aufgrund eines Verstoßes gegen EU-Sanktionsrecht kann dagegen drohen, wenn Gelder an natürliche oder juristische Personen, Organisationen oder Einrichtungen gezahlt werden, die EU-Sanktionen unterliegen. Im Hinblick auf Ransomware-Angriffe ist die Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe zu berücksichtigen. Nach Art. 3 Abs. 2 VO (EU) 2019/796 dürfen den im Anhang[69] Aufgeführten weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugutekommen. Darin werden Personen bzw. Hackergruppen gelistet, die in der Vergangenheit für Ransomware-Angriffe verantwortlich waren.[70]

Selbst wenn die Cyberkriminellen einer EU-Sanktion unterliegen, kann es an dem erforderlichen Vorsatz fehlen, wenn die Identität der Cyberkriminellen den Unternehmensverantwortlichen nicht bekannt ist. Gibt es, etwa nach Untersuchung durch einen spezialisierten externen Dienstleister, Anhaltspunkte, die darauf hindeuten, dass es sich um eine sanktionierte Person oder Vereinigung handelt, wird der subjektive Tatbestand dagegen regelmäßig erfüllt sein.[71]

Ist die Identität der Zahlungsempfänger bekannt, nicht dagegen deren Listung in dem Anhang zur VO (EU) 2019/796, geht die Rechtsprechung vom Vorliegen eines Verbotsirrtums im Sinne des § 17 StGB aus.[72] Für die Strafbarkeit des Täters kommt es dann maßgeblich darauf an, ob dieser den Irrtum, dem er unterlag, vermeiden konnte. Ist der Irrtum nicht vermeidbar, handelt er gemäß § 17 S. 1 StGB ohne Schuld. Hätte er den Irrtum dagegen vermeiden können, kann die Strafe nach § 49 Abs. 1 StGB gemildert werden, § 17 S. 2 StGB. Nach der Gegenansicht handelt es sich um einen Tatbestandsirrtum, sodass allenfalls ein fahrlässiger Verstoß in Betracht kommt, den § 19 Abs. 1 Nr. 1 AWG als Ordnungswidrigkeit sanktioniert.[73]

IX. Fazit und Ausblick

Abhängig von der konkreten Ausgestaltung des jeweiligen Falles und insbesondere von der Kenntnis der Identität der den Angriff verübenden Täter(-gruppe), können Lösegeldzahlung nach einem Ransomware-Angriff grundsätzlich mit Strafbarkeitsrisiken verbunden sein.[74] Von ausgeprägter Relevanz ist dabei die Unterstützung einer (ausländischen) kriminellen Vereinigung. Ermittlungsverfahren in diesem Zusammenhang sind bisher jedoch nicht öffentlich bekannt geworden.

In der Praxis dürften jedoch in den meisten Fällen gute Argumente dafürsprechen, dass die im Rahmen der Prüfung einer Rechtfertigung gemäß § 34 StGB vorzunehmende Interessenabwägung zugunsten der Unternehmensverantwortlichen ausfällt. Auch weil die Gewichtung der hier im Einzelnen gegeneinander abzuwägenden Gesichtspunkte Argumentationsspielräume eröffnet, kann jedoch eine abweichende Bewertung durch die mit dem Sachverhalt befasste Staatsanwaltschaft nicht ausgeschlossen werden. Es empfiehlt sich daher in jedem Fall, frühzeitig rechtlichen Rat einzuholen, auch um darüber zu entscheiden, ob und wann Polizei und Staatsanwaltschaft einbezogen werden sollten.

In der Praxis können D&O-Cyberversicherungen helfen, die individuellen Risiken für Unternehmensverantwortliche und Unternehmen zu reduzieren. Bereits 2017 stellte die BaFin diesbezüglich klar, dass Cyberpolicen, die eine Lösegeldversicherung umfassen, grundsätzlich zulässig sind.[75] Zu berücksichtigen ist indes, dass die Versicherungsunternehmen dann im Falle eines Ransomware-Angriffs regelmäßig in die Entscheidungen über die Zahlung einzubeziehen sind.[76]

Wird Lösegeld gezahlt, sollten Unternehmensverantwortliche sicherstellen, dass hiermit transparent umgegangen und das Vorgehen auch zu Beweiszwecken ausreichend dokumentiert wird. Insbesondere sind entsprechende Zahlungen korrekt darzustellen. Andernfalls können auch hier Strafbarkeitsrisiken drohen, etwa wegen unrichtiger Darstellung gemäß § 331 HGB.[77]

Tabitha Schulze-Bünte, RAin, ist tätig im Bereich Wirtschaftsstrafrecht und Compliance in Frankfurt a. M. Sie promoviert an der Universität Trier zu einer strafprozessualen Thematik mit Verfassungsbezug.

Dr. Patrick Grosmann, M.A., RA, ist tätig in der Kanzlei FPS in Frankfurt a. M. sowie Lehrbeauftragter und Dozent. Er berät Unternehmen im IT- und Datenschutz sowie im Zusammenhang von Cyberangriffen.

63 *Ruhmannseder*, in: BeckOK StGB, 63. Ed., Stand: 1.11.2024, § 261 StGB, Rn. 10; *Makepeace*, StV 2022, 754, 757; *Hecker*, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 261 StGB, Rn. 5.
64 *Brodowski u. a.*, NStZ 2023, 385, 387.
65 BGH, 24.1.2006 – 1 StR 357/05, BGHSt 50, 347, 354.
66 BR-Drs. 620/20, 1; BT-Drs. 19/24180, 1.
67 BT-Drs. 12/989, 26.
68 In diesem Sinne auch *Makepeace*, StV 2022, 754, 757.
69 Anh. I geändert mit Wirkung vom 22.10.2020 durch VO (EU) 2020/1536 v. 22.10.2020 (ABl. L 351 I S. 1); geändert mit Wirkung vom 24.11.2020 durch DVO v. 20.11.2020 (ABl. L 393 S. 1).
70 *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 43.
71 *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 44.
72 BGH, 15.11.2012 – 3 StR 295/12, NZWiSt 2013, 113.
73 *Brodowski u. a.*, NStZ 2023, 385, 387; *Vogel*, Cybersicherheit im Gesundheitswesen, 2024, Kap. 19, Rn. 44.
74 Zu möglichen gesetzgeberischen Klarstellungen im Rahmen einer Überarbeitung des § 129 StGB *Kipker/Emmerich*, kes 2025, 66, 69.
75 BaFin, Lösegeldversicherung: BaFin erlaubt Bündelung mit Versicherung gegen Cyberrisiken, unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html (Abruf: 16.7.2025).
76 *Gercke*, ZUM 2021, 921, 930.
77 *Götze/Bicke*, in: Krieger/Schneider, Handbuch Managerhaftung, 4. Aufl. 2023, Rn. 34.137, 34.146.