Lösegeldzahlungen bei Cyber-Angriffen

Christoph Skoupil, Eike Bicker, Christoph Ehrke und Felix Wrocklage

A. Begriff und Erscheinungsformen

Cyberangriffe und Lösegelderpressungen mittels Schadprogrammen (sog. Ransomware) sind im digitalen Zeitalter eine allgegenwärtige Bedrohung für Unternehmen. Das Bundeskriminalamt (BKA) stuft Ransomware Angriffe bereits seit Jahren als die primäre Bedrohung im Bereich der Cyberkriminalität ein.[1] Diese Bedrohungslage hat auch die deutsche Wirtschaft längst erreicht. In einer Studie des Branchenverbandes Bitkom aus dem Jahr 2024 gaben 80 % der befragten Unternehmen an, dass Cyberangriffe in den vergangenen zwölf Monaten stark oder eher zugenommen haben; der dadurch entstandene Gesamtschaden beläuft sich auf ca. EUR 178,6 Mrd.[2] Insbesondere der Einsatz von Ransomware bei Cyberangriffen steigt dabei rasant an: Während die befragten Unternehmen im Jahr 2022 angaben, dass 12 Prozent der entstandenen Schäden auf Ransomware zurückzuführen waren, hat sich dieser Wert im Jahr 2024 auf 31 Prozent mehr als verdoppelt.[3]

Cyberangriffe können jedes Unternehmen treffen. Während nach wie vor umsatzstarke Großunternehmen zum Opfer von Cyberangriffen werden (sog. „big game hunting"), rücken immer mehr kleine und mittelständische Unternehmen (KMU) in den Fokus von Cyberkriminellen. Diese gelten oftmals als „Weg des geringsten Widerstandes".[4] Während in großen Unternehmen das Verständnis für die Bedrohungslage und die notwendigen Investitionen derzeit schnell wächst, mangelt es in vielen KMU an

1 BKA, Bundeslagebild Cybercrime 2023 (im Folgenden: „Bundeslagebild Cybercrime 2023"), S. 18.

2 Bitkom e.V., Studie „Wirtschaftsschutz 2024" v. 28.8.2024 (im Folgenden: „Studie Wirtschaftsschutz 2024"), S. 12 und 13.

3 Studie Wirtschaftsschutz 2024, S. 15.

4 BSI, Die Lage der IT-Sicherheit in Deutschland 2024 (im Folgenden: „Lagebericht IT-Sicherheit 2024"), S. 61; Europol, Internet Organised Crime Threat Assessment 2024, S. 18.

ausreichender Kenntnis über das eigene Risikoprofil.[5] Erheblichen Risiken sind auch Betreiber kritischer Infrastrukturen (KRITIS) ausgesetzt, deren Störungen sich auf die Versorgung der Bevölkerung mit kritischen Dienstleistungen auswirken können.[6] Insbesondere die Zunahme von IT-Supply-Chains macht IT-Dienstleister zu einem „attraktiven" Angriffsziel, da die Täter mit einzelnen Attacken eine Vielzahl von Unternehmen und Behörden gleichzeitig treffen können.[7] Als Beispiel sei hier der Angriff auf einen kommunalen IT-Dienstleister Ende 2023 genannt, der über 70 Städte und Gemeinden in Nordrhein-Westfalen betraf und deren IT-Infrastruktur weitgehend lahmlegte.[8]

Als Unterfall sog. Malware bezeichnet Ransomware Schadprogramme, die den Zugriff auf Daten und Systeme einschränken bzw. verhindern. Zur Freigabe dieser Daten verlangen die Täter sodann Lösegeldzahlungen (engl. ransom).[9] Regelmäßig bedienen sich die Täter bei dieser Form der digitalen Erpressung des sog. Double Extortion-Modells: Zunächst versuchen die Täter ihre Opfer durch die Verschlüsselung ihrer Daten zu einer Lösegeldzahlung zu bewegen; weigern sich die Angegriffenen, drohen die Täter mit der Veröffentlichung der ausgespähten Daten.[10] Da Unternehmen vermehrt ihre Daten über Backups sichern und durch eine Verschlüsselung allein weniger erpressbar sind, gewinnt die Drohung einer Veröffentlichung an Bedeutung.[11] Um der Forderung Nachdruck zu verleihen, wird die Verschlüsselung und Exfiltration der Daten zudem teilweise mit einem sog. DDoS-Angriff kombiniert, um zudem die bestehende IT-Infrastruktur zu überlasten und dem Angriff Nachdruck zu verleihen.[12] Zur Verschleierung der Zahlungsempfänger der Lösegelder bedienen sich die Täter in der Regel anonymen Zahlungsmitteln wie Kryptowährungen oder anonymen Bezahlkarten, um einen direkten Geldtransfer ohne Einschaltung von Mittelsmännern zu ermöglichen.[13]

5 Lagebericht IT-Sicherheit 2024, S. 69.
6 Lagebericht IT-Sicherheit 2024, S. 62.
7 Bundeslagebild Cybercrime 2023, S. 26.
8 Hackerangriff stellt NRW-Kommunen weiter vor große Probleme, 2.11.2023, abrufbar unter https://www1.wdr.de/ (zuletzt abgerufen am 6.1.2025).
9 BSI, Ransomware Bedrohungslage 2022, S. 4.
10 Lagebericht IT-Sicherheit, S. 47; König/NZWiSt 2023, 167 (167).
11 Bundeslagebild Cybercrime 2023, S. 22 f.; Europol, Internet Organised Crime Threat Assessment 2024, S. 20.
12 Sog. Triple Extortion, vgl. Brodowski/Schmid/Scholzen/Zoller NStZ 2023, 385 (386).
13 BSI, Ransomware Bedrohungslage 2022, S. 4; Heinrichs/Neumeier CB 2022, 14 (15).

Eine Identifizierung der Täter ist oft schwierig. Die aktuelle Aufklärungsquote liegt bei etwa 30 %.[14] Die größte Motivation der Täter im Bereich der Ransomware Angriffe ist der dadurch erhoffte finanzielle Gewinn.[15] Hier ist eine seit Jahren zunehmende Professionalisierung zu erkennen. Die Entwicklung von Ransomware ist zu einem Massengeschäftsmodell geworden (sog. Ransomware-as-a-Service, RaaS).[16] Die Organisationsstruktur der kriminellen Organisationen zeichnet sich dabei durch Internationalität und eine hohe Dynamik aus, die auf nicht klar abgrenzbare Gruppierungen und eine Arbeitsteilung zwischen Entwicklung der Ransomware und Ausführung der Angriffe zurückzuführen ist.[17] Teilweise werden die Täter auch allein zu Sabotagezwecken tätig, sodass die Opfer keine Möglichkeit haben, die Daten zu entschlüsseln.[18] Die Hintergründe dieser Attacken können politischer oder wirtschaftlicher Natur sein, teilweise lassen sie sich auch staatlichen Akteuren zuordnen.[19] Vereinzelt agieren die Täter auch, um sich in der Hacker-Szene einen Namen zu machen oder als sog. Hacktivisten auf gesellschaftliche Problemfelder aufmerksam zu machen.[20]

Angesichts des Zeitdrucks, der mit einem Ransomware Angriff einhergeht, sehen sich betroffene Unternehmen häufig zu einer raschen Entscheidung gezwungen, die wegen der drohenden Konsequenzen für Arbeitnehmer, Kunden und Geschäftspartner oft zugunsten einer Lösegeldzahlung ausfällt.[21] Sicherheitsbehörden raten dagegen von einer Zahlung ab, da es keine Garantie dafür gibt, dass die verschlüsselten Daten tatsächlich wieder freigegeben und gestohlene Daten tatsächlich gelöscht werden.[22] Zudem besteht das Risiko, dass durch die Zahlung Angriffe auf Dritte – oder erneut auf das eigene Unternehmen – finanziert werden.[23] Da die Zahlung des Lösegeldes bei der Wahl zwischen einer Geschäftseinstellung oder der Forderungserfüllung der Erpresser jedoch eine gelebte Praxis darstellt, müssen

14 BKA, Polizeiliche Kriminalstatistik 2023, S. 26.
15 BSI, Ransomware Bedrohungslage 2022, S. 8.
16 BSI, Ransomware Bedrohungslage 2022, S. 14.
17 Bundeslagebild Cybercrime 2023, S. 20.
18 BSI, Ransomware Bedrohungslage 2022, S. 9.
19 3 Jahre NotPetya: Der Erpressungstrojaner, der keiner war, 27.6.2020, abrufbar unter www.heise.de (zuletzt abgerufen am 6.1.2025).
20 BSI, Ransomware Bedrohungslage, S. 9.
21 So betrug die weltweit durchschnittlich gezahlte Lösegeldsumme 2023 621.868 US-Dollar, vgl. Bundeslagebild Cybercrime 2023, S. 18.
22 Lagebericht IT-Sicherheit 2023, S. 19.
23 BSI, Arbeitspapier „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall", S. 15.

sich die Entscheidungsträger der betroffenen Unternehmen auch die potentiellen rechtlichen Risiken dessen vor Augen führen.

Bei der Entscheidung, ob einer Lösegeldforderung nachgekommen werden soll oder nicht, ist zu bedenken, dass stets das Risiko besteht, dass die Erpresser im Falle einer Zahlung ihre Versprechungen, wie z.B. die Entschlüsselung der Daten, nicht einhalten. Auch unter Zeitdruck sollte daher eine sorgfältige Prüfung und Abwägung aller Interessen erfolgen und ggf. externer Rat eingeholt werden. Nach Möglichkeit sollten auch die Ermittlungsbehörden einbezogen und informiert werden.

B. Strafrechtliche Risiken im Falle einer Lösegeldzahlung

I. Der Einsatz von Ransomware als Straftat

Nach Auffassung der höchstrichterlichen Rechtsprechung und der einschlägigen Literatur erfüllt den Tatbestand der Erpressung gem. § 253 StGB, wer Daten auf einem IT-System mit einer Schadsoftware verschlüsselt und die betroffenen Personen zur Zahlung eines Geldbetrags nötigt, um die Zugriffs- und Nutzungssperrungen von IT-Equipment abzuwenden. Die Infektion von Computern und Netzwerken mit entsprechender Schadsoftware und die Installation eines Sperrbildschirms kann überdies eine Datenveränderung nach 303a Abs. 1 Nr. 1 StGB sowie eine (schwere) Computersabotage nach § 303b Abs. 1 Nr. 1 und Abs. 2 StGB sein.[24] Daneben kann eine Strafbarkeit wegen der Bildung einer kriminellen oder terroristischen Vereinigung nach den §§ 129, 129a StGB in Betracht kommen.[25] Plant der Täter die Ransomware von Beginn an so einzusetzen, dass die Daten auch nach erfolgter Zahlung nicht entschlüsselt werden, kommt zudem eine Strafbarkeit wegen (gewerbsmäßigen) Betrugs gem. § 263 StGB in Betracht.[26]

24 BGH Beschl. v. 8.4.2021 – 1 StR 78/21 = NJW 2021, 2301 Rn. 11 ff.; zustimmend Brodowoski/Schmid/Scholzen/Zoller NStZ 2023, 385 (387); M. Gercke ZUM 2021, 921 (930); Neuhöfer/Schefer jurisPR-Compl 5/2021, Anm. 3; Dittrich/Erdogan ZWH 2022, 13 (15 f.); Eisele JZ 2021, 1067 (1067). So auch jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; Vogelgesang/Möllers jM 2016, 381 (383 f.).

25 Siehe hierzu Brodowski/Schmid/Scholzen NStZ 2023, 385 (387).

26 JurisPK-Internetrecht/Heckmann, Kap. 8 Rn. 165; Vogelgesang/Möllers jM 2016, 381 (384). Grundsätzlich auch Eisele JZ 2021, 1067 (1067), nach dem aber der Betrug

II. Strafbarkeitsrisiken für die Geschäftsleitung nach deutschem Recht

1. Straftatbestände

Aus Sicht der von einem Ransomware-Angriff betroffenen Geschäftsleitung tritt (insbesondere wenn die betroffenen Daten nicht mittels Backup oder Unterstützung eines IT-Dienstleisters wiederhergestellt werden können) die Überlegung in den Fokus, eingefordertes Lösegeld zu zahlen, um die Freigabe verschlüsselter Daten zu erreichen. Es bestehen jedoch weiterhin nicht abschließend geklärte Strafbarkeitsrisiken, wenn Geschäftsleiter Zahlungsaufforderungen von Erpressern nachkommen. Auch wenn das Unternehmen in erster Linie Opfer von Cyberattacke und anschließender Erpressung ist, wird kontrovers diskutiert, ob Lösegeldzahlungen eine strafbare Unterstützung einer kriminellen oder terroristischen Vereinigung nach §§ 129, 129a StGB darstellen können.[27] Daneben kommen Verstöße gegen das Finanzsanktionsregime der EU (§ 18 AWG i.V.m. Art. 2 Abs. 2, 2a VO (EU) 881/2002) oder gegen weitere Finanzierungsverbote außereuropäischen Rechts in Betracht.[28] Die mitunter erörterte Gefahr der Terrorismusfinanzierung nach § 89c Abs. 1 Var. 3 StGB[29] wird sich in den Fällen einer Lösegeldzahlung regelmäßig nicht verwirklichen, da der Zahlende (als Täter) dafür mit dem Wissen – bedingter Vorsatz genügt nicht – oder sogar in der Absicht handeln müsste, dass das Lösegeld zur Begehung einer Katalogtat im Sinne des § 89c StGB verwendet werden soll.[30] Eine entsprechende positive Kenntnis eines solchen Verwendungszwecks wird im Zeitpunkt der Lösegeldzahlung regelmäßig fehlen. Die bloße Berichterstattung über die konkreten Täter der Cyberattacke und deren sonstige

---

im Wege der Konkurrenz verdrängt wird oder zumindest an einem eigenständigen Schaden Zweifel bestehen.

27 S. Salomon MMR 2016, 575 (575 ff.); Habbe/Gergen CCZ 2020, 281 (286); Fuhlrott/Schröder NZA-RR 2017, 625 (629); Gabel/Heinrich/Kiefner Rechtshandbuch Cyber-Security/Xylander/Gans Kap. 11 Rn. 21; jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; Scheurer AnwZert ITR 6/2017 Anm. 2; Rückert GWuR 2021, 103 (105).

28 Vgl. Brodowski/Schmid/Scholzen NStZ 2023, 385 (387); Fuhlrott/Schröder NZA-RR 2017, 625 (629); Rückert GWuR 2021, 103 (105). Zur Sanktionierung von Verstößen gegen das unionsrechtliche Außenwirtschafts- und Sanktionsrecht s. Spoerr/Gäde CCZ 2016, 77 (77 ff.).

29 So abstrakt Fuhlrott/Schröder NZA-RR 2017, 625 (629), für die Tatvariante des „zur Verfügung Stellens" von Vermögenswerten.

30 So auch Rückert GWuR 2021, 103 (105). Zu den hohen Anforderungen im subjektiven Tatbestand vgl. BGH Urt. v. 12.11.2020 – 3 StR 31/20 = NStZ 2021, 671 (673) Rn. 27; MünchKomm. StGB/Schäfer/Anstötz StGB § 89c Rn. 15.

kriminelle Aktivitäten reichen grundsätzlich nicht aus, um Anforderungen an den subjektiven Tatbestand zu erfüllen.[31] Abhängig von den Umständen des jeweiligen Einzelfalls kann aber eine Strafbarkeit wegen Urkundenfälschung (§ 267 StGB), Untreue (§ 266 StGB), Steuerhinterziehung (§ 370 AO) und unrichtiger Darstellung (§ 331 HGB) in Betracht kommen, wenn die Geschäftsleitung die wahren Hintergründe der Zahlung verschleiert.[32]

Den Schwerpunkt der strafrechtlichen Diskussion bildet die Frage nach einer Strafbarkeit gemäß den §§ 129, 129a StGB. Der objektive Tatbestand des § 129 StGB verlangt dabei eine Zahlung an eine kriminelle oder terroristische Vereinigung. Hierunter ist ein auf längere Dauer angelegter, organisierter Zusammenschluss von mehr als zwei Personen zur Verfolgung eines übergeordneten gemeinsamen Interesses zu verstehen, dessen Zweck oder Tätigkeit auf die Begehung von bestimmten schweren Straftaten[33] gerichtet ist.[34] Auch wenn die Struktur hinter den Tätern von Ransomware-Angriffen regelmäßig schwer zu ermitteln sein wird, liegt die Annahme einer kriminellen Vereinigung jedenfalls in den Fällen nahe, in denen Hacker-Gruppen den Ransomware-Angriff verüben.[35]

Unter einem Unterstützen im Sinne des § 129 StGB ist grundsätzlich jedes Tätigwerden zu verstehen, das durch ein Nichtmitglied der Vereinigung deren innere Organisation und ihren Zusammenhalt unmittelbar fördert, die Realisierung der von ihr geplanten Straftaten – wenn auch nicht zwingend maßgeblich – erleichtert oder das sich sonst auf deren Handlungsmöglichkeiten oder Zwecksetzung in irgendeiner Weise positiv auswirkt und damit die ihr eigene Gefährlichkeit festigt.[36] Hierfür reicht es aus, dass die Hilfe für die Bestrebungen der Vereinigung in irgendeiner Weise objektiv nützlich und vorteilhaft ist.[37] Der Tatbestand setzt dagegen

31 Rückert GWuR 2021, 103 (105), der für die Bejahung des Vorsatzes eine „glaubhafte, konkrete Information über den Verwendungszweck des gezahlten Lösegeldes (z.B. durch Behörden)" für notwendig hält, die im Regelfall nicht existiert.

32 Vgl. Fuhlrott/Schröder NZA-RR 2017, 625 (629) (Fn. 54).

33 Für die kriminelle Vereinigung auf die Begehung von Straftaten, die im Höchstmaß mit Freiheitsstrafe von mindestens zwei Jahren bedroht sind, und für die terroristische Vereinigung auf die in § 129a StGB aufgeführten Katalogtaten.

34 Vgl. nur Schönke/Schröder/Sternberg-Lieben/Schittenhelm StGB § 129 Rn. 4 f.

35 Brodowski/Schmid/Scholzen NStZ 2023, 385 (387).

36 BGH Urt. v. 19.4.2018 – 3 StR 286/17 = NJW 2018, 2425 (2426); LK-StGB/Krauß StGB § 129 Rn. 120; Schönke/Schröder/Sternberg-Lieben/Schittenhelm StGB § 129 Rn. 15; Lackner/Kühl/Heger StGB § 129 Rn. 6.

37 BGH Urt. v. 25.1.1984 – 3 StR 526/83 (S), juris-Rn. 5 = BGHSt 32, 243 (244); BeckOK StGB/von Heintschel-Heinegg StGB § 129 Rn. 13.

nicht voraus, dass der Vorteil von der Vereinigung konkret genutzt wird oder dass hierdurch eine konkrete, aus der Organisation heraus begangene Straftat oder auch nur eine organisationsbezogene Handlung geprägt wird.[38] Die Zahlung von Geldern an eine entsprechende Organisation ist ein typischer Fall der Unterstützung[39], so dass auch die (erpresste) Auskehr eines Lösegelds als Unterstützungshandlung anzusehen ist.[40] Die Geschäftsleitung muss es für eine Verwirklichung des vollständigen Tatbestands im Zeitpunkt der Lösegeldzahlung zumindest für möglich halten und billigend in Kauf nehmen, dass durch die Zahlung eine kriminelle Organisation unterstützt wird.[41] Ob dies der Fall ist, richtet sich nach den Umständen des Einzelfalls. Ob durch die Zahlung die Ziele der Organisation befürwortet werden oder der Erfolgseintritt an sich unerwünscht ist, ist für den Vorsatz nicht relevant.[42] Verkennt die Geschäftsleitung, dass die von der kriminellen Vereinigung begangenen oder geplanten Maßnahmen strafrechtlich relevant sind, oder hält sie entsprechende Verhaltensweisen mangels genauerer Kenntnis als von untergeordneter Bedeutung (vgl. § 129 Abs. 3 Nr. 2 StGB), handelt sie grundsätzlich (irrtumsbedingt) nicht vorsätzlich.[43]

Mit der Herausforderung für die Geschäftsleitung einerseits, in Ungewissheit über die Täter der Erpressung mit dem Cyber-Angriff konfrontiert zu sein, geht zugleich die Feststellung einher, dass der Nachweis eines festen, organisierten Zusammenschlusses von mindestens drei Personen mit gemeinsamem übergeordnetem Ziel als Täter der Erpressung in der Praxis oftmals nur schwierig zu führen sein wird. Geben sich die Täter nicht zu erkennen, wird häufig weder von der Geschäftsleitung noch von

38 Vgl. LK-StGB/Krauß StGB § 129 Rn. 123 m.w.N.; MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 112.

39 König NZWiSt 2023, 167 (168); LK-StGB/Krauß StGB § 129 Rn. 127.

40 Salomon MMR 2016, 575 (576); Rückert GWuR 2021, 103 (105); wohl auch Fuhlrott/Schröder NZA-RR, 2017, 625 (629).

41 So die h.M., vgl. nur BGH Urt. v. 3.10.1979 – 3 StR 264/79 = NJW 1980, 64; Brodowski/Schmid/Scholzen NStZ 2023, 385 (388);LK-StGB/Krauß StGB § 129 Rn. 147; König NZWiSt 2023, 167 (168 f.); Fischer StGB § 129 Rn. 48; Meyer/Biermann MMR 2022, 940 (943); jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; a.A. NK-StGB/Ostendorf StGB § 129 Rn. 25, der unter Verweis auf BGH bei Schmidt MDR 1991, 186 direkten Vorsatz fordert.

42 Salomon MMR 2016, 575 (576); Schönke/Schröder/Sternberg-Lieben/Schuster StGB § 15 Rn. 8.

43 Vgl. BGH Urt. v. 27.9.1956 – 6 StR 23/56 = LM Nr. 6 zu § 129 StGB; MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 123, 125;LK-StGB/Krauß StGB § 129 Rn. 147.

den Ermittlungsbehörden zu klären sein, ob sich hinter den (anonymen) Erpressern eine kriminelle oder terroristische Vereinigung verbirgt.[44] Auch wenn sich statistisch betrachtet eine Vielzahl solcher Vereinigungen aus der Erpressung von Lösegeldern im Zusammenhang mit Cyber-Angriffen finanziert,[45] kann hieraus nicht geschlossen werden, dass jeder anonyme Erpresser einer kriminellen oder terroristischen Vereinigung angehört, die von einer Lösegeldzahlung profitieren würde.[46] Dies gilt auch, wenn man versucht vorsätzliches Handeln von (hier nicht strafbaren) fahrlässigen Verhaltensweisen abzugrenzen, wenn unklar ist, wer hinter der Erpressung steht da sich der Eventualvorsatz auf eine konkrete Vereinigung beziehen muss. Es reicht also nicht aus, dass der Täter damit rechnet, dass er das Geld an eine „beliebige" kriminelle Vereinigung zahlt.[47] Bloße Vermutungen oder Spekulationen über eine konkrete Vereinigung reichen ebenfalls nicht aus.[48]

Dabei handelt es sich insgesamt um faktische Probleme der Beweisermittlung und des Tatnachweises durch Ermittlungsbehörden. Die Geschäftsleitung darf bei der Einschätzung, ob eine Zahlung strafrechtlich und gesellschaftsrechtlich zulässig ist, zwar berücksichtigen, ob für sie überhaupt Anhaltspunkte vorliegen, dass die Zahlung einen Straftatbestand erfüllen könnte. Ist dies der Fall, dürfen Erwägungen über eine faktische Verfolgung oder Nachweisschwierigkeiten durch die Ermittlungsbehörden bei der Entscheidung über eine Zahlung aber keine Rolle spielen.

2. Straflosigkeit durch Rechtfertigungsgründe?

Unabhängig von den tatsächlichen (Beweis-)Schwierigkeiten bei der Ermittlung der tatbestandlichen Voraussetzungen kann eine Lösegeldzahlung

44 So auch Rückert GWuR 2021, 103 (105); Hilgendorf/Kudlich/Valerius Handbuch des Strafrechts Bd. 6/Eisele § 63 Rn. 145; Nadeborn/Dittrich International Cybersecurity Law Review 3 (2022), 147 (157 f.).

45 Nach Salomon MMR 2016, 575 (576) sei es „bekannt, dass gerade auch Gruppierungen Erpressungstrojaner als Geschäftsmodell entdeckt haben".

46 So aber ohne tiefere Begründung Salomon MMR 2016, 575 (576). Für die Bejahung eines hinreichenden Tatverdachts müsste die Qualifikation als Vereinigung jedenfalls feststehen, da sonst eine Verurteilung gem. §§ 129, 129a StGB nicht möglich wäre, ohne gegen den *in dubio pro reo*-Grundsatz zu verstoßen. Zu dessen Anwendung auf tatbestandsbegründende Umstände vgl. nur KK-StPO/Ott StPO § 261 Rn. 6 m.w.N.

47 Rückert GWuR 2021, 103 (105).

48 Vgl. Rückert GWuR 2021, 103 (105).

wegen der besonderen Erpressungssituation gerechtfertigt sein. Dies wird vor dem Hintergrund der Notstandsregeln diskutiert.[49] Geht man davon aus, dass die Lösegeldzahlung den Tatbestand der §§ 129 ff. StGB erfüllt, läge ein sogenannter Nötigungsnotstand vor. Die Notstandslage ergibt sich aus der der Nötigung der Geschäftsleitung durch den Erpresser; die Geschäftsleitung würde durch Lösegeldzahlungen in die Rechtsgüter der inneren öffentlichen Sicherheit und staatlichen Ordnung einschließlich des öffentlichen Friedens[50] eingreifen, die von den §§ 129 ff. StGB geschützt werden.[51]

Bei einer unter Druck erfolgten Zahlung von Schutz- bzw. Lösegeld soll nach teilweise vertretener Auffassung ein rechtfertigender Notstand nach § 34 StGB regelmäßig ausscheiden.[52] Nach dieser Ansicht kann die Rechtsordnung keine Verhaltensweisen billigen, durch die sich der Notstandstäter zur Abwendung eines ihm angedrohten Übels zum Werkzeug eines rechtswidrig handelnden Dritten machen lässt[53] und insoweit selbst auf die Seite des Unrechts tritt.[54] Straffreiheit könne der Nötigungstäter allenfalls unter den Voraussetzungen des entschuldigenden Notstands nach § 35 StGB (analog) erlangen.[55] Dieses Verständnis dehnt ein mögliches Strafbarkeitsrisiko von Geschäftsleitern bei Ransomware-Angriffen zu weit aus, da in der Regel die für eine Entschuldigung nach § 35 StGB (analog) erforderliche Gefahr für Leben, Leib oder Freiheit[56] nicht vorliegen und ein Schuldausschluss damit in den meisten Fällen ausscheiden wird.[57] Häufig wird der zu erwartende Nachteil weder den Handelnden selbst noch eine von § 35 Abs. 1 StGB genannte Person treffen, weshalb zusätzlich ein

49 Vgl. allgemein Arzt/Weber/Heinrich/Hilgendorf Strafrecht BT/Hilgendorf § 44 Rn. 17 und § 10 Rn. 10; jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; SK-StGB/Stein/Greco StGB § 129 Rn. 53.

50 S. MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 1.

51 Vgl. Salomon MMR 2016, 575 (576) m.w.N.; Rückert GWuR 2021, 103 (106).

52 MünchKomm. StGB/Schäfer/Anstötz StGB § 129 StGB Rn. 126; Schönke/Schröder/Sternberg-Lieben/Schittenhelm StGB § 129 StGB Rn. 17; Fischer StGB § 129 Rn. 41; SSW-StGB/Lohse StGB § 129 Rn. 53.

53 Vgl. Schönke/Schröder/Perron StGB § 34 StGB Rn. 41b.

54 Ausführlich Schönke/Schröder/Perron StGB § 34 Rn. 41b; im Ergebnis auch Arzt JZ 2001, 1052 (1054 ff.).

55 MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 126; Schönke/Schröder/Perron StGB § 43 Rn. 41b; Fischer StGB § 129 Rn. 41.

56 Siehe hierzu MünchKomm. StGB/Müssig StGB § 35 Rn. 12 ff.

57 König NZWiSt 2023, 167 (169); Brodowski/Schmid/Scholzen NStZ 2023, 385 (388); Meyer/Biermann MMR 2022, 940 (942).

übergesetzlicher entschuldigender Notstand zu erwägen ist.[58] Etwas anderes wird man insbesondere bei Attacken auf kritische Infrastrukturen, wie Krankenhäuser, annehmen müssen, bei denen eine Gefahr für Leib und Leben in den Vordergrund tritt.[59] Auch ein Schuldausschluss nach § 17 StGB dürfte regelmäßig ausscheiden. Ransomware-Angriffe haben inzwischen keinen Seltenheitswert mehr.[60] Durch den Anstieg der Ransomware-Angriffe und der damit verbundenen Bedrohungslage für Unternehmen könnten Ermittlungsbehörden davon ausgehen, dass betroffene Geschäftsleitungen es jedenfalls für möglich halten werden, mit Lösegeldzahlungen eine kriminelle Vereinigung zu unterstützen und sich dem Risiko einer Strafbarkeit nach § 129 StGB auszusetzen.[61] In einem solchen Fall würde ein Verbotsirrtum nach § 17 StGB ausscheiden.[62] Durch die Möglichkeit, im Falle eines Ransomware-Angriffs Rechtsrat einzuholen, würde ein etwaiger Irrtum von Ermittlungsbehörden voraussichtlich zudem als vermeidbar angesehen sein und insoweit allenfalls eine Milderung nach § 17 S. 2 StGB in Betracht kommen.[63]

Überzeugender ist es deshalb im Fall von Lösegeldzahlungen die Regeln des rechtfertigenden Notstands gemäß § 34 StGB anzuwenden. Anders als der entschuldigende Notstand (gem. § 35 StGB) sieht der offenere Wortlaut des § 34 StGB keine Restriktionen hinsichtlich des Ursprungs der Gefahr vor. Auch beim Nötigungsnotstand verdient der unter dem Nötigungsdruck handelnde Täter die Solidarität der Rechtsordnung.[64] Der in Zwangslage handelnde (Nötigungs-)Täter tritt auch nicht freiwillig auf die Seite des Unrechts, sondern wird vom Erpresser auf diese Seite gedrängt[65]. Möglicherweise beeinträchtigte Interessen Dritter können im Rahmen der Interessenabwägung angemessen berücksichtigt werden.[66]. Die Anwendung von

58 Vgl. Salomon MMR 2016, 575 (577). Dazu Bechtel JuS 2021, 401 (401 ff.).
59 So Meyer/Biermann MMR 2022, 940 (942); wohl auch Salomon MMR 2016, 575 (576); Dittrich/Erdogan ZWH 2022, 13 (17).
60 BSI, Ransomware Bedrohungslage 2022, S. 4 f.
61 König NZWiSt 2023, 167 (169).
62 BGH, Beschl. v. 24.2.2011 – 5 StR 514/09 = NJW 2011, 1236 (1239); Fischer StGB, § 17 Rn. 2.
63 König NZWiSt 2023, 167 (169); vgl. Graf/Jäger/Wittig Wirtschafts- und Steuerstrafrecht/Sackreuther StGB § 17 Rn. 16 ff.
64 MünchKomm. StGB/Erb StGB § 34 Rn. 192 ff. m.w.N. zu beiden Ansichten. Zustimmend Salomon MMR 2016, 575 (577). Wohl auch jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165. Ausführlich auch Brand/Lenk JuS 2013, 883 (883 ff.).
65 Brand/Lenk JuS 2013, 883 (884).
66 MünchKomm. StGB/Erb StGB § 34 Rn. 194.

§ 34 StGB auf Fälle der durch einen Ransomware-Angriff hervorgerufenen Notstandshandlung, ermöglicht danach sachgerechte Ergebnisse im jeweiligen Einzelfall.[67]

Bei Zahlung eines Lösegeldes muss daher stets eine Interessenabwägung zwischen dem bedrohten Rechtsgut (hier des Erpressungsopfers) und dem Rechtsgut, in das durch die abgenötigte Straftat eingegriffen wird, erfolgen. Eine solche Abwägung wird regelmäßig zur Rechtfertigung der Zahlung führen[68], auch wenn in der Literatur teilweise ein deutliches Überwiegen der Interessen des Genötigten gefordert wird:[69]

Durch die Zahlung wird in keine Individualrechtsgüter, wie Leib, Leben oder persönliche Freiheit einer anderen Person, eingegriffen sodass auch keine problematischen Duldungspflichten auf Seiten anderer Individuen bestehen.[70] Es gibt hier kein konkretes Notstandsopfer, da die §§ 129 ff. StGB ausschließlich abstrakte Allgemeinrechtsgüter schützen, d.h. insbesondere die innere öffentliche Sicherheit und die staatliche Ordnung einschließlich des öffentlichen Friedens.[71] Die Schwere der durch die Lösegeldzahlung tatbestandlich verwirklichten Notstandstat ist abstrakt als sehr gering zu bewerten. Auch unter Berücksichtigung des jeweiligen Einzelfalls wird durch die Zahlung des Lösegelds die innere öffentliche Sicherheit und die staatliche Ordnung allenfalls gering konkret betroffen sein.[72]

Selbst wenn das angegriffene Unternehmen keine schwerwiegenden Rechtsgutsbeeinträchtigungen (wie z.B. die Gefährdung von Menschen) zu befürchten hat, werden im Rahmen der Interessenabwägung die Beeinträchtigung des Eigentums und der Berufsausübungsfreiheit regelmäßig überwiegen. Eine entsprechende Beeinträchtigung liegt bei einem Ransomware-Angriff regelmäßig vor, da die Erpresser regelmäßig den Zugriff auf die Unternehmensdaten verhindern und diese löschen oder veröffentlichen können.[73] Das Unternehmen hat ein Interesse an der Vermeidung

67 So auch König NZWiSt 2023, 167 (169).
68 So auch König NZWiSt 2023, 167 (169); Rückert GWuR 2021, 103 (106); Salomon MMR 2016, 575 (577); SK-StGB/Stein/Greco StGB § 129 Rn. 53, die offenlassen, ob Rechtfertigung oder Entschuldigung einschlägig ist.
69 So MünchKomm. StGB/Erb StGB § 34 Rn. 194; BeckOK StGB/Momsen/Savić StGB § 34 Rn. 17; Meyer/Biermann MMR 2022, 940 (942).
70 Vgl. Rückert GWuR 2021, 103 (106); Salomon MMR 2016, 575 (577).
71 Vgl. hierzu MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 1.
72 So auch Salomon MMR 2016, 575 (578); Rückert GWuR 2021, 103 (106).
73 Vgl. Salomon MMR 2016, 575 (577 f.); vgl. auch Brodowski/Schmid/Scholzen/Zoller NStZ 2023, 385 (388).

erheblicher wirtschaftlicher Schäden, der Wiedererlangung der häufig für den Geschäftsbetrieb unverzichtbaren Daten und der Vermeidung eines drohenden Reputationsverlusts. Auch kann die wirtschaftliche Existenz des Unternehmens durch den Ransomware-Angriff und der damit einhergehenden Folgen gefährdet sein. Dies (sowie die Cyber-Attacke selbst) haben auch Auswirkungen auf Beschäftigte die bspw. freigestellt werden müssen, solange kein Zugriff auf wichtige Daten besteht, da hierdurch die Funktionsfähigkeit des gesamten Unternehmens eingeschränkt sein kann. Bei Angriffen auf kritische Infrastrukturen, wie Krankenhäuser, treten weitere Rechtsgüter auf Seiten der Erpressten in die Abwägung ein (z.B. die Aufrechterhaltung der öffentlichen Gesundheitsvorsorge).[74]

Für ein Überwiegen der Interessen des angegriffenen Unternehmens spricht auch, dass die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Jahr 2017 eine Ransomware-Versicherung in Cyber-Versicherungspolicen genehmigt hat (siehe hierzu auch Rz. 34.151).[75] Der Genehmigung der BaFin kommt zwar keine rechtsverbindliche Wirkung zu, sie entfaltet jedoch eine starke Indizwirkung gegen eine Strafbarkeit von Lösegeldzahlungen nach deutschem Recht. Andernfalls hätte die BaFin eine solche Genehmigung voraussichtlich nicht erteilt. Es gebietet daher der Gedanke der Einheit der Rechtsordnung, die als rechtlich legitimen Versicherungsgegenstand anzusehende Lösegeldzahlung auch als strafrechtlich möglich/gerechtfertigt anzusehen. Dem stehen auch die Ausführungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und BKA zu Lösegeldzahlungen bei Ransomware-Angriffen nicht entgegen:[76] So führen BSI und BKA zwar aus, dass auf eine Erpressung nicht eingegangen und ein Lösegeld nicht bezahlt werden sollte. Zur Begründung weisen sie jedoch insbesondere darauf hin, dass eine Zahlung die Gefahr möglicher weiterer Angriffe berge und selbst bei Zahlung keine Garantie bestünde, dass der kriminelle „Verhandlungspartner" die Verschlüsselung nach der Lösegeld-

74 So auch insg. Rückert GWuR 2021, 103 (106).

75 BaFin Mitteilung vom 15. September 2017, abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html (zuletzt abgerufen am 6.1.2025).

76 Vgl. BSI, Erste Hilfe bei einem schweren IT-Sicherheitsvorfall, Arbeitspapier – Version 1.2 (7. Oktober 2022), S. 15; BKA, Ransomware – Unternehmen und Institutionen als Zielscheibe, S. 10 f.; auch im Bundeslagebild Cybercrime 2021 führt das BKA zu einer Strafbarkeit von Lösegeldzahlungen nicht aus, vgl. Bundeslagebild Cybercrime 2023, S. 25 f.; auf eine kleine Anfrage der AfD-Fraktion ist die Bundesregierung den Ausführungen von BSI und BKA nicht entgegengetreten, vgl. BT-Drs. 20/2926, S. 3.

zahlung tatsächlich aufhebe. Eine mögliche Strafbarkeit einer Lösegeldzahlung wird zur Begründung dagegen nicht herangezogen. Vielmehr weist das BKA ausdrücklich darauf hin, dass im Einzelfall eine Zahlung in Betracht gezogen werden kann, wenn das Unternehmen vor der Wahl steht, den Geschäftsbetrieb einzustellen oder Lösegeld zu zahlen.[77]

Um etwaige strafrechtliche Risiken weiter zu reduzieren, sollten frühzeitig (spätestens jedoch) bei Eingang einer konkreten Lösegeldforderung die Ermittlungsbehörden (und dort zunächst die zuständige Spezialstelle des Landeskriminalamtes) informiert und eine mögliche Lösegeldzahlung im Vorfeld mit den Ermittlungsbehörden (auch der zuständigen Staatsanwaltschaft) abgestimmt werden. Zusätzlich sollte in diesem Fall eine detaillierte Prüfung der hier skizzierten Risiken anhand des konkreten Einzelfalls stattfinden.

Die Möglichkeit einer Rechtfertigung der Lösegeldzahlung nach § 34 StGB unter Abwägung der widerstreitenden Interessen kommt auch für weitere Straftatbestände in Betracht. So schützen die Verbotstatbestände des § 18 Abs. 1 Nr. 1 und 2 AWG die abstrakten Rechtsgüter der Sicherheit der Bundesrepublik und des Völkerfriedens[78]. Erfolgt eine Lösegeldzahlung, muss diese im Unternehmen und der Buchhaltung korrekt und transparent dargestellt werden, so dass die oben angesprochenen Tatbestände der Urkundenfälschung (§ 267 StGB), Untreue (§ 266 StGB), Steuerhinterziehung (§ 370 AO) und unrichtiger Darstellung (§ 331 HGB) nicht drohen verwirklicht zu werden.

III. Sanktionsrisiken nach US-amerikanischem Recht (insbesondere „civil monetary penalties")

Sofern die vom Cyberangriff betroffene Gesellschaft Geschäfte mit einem Bezug zur US-Jurisdiktion betreibt, sind zudem erhebliche Risiken mit Blick auf die dortigen Sanktionsvorschriften zu beachten.[79] In seinen unverbindlichen Leitlinien aus September 2021 weist das *U.S. Department of the Treasury's Office of Foreign Assets Control* (*OFAC*) insofern darauf hin, dass sich Gesellschaften in zivilrechtlicher Hinsicht („*civil monetary*

77 Vgl. BKA, Ransomware – Unternehmen und Institutionen als Zielscheibe, S. 10.

78 Vgl. MünchKomm. StGB/Wagner AWG § 18 Rn. 11.

79 Rückert GWuR 2021, 103 (104); vgl. auch: *U.S. Department of the Treasury's Office of Foreign Assets Control* (OFAC), Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments v. 21.9.2021.

penalty") einer „*strict liability*", d.h. einer von der Bösgläubigkeit ihrer Geschäftsleiter unabhängigen Haftung, ausgesetzt sähen.

C. Gesellschaftsrechtliche Haftungsrisiken

I. Ransomware-Angriffe als Haftungsfall?

Sofern und soweit die Zahlung von Lösegeld im Falle eines Cyberangriffs nach der hier vertretenen Auffassung gerechtfertigt ist (und zudem kein Verstoß gegen EU- oder US-Sanktionsregelungen vorliegt), liegt eine unternehmerische Entscheidung vor. Die Geschäftsleitung hat dann eine Interessenabwägung vorzunehmen, bei der sämtliche der Geschäftsleitung bekannten Kriterien einzubeziehen sind. Nach den Grundsätzen der Business Judgement Rule hat die Geschäftsleitung allerdings das Unternehmenswohl stärker zu berücksichtigen als bei der Abwägung im Rahmen des § 34 StGB. Es ist im Einzelfall abzuwägen, ob die Zahlung eines Lösegeldes zum Wohle des Unternehmens das bessere Mittel darstellt oder ob es vorzugswürdig ist, zunächst abzuwarten und die Daten durch die eigene IT-Abteilung oder externe Experten wiederherstellen zu lassen bzw. dies zu versuchen.

Bei einem erfolgreichen Ransomware-Angriff wird spätestens bei der nachträglichen Aufarbeitung auch die Haftung des Vorstands wegen eines etwaigen Organisationsversagens zu prüfen sein, unabhängig davon, ob Lösegeld gezahlt wurde oder nicht. Denn die Risikovorsorge ist – auch in der Informationssicherheit – originäre Aufgabe des Managements. Der Vorstand muss daher ausreichende Schutzvorkehrungen zur Vermeidung eines erpresserischen Cyber-Angriffs treffen.[80] Wird dies in einem Organhaftungsprozess angezweifelt, bestehen für die an sich darlegungs- und beweisbelastete Gesellschaft nach der Rechtsprechung Beweiserleichterungen für den Nachweis eines kausalen Schadens. Für den Ursachenzusammenhang zwischen Zahlung einer Beraterleistung und Schaden hat etwa das LG München I in seiner „Siemens/Neubürger"-Entscheidung § 287 ZPO herangezogen.[81] Danach muss die Gesellschaft nur Tatsachen vortra-

80 Vgl. zu den denkbaren (präventiven) Maßnahmen Heinrichs/Neumeier CB 2022, 14 (17 f.). Zur drohenden gesellschaftsrechtlichen Haftung der Geschäftsleiter in diesem Kontext vgl. u.a. Mehrbrey/Schreibauer MMR 2016, 75 (79 f.); Daghles DB 2018, 2289; Grieger WM 2021, 8 (11 ff.); Schmidt-Versteyl NJW 2019, 1637 (1638 f.).

81 LG München I Urt. v. 10.12.2013 – 5 HK O 1387/10 = AG 2014, 33. Vgl. hierzu auch Scholz ZZP 133 (2020), 491 (506 f.).

gen und unter Beweis stellen, die für eine Beurteilung nach § 287 ZPO ausreichend greifbare Anhaltspunkte bieten. Das beklagte Organmitglied hat demgegenüber darzulegen und erforderlichenfalls zu beweisen, dass es seinen Sorgfaltspflichten nachgekommen ist oder es kein Verschulden trifft oder dass der Schaden auch bei pflichtgemäßem Alternativverhalten eingetreten wäre. Andere wollen die Regelungen über den Anscheinsbeweis anwenden.[82]

Nach einem erfolgten Cyberangriff sind in jedem Fall unverzüglich die erforderlichen Maßnahmen zu ergreifen, um das Schadensrisiko zu begrenzen sowie den Sachverhalt aufzuklären, mögliche Verstöße abzustellen und festgestelltes Fehlverhalten zu sanktionieren (Aufklärung, Abstellung, Ahndung). Dazu gehört auch, die IT-Systeme einer Prüfung zu unterziehen und Schwachstellen zu identifizieren und zu beseitigen. Darüber hinaus ist die bestehende IT-Compliance-Organisation und -Infrastruktur kritisch zu hinterfragen und auf Basis der gewonnenen Erkenntnisse und Erfahrungen weiterzuentwickeln.

II. Erweiterte Pflichten und Haftung nach der NIS-2-Richtlinie

Am 16. Januar 2023 ist die NIS-2-Richtlinie in Kraft getreten.[83] Sie erweitert den Anwendungsbereich der gesetzlichen Cybersicherheitspflichten, die bisher vor allem für Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste galten, auf weite Teile der Wirtschaft und verschärft das Sanktionsregime bei Verstößen erheblich. Die Mitgliedsstaaten der Europäischen Union (EU) hätten die NIS-2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen müssen. In Deutschland ist dies bislang nicht geschehen.

Durch die NIS-2-Richtlinie und die geplante nationale Umsetzung werden öffentliche und private Stellen zur Einhaltung eines hohen Cybersicherheitsniveaus verpflichtet. Dabei ist nicht nur der Anwendungsbereich der Regelungen deutlich weiter als bei der Vorgängerrichtlinie – viele Unternehmen werden erstmals von konkreten Cybersicherheitspflichten

82 KölnKomm. AktG/Cahn AktG § 93 Rn. 142.

83 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148.

betroffen sein. Die Regelungen gehen auch inhaltlich weiter, als dies bisher der Fall war.[84] Das Umsetzungsgesetz sieht insbesondere eine Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG) vor (folgend „BSIG-E").

§ 28 BSIG-E definiert die besonders wichtigen Einrichtungen und die Betreiber kritischer Anlagen, die in den Anwendungsbereich fallen. Neben dem Datenschutz gelten weitergehende Cybersicherheitsanforderungen bislang nur für bestimmte Unternehmen, insbesondere im Bereich kritischer Infrastrukturen und digitaler Dienste. Mit der NIS2-Richtlinie und dem BSIG-E wird die Liste der Sektoren, für die verbindliche Cybersicherheitspflichten gelten sollen, deutlich erweitert. Ausweislich der Gesetzesbegründung ist nunmehr davon auszugehen, dass ca. 8.250 Unternehmen als besonders wichtige und rund 21.600 Unternehmen als wichtige Einrichtungen klassifiziert werden.[85] Nach Angaben des BSI waren bisher nur ca. 1.100 kritische Infrastrukturen mit ca. 2.000 kritischen Anlagen von der KRITIS-Regulierung erfasst.[86]

Nach § 30 des BSIG-E müssen besonders wichtige und wichtige Einrichtungen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Betroffene Unternehmen müssen u.a. ein Risikomanagementsystem zum Schutz ihrer IT-Strukturen einrichten und dokumentieren und Sicherheitsvorfälle müssen innerhalb von 24 Stunden gemeldet werden (§ 32 BSIG-E).[87] Pflichtverstöße können Geldbußen von bis zu EUR 10 Mio oder 2 % des Jahresumsatzes nach sich ziehen (§ 65 BSIG-E). Die Geschäftsleitung trägt die Verantwortung für die Umsetzung und Überwachung dieser Maßnahmen und kann bei Pflichtverletzungen haftbar gemacht werden. Die Geschäftsleitungen besonders wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der

84 Schmidt RDi 2024, 550 (550) Rn 2.
85 BT-Drs. 20/13184, S. 102.
86 Vgl. Schmidt RDi 2024, 550 (551) Rn 4.
87 Dazu Kipker/Dittrich MMR 2023, 481 (483).

Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können (§ 38 BSIG-E).[88]

III. Absicherung durch Cyberversicherungen

Um das Risiko von Schäden nach einem Cyber-Angriff zu reduzieren, werden mittlerweile häufig, entsprechende Cyber-Versicherungen abgeschlossen, die auch die Zahlung von Lösegeld einschließen können.[89] Lösegeldversicherungen waren zwar früher verboten, wurden aber schon durch die Vorgängerbehörde der BaFin für zulässig erklärt[90] und dürfen nun auch gebündelt mit einer Cyber-Versicherung abgeschlossen werden, wobei die Lösegeldversicherung selbst nicht beworben werden darf.[91] Je nach Risikolage des Unternehmens, etwa bei Geschäftsfeldern, die oft ins Visier von Cyber-Attacken geraten, müssen Vorstand und Aufsichtsrat abwägen, ob der Abschluss einer solchen Versicherung im Interesse des Unternehmens liegt, was zumindest bei größeren Unternehmen der Fall sein dürfte.[92]

Um aufgrund der sicher erscheinenden Auszahlung keine zusätzlichen Anreize für Erpresser zu schaffen, müssen Cyber-Versicherungen nach den Versicherungsbedingungen geheim gehalten werden.[93] Aus diesem Grund stehen Versicherungen für Lösegeldzahlungen auch in der Kritik, da damit das Geschäftsmodell Cyber-Erpressung nicht „ausgetrocknet" wird, sondern weiter attraktiv bleibt.[94] Ein Verbot wurde von der Bundesregierung jedoch als nicht notwendig und nicht zielführend erachtet, da die

88 Kipker/Dittrich MMR 2023, 481 (485); Schmidt RDi 2024, 550 (554 f.) Rn. 22 ff.

89 Zur Möglichkeit der Versicherung Veith/Gräfe Der Versicherungsprozess/Gebert/Klapper § 24 Rn. 96; Fortmann r+s 2019, 429 (434 f.); Gabel/Heinrich/Kiefner Rechtshandbuch Cyber-Security/Wirth Kap. 12 Rn. 67 ff.; Wirth BB 2018, 200 (204); Prölss/Martin VVG/Klimke A1_17 A1–17 AVB Cyber Rn. 23; Notthoff r+s 2022, 61 (65); vgl. aber noch die Regelung A1–17.7 der AVB Cyber (Stand: April 2017), die inzwischen durch die Praxis überholt wurde.

90 Bundesaufsichtsamt für das Versicherungswesen (BAV): Rundschreiben 3/1998 (VA).

91 BaFin, BaFin Journal, September 2017, S. 4 f., abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html (zuletzt abgerufen am 6.1.2025).

92 Kiefner/Happ BB 2020, 2051 (2055); Daghles DB 2018, 2289 (2292).

93 BaFin, BaFin Journal, September 2017, S. 4 f.; vgl. dazu auch Fortmann r+s 2019, 429 (435).

94 Dittrich/Erdogan ZWH 2022, 13 (17); Stellungnahme der Gesellschaft für Informatik et al. aus Juni 2022, abrufbar unter: https://gi.de/offener-brief-zu-loesegeldzahlu

Unternehmen auch ohne Versicherung nicht davon abgehalten würden, ein Lösegeld (selbst) zu zahlen.[95]

ngen-bei-ransomware-angriffen-ein-geostrategisches-risiko (zuletzt abgerufen am 6.1.2025).

95 BT-Drs. 20/2926, S. 6.