Handelsgericht des Kantons Zürich

Geschäfts-Nr.: HG210017-O U/dz

Mitwirkend: Oberrichterin Dr. Claudia Bühler, Präsidentin, und Oberrichter Dr. Daniel Schwander, die Handelsrichterin Dr. Petra Ginter, die Handelsrichter Marco La Bella und Dr. Alexander Müller sowie der Gerichtsschreiber Dr. Giulio Donati

Urteil vom 9. März 2023

in Sachen

A1._____ Ltd.,
Klägerin

vertreten durch Rechtsanwalt lic. iur. X1._____,
vertreten durch Advokat Prof. Dr. iur. X2._____,

gegen

B._____ Limited,
Beklagte

vertreten durch Rechtsanwalt Dr. iur. Y1._____,
vertreten durch Rechtsanwalt lic. iur. Y2._____,

betreffend **Forderung**

Rechtsbegehren:
(act. 1 S. 2)

"1. Es seien die Beklagten zu verpflichten, der Klägerin den Betrag von … [Teil des Schadens] zzgl. Zinsen von 5 % seit dem tt.mm.Tatjahr+1 zu bezahlen;

2. unter Kosten- und Entschädigungsfolgen, zuzüglich Mehrwertsteuer, zu Lasten der Beklagten."

Inhaltsverzeichnis

Sachverhalt und Verfahren

A. Sachverhaltsübersicht

a. Parteien und ihre Stellung

Die Klägerin ist eine … Aktiengesellschaft [eines europäischen Staates] mit Sitz in C._____. Sie ist die börsenkotierte Holdinggesellschaft der A._____. Die Gruppe beschäftigt ca. … Personen weltweit. Unter der Marke A1._____ werden … [Zweck] (act. 1 Rz. 12 ff.).

Die Beklagte ist eine in E._____ [Staat in Europa] registrierte Versicherungsgesellschaft mit Sitz in F._____, die das Versicherungsgeschäft hauptsächlich in F._____, G._____, H._____ und I._____ aktiv betreibt. Seit 2018 wird die Beklagte zu 100% von der *J._____ Group, Inc.* ("*J._____ Inc.*"), einer nach U.S.-amerikanischem Recht organisierte Gesellschaft, indirekt gehalten und kontrolliert (act. 1 Rz. 23 f.).

b. Prozessgegenstand

Am tt.mm.Tatjahr wurde die Klägerin Opfer einer Cyber-Erpressung unter Verwendung der Ransomware *K._____*. Diese Schadsoftware verschlüsselte Dateien (unter anderem auch Kundendaten) auf den Systemen der Klägerin. Die Dateien konnten nicht mehr gelesen werden. Die Klägerin sah sich gezwungen, den Betrieb ihrer Callcenter, Webseiten und einiger Online-Dienste, darunter *A2._____* und *A3._____*, einzustellen (vgl. act. 1 Rz. 44; act. 17 Rz. 20). Ein Dechiffriercode, um die verschlüsselten Dateien wieder verwenden zu können, wurde von den Angreifern erst nach Zahlung eines Lösegelds in Höhe von … [hohe Summe] in Aussicht gestellt (act. 1 Rz. 42 ff.). Die Klägerin beauftragte das U.S. Cybersicherheitsunternehmen *N._____ LLC (N._____)*, das Lösegeld in Bitcoins zu bezahlen (vgl. act. 28 Rz. 99). Im Verlaufe des tt.mm.Tatjahr waren die Systeme der Klägerin wieder operabel (vgl. act. 28 Rz. 71). Aus dem Angriff erwuchs der Klägerin ein Schaden von circa … [grosser Schaden]. Die Klägerin war gegen derartige Cyberangriffe versichert, wobei die Beklagte Mitversicherin der einschlägigen Police war. Die Klägerin fordert mit der vorliegenden Klage von der Beklagten den entsprechenden Anteil der Beklagten an der Versicherungssumme. Die Beklagte

verweigert als einziges der beteiligten Versicherungsunternehmen die Zahlung und beruft sich auf eine in der Police vereinbarte Sanktionsklausel (act. 1 Rz. 59, Rz. 105 f., act. 17 Rz. 31, Rz. 177). Gemäss der Sanktionsklausel wird das Versicherungsunternehmen von seiner Zahlungspflicht befreit, wenn die Zahlung der Versicherungssumme gegen das Sanktionsrecht unter anderem der USA verstösst. Laut der Beklagten würde sie U.S.-Sanktionsrecht verletzen, wenn sie der Klägerin die Versicherungsleistung auszahlen würde.

B. Prozessverlauf

Am 25. Januar 2021 (Datum Poststempel) reichte die Klägerin ihre Klage mit dem oben aufgeführten Rechtsbegehren beim Handelsgericht des Kantons Zürich ein und beantragte mit gleicher Eingabe die Anordnung superprovisorischer Massnahmen sowie den Ausschluss der Öffentlichkeit vom vorliegenden Verfahren (act. 1; act. 3/1–27). Mit Verfügung vom 29. Januar 2021 wurde auf das klägerische Gesuch um Erlass (super-)provisorischer Massnahmen nicht eingetreten und der Antrag betreffend Ausschluss der Öffentlichkeit abgewiesen. Gleichzeitig wurde der Klägerin Frist angesetzt, um sich zur (Person/) Parteibezeichnung der Beklagten und deren allfälligen Vertretung zu äussern sowie um einen Kostenvorschuss zu leisten (act. 4). Mit Eingabe vom 19. Februar 2021 äusserte sich die Klägerin unter anderem zur Parteibezeichnung und präzisierte diese (vgl. act. 7). Mit Verfügung vom 10. März 2021 wurde der Beklagten, nach Eingang des klägerischen Kostenvorschusses (act. 9), Frist zur Einreichung ihrer Klageantwort angesetzt, sowie das Rubrum betreffend die Bezeichnung der Beklagten berichtigt (act. 11). Mit Eingabe vom 28. Juni 2021 erstattete die Beklagte innert erstreckter Frist (vgl. act. 13) ihre Klageantwort (act. 17; act. 18/1–33). Am 29. September 2021 fand am hiesigen Gericht unter der Leitung von Oberrichter Dr. Daniel Schwander als Instruktionsrichter eine Vergleichsverhandlung statt, anlässlich welcher die Parteien keine Einigung erzielen konnten. Das Verfahren wurde auf beidseitiges Ersuchen informell bis Ende Oktober 2021 sistiert (Prot. S. 7 f.). Nach deren Ablauf wurde mit Verfügung vom 3. November 2021 wurde ein zweiter Schriftenwechsel angeordnet (act. 23). Die Klägerin reichte ihre Replik am 21. Februar 2022 (Datum Poststempel) innert einmalig erstreckter Frist (act. 25) ein (act. 28; act. 29/1–27). Darin stellte sie neu einen Eventualantrag für den Fall

der Klageabweisung mangels Fälligkeit der geforderten Versicherungsleistung (act. 28 S. 9). Die Beklagte reichte ihre Duplik mit Eingabe vom 10. Mai 2022 ein (Datum Poststempel; act. 32 und act. 33/34–42). Mit Verfügung vom 16. Mai 2022 wurde die Duplik der Klägerin zugestellt und der Aktenschluss verfügt (act. 34). Die Klägerin ersuchte mit Eingabe vom 23. Mai 2022 (Datum Poststempel) um Ansetzung einer Frist bis 14. Juni 2022, um ihr unbedingtes Replikrecht auszuüben, was bewilligt wurde (vgl. act. 36). Mit Eingabe vom 14. Juni 2022 (Datum Poststempel) reichte die Klägerin ihre Stellungnahme zur Duplik ein (act. 38; act. 39/1–2). Die Beklagte ersuchte am 22. Juni 2022 schriftlich um Ansetzung einer Frist bis 11. Juli 2022, um zur klägerischen Eingabe vom 14. Juni 2022 Stellung zu nehmen, was bewilligt wurde (act. 41). Noch vor Eingang der Stellungnahme der Beklagten beantragte die Klägerin, ihr seien in den Gerichtsferien keine fristauslösenden Zustellungen zuzustellen. Das hiesige Gericht bewilligte den klägerischen Antrag bis 5. September 2022 mit dem Hinweis, danach würden keine Fristansetzungen mehr erfolgen (vgl. act. 43). Mit Eingabe vom 11. Juli 2022 (Datum Poststempel) reichte die Beklagte ihre Stellungnahme zur klägerischen Eingabe vom 14. Juni 2022 hierorts ein (act. 44; act. 45/43–45). Die Klägerin nahm zu dieser Eingabe der Beklagten ihrerseits mit Eingabe vom 2. September 2022 (Datum Poststempel) Stellung (act. 48; act. 49/1–4). Die Beklagte ersuchte am 14. September 2022 (Datum Poststempel) schriftlich um Fristansetzung bis 12. Oktober 2022 zur Stellungnahme. Der Antrag der Beklagten auf Fristansetzung wurde am 15. September 2022 abgewiesen (act. 43), mit dem Hinweis, dass vor Ablauf von 20 Tagen keine weiteren Verfahrensschritte erfolgen würden (vgl. act. 50). Die Beklagte reichte ihre Stellungnahme zur klägerischen Eingabe vom 2. September 2022 am 30. September 2022 (Datum Poststempel) ein (act. 52; 54/46–47). Die Klägerin reagierte auf die Eingabe der Beklagten mit Eingabe vom 14. Oktober 2022 (Datum Poststempel; act. 56; act. 57/1–2). Die Beklagte teilte am 31. Oktober 2022 mit, sie verzichte auf eine erneute Stellungnahme (act. 59). Mit Verfügung vom 7. Februar 2023 wurde den Parteien Gelegenheit eingeräumt, um auf die Durchführung einer Hauptverhandlung zu verzichten (act. 60). Die Klägerin verzichtete mit Schreiben vom 10. Februar 2023 auf die Durchführung der Hauptverhandlung. Sie reichte zudem mit gleichem Schreiben eine Noveneingabe ein, welche der Beklagten zugestellt wurde (vgl. act. 62; act. 63/1A–B; Prot.

S. 19). Die Beklagte teilte mit Schreiben 15. Februar 2023 (Datum Poststempel) mit, dass sie auf die Durchführung der Hauptverhandlung verzichte. Sie zeigte zudem an, dass sie betreffend die klägerische Noveneingabe vom 10. Februar 2023 das unbedingte Replikrecht wahrnehmen werde (vgl. act. 64). Mit Eingabe vom 23. Februar 2023 reichte die Beklagte in Wahrnehmung des unbedingten Replikrechts ihre angekündigte Stellungnahme sowie eine neue Vollmacht ein (vgl. act. 65 und act. 66). Der Prozess ist spruchreif (Art. 236 Abs. 1 ZPO).

Erwägungen

1. Zuständigkeit und anwendbares Recht

1.1. Örtliche und sachliche Zuständigkeit

1.1.1. Die Klägerin hat ihren Sitz in … [Staat in Europa], die Beklagte in … [Staat in Europa]. Es liegt demnach ein internationaler Sachverhalt vor. Die Klägerin beruft sich auf eine Gerichtsstandsvereinbarung in der Police, welche die Gerichte des Kantons Zürich als zuständig erklärt (vgl. act. 1 Rz. 34; act. 18/1 S 25 Ziffer 8 der Versicherungspolice). Es liegt eine gültige Gerichtsstandsklausel im Sinne von Art. 23 Abs. 1 LugÜ vor, was auch von der Beklagten nicht infrage gestellt wird (act. 17 Rz. 6).

1.1.2. Die sachliche Zuständigkeit des Handelsgerichts des Kantons Zürich ist gestützt auf Art. 6 Abs. 2 ZPO i.V.m § 44 lit. b GOG gegeben.

1.2. Anwendbares Recht

Die Parteien haben gültig Schweizer Recht für anwendbar erklärt (vgl. act. 1 Rz. 30; act. 17 Rz. 5).

2. Unbestrittener Sachverhalt

2.1. Unbestritten ist, dass die Klägerin und die Beklagte eine Versicherungspolice abschlossen. Fest steht sodann, dass die Klägerin am tt.mm.Tatjahr unter Verwendung der Ransomware *K._____* angegriffen und anschliessend erpresst wurde. Unbestritten ist weiter, dass die Klägerin gegen derartige Cyberangriffe versichert war, und dass jedes an der Police beteiligte Versicherungsunterneh-

men gemeinsam mit den anderen Versicherungsunternehmen, aber nicht solidarisch für seinen gezeichneten Anteil leistungspflichtig ist (act. 1 Rz. 87; act. 17 Rz. 250). Für beide Parteien steht fest, dass der Cyberangriff und der daraus entstandene Schaden grundsätzlich unter die Versicherungspolice fällt und einen versicherten Schadensfall darstellt, wenn keine Ausnahmeklausel greift (vgl. act. 17 Rz. 26, Rz. 31, Rz. 177). Total erlitt die Klägerin unbestrittenermassen einen Schaden in Höhe von … [grosser Schaden] (bestehend aus Lösegeldzahlung, Kosten im Zusammenhang mit forensischen Dienstleistungen sowie Kosten aus dem Erwerb eines Entschlüsselungsprogrammes). Der klägerische Selbstbehalt unter dem Versicherungsvertrag betrug … [ca. 1/3 des Schadens], womit der versicherte Schaden noch … [ca. 2/3 des Schadens] betrug (act. 1 Rz. 83, Rz. 130 f.). Der Anteil der Beklagten daran beträgt … [ca. 10 % des versicherten Schadens] (act. 1 Rz. 130; in act. 1 Rz. 131 geht die Klägerin von einem Anteil von … aus; es handelt sich dabei um einen Rechenfehler der Klägerin).

2.2. Unstrittig ist sodann, dass die von der Beklagten für den Angriff verantwortlich gemachte … *cybercrime*-Gruppe [aus dem Staat O._____] *P._____* (auch *Q._____* genannt) vom *Office of Foreign Assets Control* (OFAC) des U.S.-Finanzministeriums sanktioniert und auf die SDN-Liste (SDN = *Specially Designated Nationals And Blocked Persons List*) gesetzt wurde.

2.3. Unbestritten ist schliesslich, dass die vereinbarte Sanktionsklausel wie folgt lautet (vgl. act. 18/1 S. 60):

"SANCTION LIMITATION AND EXCLUSION CLAUSE

> No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America."

3. Parteivorbringen

3.1. Die Klägerin bringt vor, die Beklagte habe auf die Einrede der Sanktionsklausel verzichtet (act. 1 Rz. 121). Sollte kein Einredeverzicht vorliegen, so müsse

die in den Allgemeinen Versicherungsbedingungen enthaltene Sanktionsklausel in Anwendung der Ungewöhnlichkeitsregel als ungewöhnlich qualifiziert werden, womit sie nicht Vertragsbestandteil geworden sei. Wenn die Sanktionsklausel nicht ungewöhnlich sei, so sei sie unklar. Die Auslegung ergebe, dass niemals die Übernahme von U.S.-Cyber-Sanktionsrecht beabsichtigt gewesen sei, zumindest nicht in dem Ausmass, wie es die Beklagte behaupte. Komme gleichwohl U.S.-Cyber-Sanktionsrecht zur Anwendung, so falle eine Bestrafung der Beklagten durch das OFAC ausser Betracht, weil keine rechtliche Grundlage bestehe. Schliesslich sei nicht schlüssig nachgewiesen, dass eine Verbindung zwischen der sanktionierten *P.*_____ und dem Cyber-Angriff auf die Klägerin bestehe. Da keine Zahlung an eine SDN erfolgt sei, könne gar keine Verletzung des U.S.-Sanktionsrechts vorliegen.

3.2. Die Beklagte führt aus, ein Einredeverzicht, der auch die Beklagte binde, liege nicht vor (act. 17 Rz. 38). Die Sanktionsklausel sei sodann weder ungewöhnlich noch unklar. Das anwendbare U.S.-Cyber-Sanktionsrecht habe zur Folge, dass die Beklagte dieses verletzen würde, wenn sie die Versicherungsleistung auszahlen würde. Eine Verbindung zwischen der eingesetzten Ransomware *K.*_____ und der von der OFAC sanktionierten *P.*_____ könne zudem nicht ausgeschlossen werden, wobei ein erhebliches Risiko einer Verbindung genüge, damit die vereinbarte Sanktionsklausel greife (act. 17 Rz. 31, Rz. 45, Rz. 49).

4. Einredeverzicht der Beklagten

4.1. Parteivorbringen

4.1.1. Die Klägerin macht geltend, es liege ein Einredeverzicht vor, der auch die Beklagte binde. Es liege zwischen den an der Police beteiligten Versicherungsunternehmen ein Mitversicherungsverhältnis vor. Im Mitversicherungsverhältnis würde jeweils eine Versicherung (oder ein Versicherungskonsortium) in einem sogenannten Führungsvertrag als *Lead* vereinbart. Der *Lead*-Versicherer sei zuständig für die eingehenden Schadensmeldungen. Ihm obliege es auch, auf Einreden zu verzichten, wobei ein solcher Verzicht auch die anderen Mitversicherer

binde (Folgepflicht der Mitversicherer). Vorliegend sei als *Lead* das *R.*_____-Konsortium eingesetzt worden, unterstützt von der Kanzlei *S.*_____. Diese hätten mit Schreiben vom tt.mm.Tatjahr und vom tt.mm.Tatjahr die Versicherungsdeckung anerkannt und damit auch auf die Einrede der Sanktionsklausel namens sämtlicher Mitversicherer – und damit insbesondere auch namens der Beklagten – verzichtet (vgl. act. 1 Rz. 118, Rz. 124).

4.1.2. Die Beklagte anerkennt, dass *R.*_____ als *Slip Leader* fungierte und die Beklagte *Follower* war (act. 17 Rz. 269). Sie bringt vor, sie habe ihre Einwendungen schon frühzeitig der Klägerin dargelegt, und verweist auf eine E-Mail vom tt.mm.Tatjahr, die sie an die *T.*_____ *Ltd.* als *Coverholder* sowie in Kopie an den Broker der Klägerin (*U.*_____ *Limited*) gesandt habe. Darin habe sie erklärt, sie könne ihren Anteil an der Versicherungsleistung nicht bezahlen, bevor die Angelegenheit mit dem OFAC geklärt sei (act. 17 Rz. 41, Rz. 292 und act. 18/4). Ausserdem würden die von der Klägerin angerufenen Schreiben vom tt.mm.Tatjahr und vom tt.mm.Tatjahr keinen Einredeverzicht darstellen, weil in den Schreiben jeweils ein klarer Vorbehalt enthalten sei, wonach allfällige Vertragseinreden vorbehalten blieben (act. 17 Rz. 293; act. 32 Rz. 167 f.).

4.2. Würdigung

4.2.1. Aus beiden von der Klägerin zum Beweis offerierten Schreiben geht hervor, dass allfällige Vertragseinreden vorbehalten bleiben würden. So wird im Schreiben vom tt.mm.Tatjahr auf Seite 9 ausdrücklich die Sanktionsklausel erwähnt und diese im vollständigen Wortlaut wiedergegeben. Auf Seite 10 wird festgehalten, die Klägerin sowie ihre Vertreter seien zum Schluss gelangt, dass die Zahlung der Versicherungssumme keinem Verbot seitens des OFAC unterliege. Gestützt auf diese Informationen der Klägerin seien die Versicherungsunternehmen bereit, die Versicherungssumme auszuzahlen. Jedoch würde unter anderem die Sanktionsklausel vorbehalten, solange nicht abschliessend feststehe, dass keine Verletzung von U.S.-Sanktionsrecht vorliege. Festgehalten wird schliesslich auch, dass die Versicherungsunternehmen es zwar für unwahrscheinlich hielten, dass die Zahlung der Versicherungssumme gegen U.S.-Sanktionsrecht verstossen würde; man behalte sich aber für diesen Fall einen Rückforderungsanspruch für bereits ausgerichtete Zahlungen vor (vgl. act. 3/9 S. 9 f.). Im Schreiben vom

tt.mm.Tatjahr ist eine nahezu identische Passage enthalten (vgl. act. 3/15 S. 3 f.). Aus beiden Schreiben geht demnach gerade *kein Einredeverzicht der Beklagten* hervor. Das Schreiben vom tt.mm.Tatjahr kann zudem ohnehin keinen Einredeverzicht der Beklagten darstellen: Dieses erfolgt einzig im Namen der Konsortien R._____, *V.*_____ und *W.*_____ (letztere zwei als Teil von *T.*_____, vgl. act. 3/15 S. 1). Aus der Police ist ersichtlich, dass damit nicht die Beklagte gemeint ist. Die Beklagte wird betreffend den hier streitgegenständlichen non-EEA-Risiken (EEA bedeutet *European Economic Area*) in der Police als *AA.*_____ geführt (vgl. act. 18/1 S. 13 von 84). Das Schreiben vom tt.mm.Tatjahr erfolgte nicht im Namen der Beklagten.

4.3. Fazit

Die Klägerin kann mit den zum Beweis offerierten Schreiben vom tt.mm.Tatjahr und vom tt.mm.Tatjahr keinen Einredeverzicht der Beklagten nachweisen. Vielmehr war die Frage, ob die Zahlung der Versicherungssumme konform mit dem U.S.-Sanktionsrecht sei, noch nicht abschliessend geklärt, und die entsprechende Einrede der Sanktionsklausel wurde ausdrücklich vorbehalten.

5. Ungewöhnlichkeit der Sanktionsklausel

5.1. Parteivorbringen

5.1.1. Die Klägerin behauptet, sie habe die AVB (Allgemeine Versicherungsbedingungen) zur Police global übernommen (act. 28 Rz. 41). Die Sanktionsklausel sei derart ungewöhnlich, dass ihr gestützt auf die Rechtsprechung zum AGB-Recht jede Wirksamkeit zu versagen sei. Beide Verfahrensparteien hätten ihren Sitz in Europa und es habe für die Klägerin als … Gesellschaft [eines europäischen Staates] kein erkennbarer Bezug zu den USA bestanden. Keine Vertragspartei müsse mit einer Klausel rechnen, die derart weitreichend auf U.S.-Sanktionsrecht verweise (vgl. act. 28 Rz. 34 ff.).

5.1.2. Die Beklagte bestreitet eine Ungewöhnlichkeit der Sanktionsklausel im Sinne der AGB-Rechtsprechung. Derartige Klausel seien im Versicherungsvertragsrecht vielmehr üblich (vgl. act. 32 Rz. 149 ff.).

5.2. Rechtliches

5.2.1. Da die Parteien schweizerisches Recht für anwendbar erklärten, beantwortet sich die Frage nach der Geltung der Sanktionsklausel anhand der schweizerischen Rechtsprechung zum AGB-Recht.

5.2.2. Die Geltung vorformulierter allgemeiner Geschäftsbedingungen wird gemäss der Rechtsprechung durch die Ungewöhnlichkeitsregel eingeschränkt. Danach sind von der global erklärten Zustimmung zu allgemeinen Vertragsbedingungen alle ungewöhnlichen Klauseln ausgenommen, auf deren Vorhandensein die schwächere oder weniger geschäftserfahrene Partei nicht gesondert aufmerksam gemacht worden ist. Der Verfasser von allgemeinen Geschäftsbedingungen muss nach dem Vertrauensgrundsatz davon ausgehen, dass ein unerfahrener Vertragspartner ungewöhnlichen Klauseln nicht zustimmt. Die Ungewöhnlichkeit beurteilt sich aus der Sicht des Zustimmenden im Zeitpunkt des Vertragsabschlusses. Für einen Branchenfremden können deshalb auch branchenübliche Klauseln ungewöhnlich sein. Die Ungewöhnlichkeitsregel kommt jedoch nur dann zur Anwendung, wenn neben der subjektiven Voraussetzung des Fehlens von Branchenerfahrung die betreffende Klausel objektiv beurteilt einen geschäftsfremden Inhalt aufweist. Dies ist dann zu bejahen, wenn sie zu einer wesentlichen Änderung des Vertragscharakters führt oder in erheblichem Masse aus dem gesetzlichen Rahmen des Vertragstypus fällt (vgl. BGE 138 III 411, E. 3.1; PERRIG, Roman, in: Kramer/Probst/Perrig (Hrsg.), Schweizerisches Recht der Allgemeinen Geschäftsbedingungen, Bern 2016 N 173 ff.). Bei Versicherungsverträgen sind die berechtigten Deckungserwartungen zu berücksichtigen. Entsprechend wurde eine in allgemeinen Versicherungsbedingungen vorgesehene Haftungsbeschränkung als ungewöhnlich qualifiziert, welche die von der Bezeichnung des Vertrages erfasste Deckung erheblich reduzierte, so dass gerade die häufigsten Risiken nicht mehr gedeckt waren (vgl. BGE 138 III 411, E. 3.1).

5.3. Würdigung

5.3.1. Unstreitig sind die vereinbarten Versicherungsbedingungen als AVB zu qualifizieren.

5.3.2. Die Klägerin muss sich auch bei einer Globalübernahme das fachspezifische Wissen ihres Brokers anrechnen lassen. Dies gilt nicht nur für Sachverhaltsfragen, sondern auch für versicherungsrechtliches Know-how, welches beim Broker vorhanden ist (GRABER, Christoph, Diener zweier Herren? – Zur Rolle des Versicherungsbrokers, in: Luterbacher [Hrsg.], Versicherungen und Broker, Tagungsband 2014, Band 10, Zürich 2015, 1 ff., S. 12). Sofern ein Versicherungsnehmer beim Abschluss des Versicherungsvertrages durch einen Broker beraten oder gar vertreten wird, ist davon auszugehen, dass der Versicherungsnehmer durch die fragliche Versicherungsbestimmung nicht überrascht worden ist, sondern den Vertrag im Wissen um die fragliche Klausel abgeschlossen hat. Dies, weil nicht davon auszugehen ist, dass der Versicherungsbroker den Wortlaut der Police, welchen er seiner Kundin empfiehlt und dieser erläutern muss, selber nicht genau kennt (vgl. Urteil und Beschluss des Handelsgericht HG160125-O vom 19. September 2018, E. 2.9.2 S. 48; GRABER, Christoph, a.a.O., S. 14). Die Klägerin war bei den Vertragsverhandlungen durch ihren Broker *U.*_____ vertreten, dessen professionelles Wissen sie sich anrechnen lassen muss. Aus dem von der Klägerin eingereichten Vertragsdokument ergibt sich auch, dass *U.*_____ die Klägerin ausdrücklich aufforderte, die Vertragsklausel zu lesen, und sich die Klägerin sofort melden solle, falls einzelne Klauseln nicht ihrem Willen entsprechen würden (vgl. act. 3/3 S. 1: "*We* (Anmerkung: gemeint ist der Broker) *thank you for your* (Anmerkung: gemeint ist die Klägerin) *instructions and confirm that we have placed this Insurance on your behalf as detailed below. Please check the details and advise us immediately should they not conform to your request.*", und auch S. 10: "*Please examine this Broker Insurance Document carefully to confirm that cover has been arranged in accordance with your requirements and that the Insurers are acceptable: please advise us immediately if this is not the case. This document is not your contract of Insurance, but is evidence of the terms and conditions of the contract.*"). Da davon auszugehen ist, dass *U.*_____ die AVB kannte und deren Funktionsweise, insbesondere auch die Relevanz der Sanktionsklausel, verstand, fehlt es an der *subjektiven* Ungewöhnlichkeit (vgl. für einen ähnlich gelagerten Sachverhalt auch Urteil und Beschluss des Handelsgericht

HG160125-O vom 19. September 2018, E. 2.9.2 S. 48, wo aufgrund des fachspezifischen Wissens des Brokers bereits eine Globalübernahme verneint wurde).

5.3.3. Ohnehin erscheint die Sanktionsklausel objektiv nicht als ungewöhnlich. Die Klausel führt weder zu einer wesentlichen Änderung des Vertragscharakters noch fällt der Versicherungsvertrag wegen der Klausel in erheblichem Masse aus dem gesetzlichen Rahmen des Vertragstypus. Die Klausel ist nicht objektiv geschäftsfremd, zumal es vorliegend um die *non-EEA-Risiken* geht und es somit nicht überraschend ist, dass bei *non-EEA-Risiken* U.S. Recht relevant sein kann (wie es sich betreffend *EEA-Risiken* verhält, kann demgegenüber offen bleiben). Die Klausel muss vielmehr als üblich betrachtet werden, insbesondere bei Versicherungen, die Risiken betreffen, die eine Vielzahl von Rechtsordnungen berühren können (vgl. auch VISCHER, Frank/WIDMER LÜCHINGER, Corinne, in: Zürcher Kommentar zum IPRG, Band I: Art. 1–108, 3. Aufl., Zürich/Basel/Genf 2018, N 40 zu Art. 19, welche die *Sanctions Limitation Clause* ausdrücklich erwähnen; siehe auch MANKOWSKI, Peter, in: IPRax 2016, Heft 5, S. 485 ff., S. 492, der festhält, auf dem F._____er Versicherungsmarkt habe sich die Sanktionsklausel eingebürgert). Wie die Beklagte zu Recht hervorhebt, bezeichnet auch der klägerische Rechtsgutachter die Sanktionsklausel als typisch für die streitgegenständliche Police (vgl. act. 32 Rz. 195 mit Verweis auf act. 29/17 [recte: 29/16]: "[…] *the relevant clause is very typical of such policies*"). Wer am F._____er Versicherungsmarkt seine Versicherung abschliesst, muss damit rechnen, dass dort übliche Vertragsklauseln anwendbar sind. Ohne derartige Klauseln wäre es im Ergebnis äussert schwierig, einen weltweiten Versicherungsschutz anzubieten, weil sich die Versicherungsunternehmen einem kaum voraussehbaren Risiko des Rechtsbruchs aussetzen würden. Abschliessend fehlt es somit auch an der objektiven Ungewöhnlichkeit als weitere Voraussetzung der Ungewöhnlichkeitsregel.

5.4. Fazit

Zusammenfassend kann sich die Klägerin nicht auf die Ungewöhnlichkeitsregel berufen, weil die Sanktionsklausel weder subjektiv noch objektiv ungewöhnlich ist. Die Klausel wurde somit gültig vereinbart.

6. Auslegung der Sanktionsklausel

6.1. Parteivorbringen

6.1.1. Die Klägerin hält dafür, dass die durch einen Versicherer ausgerichtete Entschädigung für ein bereits durch die Versicherungsnehmerin an eine inkriminierte Einheit aus eigener Kasse ausbezahltes Lösegeld gar nicht in den Anwendungsbereich der Sanktionsklausel falle. Potentiell erfasst von OFAC-Massnahmen seien die nicht direkt mit einer Erpressungsdrohung konfrontierten Dienstleister nur dann, wenn sie in die Transaktion der eigentlichen Erpressungszahlung direkt involviert seien (act. 1 Rz. 109 und Rz. 111). Auf die Frage der möglichen Sanktionierung der Beklagten als *non-U.S.-Person*, die über eine U.S.-amerikanische Gesellschaft indirekt gehalten werde, gehe aus den Gutachten eine klare und begründete negative Antwort hervor. Die Sanktionsklausel erfasse den indirekten Fall einer Sanktionierung nicht. Selbst wenn wider Erwarten und entgegen dem klaren Nachweis durch die Klägerin die Meinung vertreten werde, die Beklagte als *non-U.S.-Person* könnte infolge der behaupteten Verbindungen zu einer U.S.-Konzerngesellschaft in irgendeiner Weise direkt oder indirekt U.S.-Sanktionen bei einer *U.S.-Person* bewirken, wäre die Sanktionsklausel nicht anwendbar, weil nicht die Beklagte direkt sanktioniert würde (act. 28 Rz. 204 ff.).

6.1.2. Die Beklagte bringt vor, sie würde gegen das verschuldensunabhängige U.S.-Sanktionsrecht verstossen, wenn sie die Versicherungsleistung auszahle. Die Beklagte würde einen Verstoss gegen das U.S.-Sanktionsrecht durch die *U.S.-Person J._____ Inc.* begehen (vgl. act. 32 Rz. 86, Rz. 92). Die Beklagte würde weiter auch gegen U.S.-Sanktionsrecht verstossen, wenn sie eine Zahlung in U.S.-Dollar veranlassen würde, weil diese über U.S.-Finanzinstitute abgewickelt würde. Das gelte selbst dann, wenn die Zahlungen von einem Konto einer *non-U.S.-Person* bei einer *non-U.S.-Person-Bank* stammen würden und für einen *non-U.S.-Person-Empfänger* bestimmt seien (vgl. act. 32 Rz. 94–97, Rz. 103, Rz. 128). U.S.-Personen sei es untersagt, Versicherungsansprüche zu bezahlen, einschliesslich der Erstattung von Geldern, wenn eine sanktionierte Person ein Interesse an der Transaktion habe, die erstattet würde resp. daran beteiligt sei. Die

Tatsache, dass eine SDN die Lösegeldzahlung bereits erhalten habe, ändere nichts an ihrer Beteiligung. Auch wenn die *P.*_____ selber keine Empfängerin der Versicherungsleistung sei, würde das OFAC davon ausgehen, dass die *P.*_____ ein Interesse an der Versicherungsforderung habe resp. daran beteiligt sei, da das OFAC die Versicherungsforderung als Teil der gleichen Transaktion wie die Lösegeldzahlung betrachten würde. Das OFAC würde die Zahlung des Versicherungsanspruchs zur Entschädigung der Klägerin für das Lösegeld genau gleich als Teil derselben Transaktion betrachten wie die Zahlung des Lösegelds durch die Klägerin (act. 32 Rz. 101 f.).

6.2. Rechtliches

6.2.1. Vertragsauslegung

AGB-Klauseln sind, wenn sie in Verträge übernommen werden, grundsätzlich nach denselben Prinzipien auszulegen wie andere vertragliche Bestimmungen (vgl. BGE 142 III 671, E. 3.3). Ziel der Vertragsauslegung ist es, in erster Linie den übereinstimmenden wirklichen Willen der Parteien festzustellen (vgl. Art. 18 Abs. 1 OR). Steht eine tatsächliche Willensübereinstimmung fest, bleibt für eine Auslegung nach dem Vertrauensgrundsatz kein Raum (BGE 132 III 626 E. 3.1; 128 III 70 E. 1a). Erst wenn eine tatsächliche Willensübereinstimmung unbewiesen bleibt, sind zur Ermittlung des mutmasslichen Parteiwillens die Erklärungen der Parteien aufgrund des Vertrauensprinzips so auszulegen, wie sie nach ihrem Wortlaut und Zusammenhang sowie den gesamten Umständen verstanden werden durften und mussten (BGE 144 III 93 E. 5.2.3; BGE 133 III 61 E. 2.2.1). Massgebend ist dabei der Zeitpunkt des Vertragsabschlusses. Nachträgliches Parteiverhalten ist bei der Auslegung nach dem Vertrauensprinzip nicht von Bedeutung; es kann höchstens – im Rahmen der Beweiswürdigung – auf einen tatsächlichen Willen der Parteien schliessen lassen (BGE 144 III 93 E. 5.2.3; BGE 133 III 61 E. 2.2.1).

6.2.2. Ermittlung des ausländischen Rechs

6.2.2.1. Gemäss Art. 16 Abs. 1 IPRG ist der Inhalt des anzuwendenden ausländischen Rechts von Amtes wegen festzustellen. Dazu kann die Mitwirkung der Par-

teien verlangt werden. Bei vermögensrechtlichen Ansprüchen kann der Nachweis den Parteien überbunden werden.

6.2.2.2. Das ausländische Recht hat nicht Tatsachen-, sondern Normcharakter. Entsprechend handelt es sich beim Nachweis von ausländischem Recht nicht um einen (Tatsachen-)Beweis im eigentlichen Sinne. Das Gericht hat die von den Parteien vorgetragenen Nachweise zum ausländischen Recht frei zu würdigen (BGer 5A_973/2017 vom 4. Juni 2019, E. 4.2; MÄCHLER-ERNE, Monica/WOLF-METTIER, Susanne, in: Grolimund/Loacker/Schnyder (Hrsg.), Basler Kommentar zum IPRG [BSK-IPRG], 4. Aufl., Basel 2021, N 17 zu Art. 16 IPRG). Es muss im Ergebnis mindestens von der Wahrscheinlichkeit der Richtigkeit und Vollständigkeit der vorgetragenen Nachweise überzeugt sein (BGer 5A_723/2017 vom 17. Dezember 2018, E. 5.2.1; BGer 5A_702/2014 vom 31. August 2015, E. 3.2.3; MÄCHLER-ERNE, Monica/WOLF-METTIER, Susanne, BSK-IPRG., N 10 und N 17 zu Art. 16 IPRG).

6.2.3. Prozessrechtliche Zulässigkeit der Rechtsgutachten der Parteien

6.2.3.1. Die Parteien reichen für die Ermittlung des ausländischen Rechts mehrere Parteigutachten zum U.S.-Sanktionsrecht ein; die Klägerin insgesamt vier, die Beklagte insgesamt drei (vgl. act. 29/16; act. 33/36; act. 39/2; act. 45/43; act. 49/2; act. 54/47; act. 57/1). Fünf der Rechtsgutachten gingen nach Aktenschluss ein (vgl. zum Aktenschluss die Verfügung vom 16. Mai 2022, act. 34).

6.2.3.2. Gemäss Bundesgericht kann ein privates Rechtsgutachten bereits begrifflich kein Novum darstellen, weil das Recht, auch das ausländische, keine Tatsache ist. Die für tatsächliche Noven aufgestellten zeitlichen Schranken dürfen nicht unbesehen übernommen werden. Einschlägige Ausführungen dürfen darum auch ausserhalb der für Tatsachenbehauptungen und Beweismittel vorgesehenen Verfahrensabschnitte gemacht werden (vgl. BGer. 5A_973/2017 vom 4. Juni 2019, E. 4.3 und E. 6.1.1).

6.2.3.3. Sämtliche Parteigutachten zum ausländischen Recht sind damit zulässig und zu berücksichtigen.

6.3. Würdigung

6.3.1. Im Vordergrund steht die Frage, ob die Beklagte wegen Verstosses gegen das U.S.-Sanktionsrecht *persönlich* bestraft würde, wenn sie die Versicherungsleistung auszahlen würde.

6.3.2. Die Beklagte darf gemäss Sanktionsklausel die Zahlung der Versicherungssumme verweigern, wenn sie mit der Zahlung U.S.-Sanktionsrecht verletzen und sich so strafbar machen würde (vgl. die in Erw. 2.3 wiedergegebene Sanktionsklausel). Die Tragweite der Sanktionsklausel hängt entscheidend von der Auslegung der Begriffe "expose" sowie "trade or economic sanctions, laws or regulations of the United States of America" ab.

6.3.3. Beide Parteien übersetzen das Wort "expose" mit "aussetzen". Gemeint ist damit nach dem Verständnis der Parteien, dass die Sanktionsklausel dann anwendbar ist, wenn für den Versicherer ein *erhebliches Risiko* besteht, im Falle bestimmter Leistungen wegen Verletzung von U.S.-Sanktionsrecht bestraft zu werden (vgl. act. 17 Rz. 183, Rz. 181–184.; act. 28 Rz. 194, wobei die Klägerin nicht substanziiert zu den Ausführungen der Beklagten Stellung nimmt, sondern sich, soweit nachvollziehbar, vor allem an deren weiten Auslegung stört, wonach auch eine Bestrafung von *J._____ Inc.* [der indirekten Eigentümerin der Beklagten] unter die Sanktionsklausel zu subsumieren sei, vgl. act. 28 Rz. 194, Rz. 200, Rz. 204, Rz. 206 f., Rz. 209).

6.3.4. Die Parteien äussern sich nicht dazu, wann ein *erhebliches Risiko* der Bestrafung durch das OFAC vorliegt. Ein natürlicher Konsens lässt sich damit nicht feststellen. Eine Auslegung nach dem Vertrauensprinzip erhellt, dass ein *erhebliches Risiko* dann besteht, wenn eine überwiegende Wahrscheinlichkeit dafür spricht, dass das OFAC in Kenntnis des Sachverhalts und gestützt auf das U.S.-Cyber-Sanktionsrecht *nicht nur* ein *Enforcement*-Verfahren gegen die Beklagte einleiten würde, sondern im Anschluss an das *Enforcement*-Verfahren die Beklagten wegen Verstosses gegen das U.S.-Sanktionsrecht auch bestrafen würde. Als Strafe gilt dabei jede Massnahme mit Strafcharakter. Die blosse Einleitung eines *Enforcement*-Verfahrens ohne anschliessende Sanktionierung der Beklagten reicht demgegenüber nicht aus. Die Sanktionsklausel hält fest, dass die sanktionierende Behörde eine konkrete "*sanction, prohibition or restriction"* anordnen muss, damit die Einrede der Sanktionsklausel erfolgreich erhoben werden kann.

Um sich auf die Sanktionsklausel berufen zu können, ist es aber nicht nötig, dass die vom OFAC angeordneten Massnahmen vor einem U.S.-Gericht angefochten werden und dieses die Massnahmen rechtskräftig bestätigt. Zum einen ist eine solche Voraussetzung in der Klausel nicht erwähnt. Zum anderen drängt sich dieses Verständnis aufgrund des Wortes *expose* im Sinne von *aussetzen* in Verbindung mit dem von den Parteien verwendeten Begriff *Risiko* auf. Unter einem Risiko ist ein *möglicher* negativer Ausgang bei einer Unternehmung oder die *Möglichkeit* des Verlustes zu verstehen (vgl. DUDEN Band 10, Das Bedeutungswörterbuch, 5. Aufl., Berlin 2018, Stichwort "Risiko"). Einem Risiko ernsthaft ausgesetzt zu sein, bedeutet somit nicht, dass sich das Risiko *tatsächlich* oder gar *endgültig* (im Sinne von rechtskräftig) verwirklichen muss.

6.3.5. Die Klägerin bestreitet die Vorbringen der Beklagten nicht, wonach mit dem Passus "*trade or economic sanctions, laws or regulations of the United States of America*" in der Sanktionsklausel auf das gesamte U.S.-Sanktionsrecht verwiesen wird. Sie macht aber geltend, die Klausel sei Teil der im Jahr 2010 am F._____er Versicherungsmarkt formulierten AVB und könne darum nur auf das damals geltende U.S.-Sanktionsrecht verweisen, nicht jedoch auf die erst später erlassenen U.S.-Sanktionen gegen Cyberkriminalität (vgl. act. 28 Rz. 197). Das überzeugt nicht. Massgebend für den Vertragsinhalt ist der Zeitpunkt des Vertragsabschlusses. Der vorliegend relevante Versicherungsvertrag wurde nach Erlass der Cyber-Sanktionen abgeschlossen. Damit ist das U.S.-Sanktionsrecht gegen Cyberkriminalität Vertragsbestandteil, war es doch bei Vertragsabschluss bereits in Kraft (zutreffend die Beklagte in act. 32 Rz. 191). Ob nach Vertragsschluss neu erlassene Sanktionen von der Sanktionsklausel erfasst sind, kann offen bleiben.

6.3.6. Damit stellt sich die Frage, ob das geltende U.S.-Sanktionsrecht gegen Cyberkriminalität die Auszahlung der Versicherungssumme durch die Beklagte verbietet.

6.3.7. Das OFAC wendet bei der Durchsetzung des U.S.-Sanktionsrechts einen verschuldensunabhängigen Massstab der Haftung an: Verschulden oder Vorsatz sind keine Voraussetzungen, um eine zivilrechtliche Strafe zu verhängen (vgl. act. 29/15 S. 4: "*OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held*

civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC).

6.3.8. Rechtsgrundlage für die U.S.-Cyber-Sanktionen bildet das *International Emergency Economic Powers Act* (IEEPA, integriert im United States Code, Title 50, §§ 1701–1707), welches dem U.S.-Präsidenten weitreichende Kompetenzen einräumt, um die nationale Sicherheit, die Aussenpolitik oder die Wirtschaft der Vereinigten Staaten zu schützen, sofern die Bedrohung der genannten Interessen ihren Ursprung ganz oder zu einem wesentlichen Teil ausserhalb der Vereinigten Staaten hat (vgl. 50 U.S. Code § 1701 (a)). Das IEEPA sieht dabei nicht etwa konkrete Sanktionen vor, sondern räumt dem U.S.-Präsidenten die Kompetenz ein, unter anderem Wirtschaftssanktionen als aussenpolitisches Mittel einzusetzen. 50 U.S. Code § 1705 (IEEPA) untersagt, gegen einen *Executive Order* des Präsidenten oder eine *Regulation* einer Behörde zu verstossen. Strafbar ist auch der Versuch eines Verstosses, sich zu einem Verstoss zu verschwören oder einen Verstoss zu verursachen ("*It shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter.*").

6.3.9. Der damalige U.S.-Präsident Barack Obama machte im Bereich der Cyberkriminalität von dieser Kompetenz jeweils in den Jahren 2015 und 2016 Gebrauch, indem er die *Executive Order 13694* vom 1. April 2015 und *Executive Order 13757* vom 28. Dezember 2016 erliess (vgl. Federal Register/ Vol- 80, No. 63/ Thursday, April 2, 2015/ Presidential Documents [18077] und Federal Register/ Vol. 82, No. 1/ Tuesday, January 3, 2017/ Presidential Documents [1]). Mit den *Executive Orders* wurden verschiedene Wirtschaftssanktionen im Bereich der Cyberkriminalität angeordnet, wobei darin nicht konkret bezeichnete Personen sanktioniert werden, sondern zu sanktionierende Personen generell-abstrakt beschrieben werden (vgl. Section 1 des Executive Order No. 13694 vom 1. April 2015). Die konkrete Umsetzung, insbesondere die Bezeichnung von sanktionierten Personen, obliegt dem *Secretary of the Treasury* (vgl. Section 8 des Executive Order No. 13694 vom 1. April 2015). Das OFAC als zuständige Behörde des *Treasury Departments* führt zu diesem Zweck eine Liste mit Personennamen (natürliche

Personen und sog. *entities*), die sanktioniert werden (SDN-Liste, vgl. auch Erw. 2.2). Es erlässt ausserdem sogenannte *Regulations*, die im *Code of Federal Regulations (CFR)* veröffentlicht werden (vgl. 31 CFR Part 578 *Cyber-Related Sanctions Regulations*). Eine *Regulation* nach U.S.-amerikanischem Recht ist eine "allgemeine Erklärung", die von einer Exekutivbehörde erlassen wird und in der Regel bindend ist. *Regulations* sind das Mittel, mit dem die Bundesbehörden die vom Kongress verabschiedeten Gesetze und sich darauf stützende *Executive Orders* umsetzen (vgl. ASIMOW, Michael/LEVIN, Ronald M., State and Federal Administrative Law, 5.ed., St. Paul (MN) 2020, S. 3 und S. 7).

6.3.10. Um die Tragweite der Sanktionen einzuschätzen, sind sodann auch das A*dvisory on Potential Sanctions Risks for Facilitating Ransomware Payments* vom 21. September 2021 und die auf der OFAC-Website aufgeschalteten *FAQ* (welche durchnummeriert und für die Praxis von grosser Relevanz sind) zu berücksichtigen, welche beide allerdings nicht bindend sind.

6.3.11. Vorweg ist festzustellen, dass betreffend die Strafbarkeit von Cyber-Erpressungsopfern, die ein Lösegeld an eine SDN bezahlt haben, noch keine Praxis des OFAC besteht. Soweit ersichtlich hat aber das OFAC bis heute noch kein einziges Mal ein *Enforcement*-Verfahren gegen ein Opfer einer Cyber-Erpressung durch eine SDN durchgeführt. Auch gegen die Hilfspersonen eines Opfers (Cyber-Versicherungsunternehmen und Cybersicherheitsunternehmen), die das Opfer bei der Abwicklung der Lösegeldzahlungen unterstützen, wurde noch nie eine Strafe ausgesprochen. Das OFAC übt somit grösste Zurückhaltung aus, was die Bestrafung des Erpressungsopfers wegen Verletzung von Sanktionsrecht anbelangt. Eine Bestrafung der Erpressungsopfer durch das OFAC käme letztlich einer doppelten Bestrafung der betroffenen Unternehmen gleich, was kaum im wirtschaftlichen Interesse der USA liegen dürfte. Gleichzeitig hat das OFAC aber in seinem Advisory vom September 2021 festgehalten, dass „[f]acilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations" (vgl. act. 29/15 S. 3 f.). Unter den Oberbegriff des *facilitating* können auch Cyber-Versicherungen subsumiert werden (vgl. act. 29/15 S. 4: "*This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, […]*".). Das OFAC führt weiter aus,

dass ein Einbezug des OFAC im Nachgang eines Angriffs (namentlich die selbst initiierte und vollständige Meldung eines Ransomware-Angriffs) als „*significant mitigating factor*“ berücksichtigt werde (vgl. act. 29/15 S. 5), was wiederum aufzeigt, dass das OFAC eine Lösegeldzahlung an eine SDN grundsätzlich als sanktionsrelevant qualifizieren kann.

6.3.12. Section 1 (a) *Executive Order 13694* hält fest, dass

> *"[a]ll property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in […]".*

Wenn somit Interessen (*property* oder *interests in property*) einer sanktionierten Person (SDN) betroffen sind, besteht ein sanktionsrechtlicher Anknüpfungspunkt. Die Interessen einer SDN werden dabei sehr weit ausgelegt. Die *Regulations* halten hierzu folgendes fest:

> ***"§ 578.314 Property; property interest.***
>
> *The terms property and property interest include money, checks, drafts, bullion, bank deposits, savings accounts, debts, indebtedness, obligations, notes, guarantees, debentures, stocks, bonds, coupons, any other financial instruments, bankers acceptances, mortgages, pledges, liens or other rights in the nature of security, warehouse receipts, bills of lading, trust receipts, bills of sale, any other evidences of title, ownership, or indebtedness, letters of credit and any documents relating to any rights or obligations thereunder, powers of attorney, goods, wares, merchandise, chattels, stocks on hand, ships, goods on ships, real estate mortgages, deeds of trust, vendors' sales agreements, land contracts, leaseholds, ground rents, real estate and any other interest therein, options, negotiable instruments, trade acceptances, royalties, book accounts, accounts payable, judgments, patents, trademarks or copyrights, insurance policies, safe deposit boxes and their contents, annuities, pooling agreements, services of any*

nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent".

6.3.13. Gemäss Section 1 (a) *Executive Order 13694* gilt sodann ein expansives Verständnis, wann ein Handeln ein Interesse einer SDN berührt: Die Interessen dürfen nicht übertragen, ausgezahlt, ausgeführt, zurückgenommen oder in anderer Weise gehandelt werden ("*[…] and may not be transferred, paid, exported, withdrawn, or otherwise dealt in […]*"). Auch eine Versicherungsleistung wird zur Interessensphäre der SDN gezählt, und zwar selbst dann, wenn das Versicherungsunternehmen nicht direkt die SDN bezahlt, sondern auch dann, wenn das Versicherungsunternehmen die Versicherungssumme ihrem Versicherungsnehmer auszahlt. Die Zahlung fällt dann unter den Begriff des *facilitating a ransomware payment*, was einem *dealing in the property or interests in property of an SDN* gleichkommt (vgl. bereits Erw. 6.3.11). Vorauszusetzen ist in Bezug auf die hier relevanten *cybercrime*-Risiken, dass der Versicherungsnehmer direkt oder indirekt ein Lösegeld an eine SDN leistete oder die SDN anderweitig vom Cyber-Angriff profitierte und die Versicherungsleistung den Schaden im Zusammenhang mit der Lösegeldzahlung deckt. Ob die Auszahlung der Versicherungssumme vor oder nach Zahlung der Lösegelds erfolgt, ist dabei irrelevant (vgl. zutreffend die Beklagte in act. 17 Rz. 121 f., Rz. 125 f.). Die Urheberschaft betreffend den Quellcode einer *Ransomware* stellt hingegen für sich allein genommen nach U.S.-Sanktionsrecht kein Interesse der SDN dar. Eine Transaktion im Zusammenhang mit einer Ransomware-Attacke – wie die Auszahlung einer Versicherungssumme – ist nur dann sanktionsrechtlich relevant, wenn mit der Transaktion ein Interesse der SDN tangiert wird (regelmässig wird das Interesse der SDN in einem finanziellen Profit aus der Lösegeldzahlung bestehen). Zu weit geht jedenfalls die Beklagte, wenn sie geltend macht, *jede* Nutzung von *K._____*, auch durch Dritte, führe zu einer verbotenen Transaktion, weil *P._____* über *K._____* an dieser Transaktion entweder direkt oder indirekt beteiligt sei (act. 32 Rz. 114, vgl. auch Rz. 289). Wie die Klägerin zutreffend ausführt (vgl. act. 28 Rz. 234), würde die blosse Urheberschaft von *P._____* betreffend die *Ransomware K._____* noch nicht ausreichen, um ein Interesse im Sinne des U.S.-Sanktionsrechts der

P._____ an jeder Transaktion, die einen Berührungspunkt zu *K._____* aufweist, zu bejahen.

6.3.14. Section 1 (a) Executive Order 13694 untersagt es *U.S. Persons* direkt oder indirekt in die Interessen einer SDN involviert zu sein. Als *U.S. Person* gilt gemäss Section 6(c) Executive Order 13694 und gemäss 31 CFR § 578.318 "*[…] any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States*". Die Beklagte als nach … [dem Recht eines europäischen Staates] organisierte Gesellschaft mit Sitz in … [Staat in Europa] ist somit keine *U.S. Person* im Sinne des U.S.-Sanktionsrechts. Daran ändert auch die indirekte Eigentümerschaft durch die U.S.-Gesellschaft *J._____ Inc.* nichts. Die Beklagte ist vielmehr eine *non-U.S.-Person* (was zwischen den Parteien unstrittig ist, vgl. act. 28 Rz. 239; act. 17 Rz. 135 S. 40).

6.3.15. Eine *non-U.S.-Person* kann nach dem Verständnis des OFAC gleichwohl wegen einer Verletzung von U.S.-Sanktionsrecht belangt werden (vgl. auch das Advisory vom 21. September 2021, act. 29/15 S. 4: "[…] *any transaction that causes a violation under IEEPA, including a transaction by a non-U.S. person that causes a U.S. person to violate any IEEPA-based sanctions prohibitions, is also prohibited*". Entscheidend ist der Passus in § 1705 IEEPA, wonach sich auch strafbar macht, wer einen Verstoss gegen U.S.-Sanktionsrecht durch einen Dritten bewirkt ("*It shall be unlawful for a person to […] cause a violation of any license, order, regulation, or prohibition […]*"). Dieser Tatbestand ist unter anderem dann erfüllt, wenn eine Zahlung in U.S.-Dollar erfolgt, da diese über das amerikanische *Clearing-und-Settlement-System* abgewickelt wird. Dabei spielt es keine Rolle, ob die *direkt* involvierten Finanzdienstleister, welche die Zahlung ausführen, *U.S.-Persons* sind oder nicht. Anknüpfungspunkt ist die Zahlung in U.S.-Dollar (vgl. OFAC *Enforcement* Release vom 30. Dezember 2022 betreffend *Settlement* mit Danfoss A/S, S. 3 f., vgl. auch EMMENEGGER, Susan/ZUBER, Florence, To Infinity and Beyond: U.S. Dollar-Based Juristiction in the U.S. Sanctions Context, in: SZW/RSDA 2/2022, S. 114 ff., S. 121). Da auch Finanzdienstleister, die *non-U.S.-Persons* sind, zur Abwicklung der Zahlung in U.S. Dollar auf das *U.S.-Clearing-und-Settlement-System* zurückgreifen müssen, beteiligen sie damit

zwingend auch einen U.S.-Finanzdienstleister an der Transaktion (vgl. ausführlich zum *U.S.-Clearing-und-Settlement-System* EMMENEGGER,/ZUBER, a.a.O., S. 121 ff.). Der U.S.-Finanzdienstleister wirkt so bei einer Transaktion mit, die ihm nach U.S.-Sanktionsrecht untersagt ist, weil die Transaktion letztlich mit der Lösegeldzahlung an die SDN korreliert. Verursacht hätte diese Verletzung eine *non-U.S.-Person*, die damit auch gegen U.S.-Sanktionsrecht verstossen würde. Auch die Parteigutachter gehen von diesem Verständnis des OFAC aus (vgl. act. 33/36 Rz. 53; act. 39/2 S. 11 zu Rz. 53). Die klägerische Forderung lautet auf U.S.-Dollar (vgl. act. 1 Rz. 98; act. 32 Rz. 99). Würde die Beklagte die Versicherungssumme, die als Ersatz für den Schaden aus der Lösegeldzahlung dient, leisten, würde sie zwingend einen U.S.-Finanzdienstleister an der Transaktion beteiligen. Würde die Zahlung der Versicherungssumme weiter das Interesse einer SDN berühren, hätte der U.S.-Finanzdienstleister als *U.S.-Person* eine nach U.S.-Sanktionsrecht verbotene Transaktion ausgeführt, bewirkt durch die Beklagte, die sich so dem Risiko einer Bestrafung durch das OFAC aussetzen würde. Entscheidend ist vorliegend damit die Frage, ob aufgrund der Auszahlung der Versicherungssumme tatsächlich das Interesse der *P.*_____ als SDN betroffen wäre (siehe hierzu nachfolgende Erw. 7).

6.3.16. Offen bleiben kann damit, ob die Klausel auch greift, wenn nicht die Beklagte direkt, sondern ausschliesslich ihre indirekte Eigentümerin *J.*_____ *Inc.* als U.S.-Unternehmen wegen der Auszahlung der Versicherungssumme durch die Beklagte bestraft würde.

6.4. Fazit

Die Beklagte würde sich der Verletzung von U.S.-Sanktionsrecht strafbar machen, wenn sie durch Auszahlung der Versicherungssumme ein Interesse einer SDN tangieren würde. Das Interesse wäre bereits dann betroffen, wenn die klägerische Lösegeldzahlung an eine SDN ginge oder diese davon anderweitig profitierte und die Versicherungssumme den Schaden aus der Lösegeldzahlung ersetzte. Die Verletzung von U.S.-Sanktionsrecht wäre vorliegend dadurch gegeben, dass bei der Auszahlung der Versicherungssumme in U.S.-Dollar zwingend ein U.S.-Finanzdienstleister, mithin eine *U.S.-Person*, an der Transaktion beteiligt wäre.

7. Interesse der P._____ als SDN betreffend die Auszahlung der Versicherungssumme

7.1. Parteivorbringen

7.1.1. Die Klägerin bestreitet, dass der Cyber-Angriff auf sie von der *P.*_____ ausgeführt worden sei. Ausserdem sei nicht erstellt, dass die Ransomware *K.*_____ von der *P.*_____ entwickelt worden sei. Es lägen mehrere Hinweise vor, dass keine Verbindung bestehe. Selbst wenn die *P.*_____ die Ransomware entwickelt hätte, stünde noch nicht fest, dass sie diese auch gegen die Klägerin eingesetzt und vom Cyber-Angriff gegen die Klägerin im Sinne des U.S.-Sanktionsrechts profitiert habe (vgl. act. 28 Rz. 223 ff., Rz. 227 ff.).

7.1.2. Die Beklagte hält zunächst fest, dass das OFAC die Ransomware *Q.*_____ der sanktionierten *P.*_____ zuordne. Analysiere man *Q.*_____, liessen sich zahlreiche Gemeinsamkeiten mit einer weiteren, später verwendeten Ransomware names *AB.*_____ feststellen (vgl. act. 32 Rz. 27 f.; act. 33/34 S. 4). Noch bevor das OFAC die *P.*_____ sanktioniert habe, sei eine weitere Ransomware namens *AC.*_____ aufgetaucht, deren Quellcode zahlreiche Übereinstimmungen mit dem Programmcode der Ransomware *AB.*_____ aufgewiesen habe. Die Beklagte macht geltend, dass *AB.*_____ und *AC.*_____ nicht nur Ähnlichkeiten beim Programmcode aufwiesen, sondern auch die Infrastruktur teilen würden, die benutzt worden sei, um die Ransomware in Umlauf zu bringen. Dies lege den Schluss nahe, dass die gleiche Urheberschaft für beide Programme anzunehmen sei (act. 33/34 S. 5). Nachdem die *P.*_____ sanktioniert worden sei, sei die streitrelevante Ransomware *K.*_____ in Umlauf gesetzt worden, die zahlreiche Gemeinsamkeiten mit *AB.*_____ und *AC.*_____ aufweise (vgl. act. 33/34 S. 6). Ausgehend von *Q.*_____ über *AB.*_____ und *AC.*_____ sei die Urheberschaft der *P.*_____ für *K.*_____ – und damit die Täterschaft für den Angriff gegen die Klägerin – zu bejahen. Zahlreiche Cybersecurity-Experten hätten folgerichtig die Meinung geäussert, dass hinter *K.*_____ die *P.*_____ stehe (vgl. act. 32 Rz. 241; act. 33/34 S. 6).

7.2. Rechtliches

7.2.1. Beweislast

Gestützt auf die Rechtswahlklausel beurteilt sich die Frage der Beweislast nach der anwendbaren *lex causae* (vgl. BGE 134 III 224, E. 5.1 und E. 5.2 sowie auch JUNGO, Alexandra, in: Schmid (Hrsg.), Zürcher Kommentar zum Zivilgesetzbuch, Art. 8 ZGB. Beweislast, 3. Aufl., Zürich/Basel/Genf 2018, N 65 zu Art. 8). Vorliegend ist es die Beklagte, die sich auf die Ausnahmeklausel betreffend Sanktionen beruft, um die Klage abzuwehren. Die Anwendbarkeit der Sanktionsklausel setzt voraus, dass der Angriff von einer sanktionierten Organisation ausgeführt wurde (vgl. Erw. 6.3). Die Beklagte trägt folglich die Beweislast dafür, dass hinter dem Cyber-Angriff mit der Ransomware *K.*_____ gegen die Klägerin die sanktionierte *P.*_____ stand oder diese zumindest ein Interesse daran hatte.

7.2.2. Beweismass

Auch das Beweismass richtet sich grundsätzlich nach der *lex causae* (vgl. GROLIMUND, Pascal, in: Staehelin/Staehelin/Grolimund, Zivilprozessrecht, 3. Aufl., Zürich/Basel/Genf 2019, § 18 N 150). Vorliegend ist indes zu berücksichtigen, dass das hiesige Gericht einschätzen muss, ob das OFAC angesichts des erstellten Sachverhalts annehmen würde, dass eine sanktionierte Person hinter dem Cyber-Angriff auf die Klägerin steht. Insofern ergibt sich letztlich aus dem vertraglichen Verweis auf das U.S.-amerikanische Recht das anzuwendende Beweismass. Die Parteigutachter sind sich einig, dass die Verletzung von U.S.-Sanktionen mit einer "*preponderance of reliable, probative and substantial evidence*" (Beweismass der *preponderance*) erstellt sein muss, damit das OFAC Massnahmen anordnen kann (vgl. act. 33/36 Rz. 42 und act. 49/2 Ziffer 2, Hervorhebung hinzugefügt, auch act. 32 Rz. 135). Gemäss den Parteien muss eine Tatsache "*more likely than not*" zutreffen, damit sie als erstellt gelten kann (vgl. act. 33/36 Rz. 42; act. 39/2 S. 2; act. 49/2 Ziffer 2 und Ziffer 4; act. 54/47 Rz. 9, dort auch FN 13 und FN 14). Das ist dann der Fall, wenn die für den Nachweis einer Tatsache offerierten Beweise, "*superior evidentiary weight to the evidence presented on the other side of the issue*" haben (vgl. so die Klägerin in act. 49/2 Ziffer 4, interne Anführungszeichen im Zitat wegelassen; vgl. die Beklagte in

act. 54/47: "*A determination that a fact is more likely than not to be true is reasonably determined to have a greater than 50% probability of being true*", vgl. zur 50%-Grenze auch die Klägerin in act. 48 Rz. 96).

7.2.3. Zulässigkeit der Cybergutachten der Parteien

7.2.3.1. Beide Parteien reichen mehrere Parteigutachten ihrer Cybersecurity-Experten ein. Einzig das Gutachten vom 5. Mai 2022 der Beklagten wurde vor Aktenschluss eingereicht (vgl. act. 33/34). Es ist somit prozessrechtlich zulässig und zu berücksichtigen. Sämtliche weitere Gutachten (act. 39/1, act. 49/1 und act. 57/2; act. 45/44; act. 54/46) wurden erst nach Aktenschluss, welcher am 16. Mai 2022 verfügt wurde, eingereicht (act. 34). Laut den Parteien handelt es sich – soweit sich die Parteien überhaupt zur Novenfrage äussern – bei den nach Aktenschluss eingereichten Cyber-Gutachten jeweils um echte Noven (vgl. act. 44 Rz. 2–4 und act. 52 Rz. 3; act. 62 Rz. 3).

7.2.3.2. Anders als die Parteigutachten betreffend das ausländische Recht betreffen die Cyber-Gutachten Tatsachen, weshalb die Novenschranke gemäss Art. 229 Abs. 1 ZPO gilt. Die nach Aktenschluss eingereichten Parteigutachten der Cybersecurity-Experten stellen sog. Potestativnoven dar, weil deren Entstehung vom Willen der Parteien abhängt (auch wenn sie teilweise zu den jeweiligen Gutachten der Gegenseite Stellung nehmen). Nach dem Bundesgericht stellen Potestativnoven *unechte* Noven dar und ihre Zulässigkeit entscheidet sich danach, ob sie trotz zumutbarer Sorgfalt im Sinne von Art. 229 Abs. 1 lit. b ZPO nicht vorher vorgebracht werden konnten (BGE 146 III 416, E. 5). Der Sorgfaltsnachweis setzt voraus, dass die Dupliknoven kausal waren für die anschliessend eingereichten Potestativnoven (vgl. BGE 146 III 416, E. 6). Dabei obliegt es der Partei, die das Novenrecht beansprucht, im Einzelnen darzutun, dass bzw. inwiefern diese Voraussetzungen erfüllt sind (HGer ZH HG190089 vom 3. Mai 2021 E. 2.2.; DIKE Komm ZPO-PAHUD, Art. 229 N 15; SCHMID, Das Verfahren vor Handelsgericht: aktuelle prozessuale Probleme, ZZZ 2017, S. 156 f.).

7.2.3.3. Die klägerische Stellungnahme zur Duplik vom 14. Juni 2022 (act. 38) mit dem erstmals eingereichten Cyber-Gutachten vom 13. Juni 2022 (act. 39/1) als Beilage erfolgte unter anderem als Reaktion auf das von der Beklagten mit der

Duplik eingereichte Cyber-Gutachten vom 5. Mai 2022 (act. 33/34). Es handelt sich um eine zulässige Stellungnahme zu den Dupliknoven in Wahrnehmung des Replikrechts. Die Zulässigkeitsvoraussetzungen gemäss Art. 229 ZPO sind demnach erfüllt. Betreffend die weiteren Gutachten gehen die Parteien, wie erwähnt, von echten Noven aus, was in Anwendung der bundesgerichtlichen Rechtsprechung zu den Potestativnoven unzutreffend ist. Da es sich um unechte Noven handelt, hätten die Parteien darlegen müssen, weshalb es ihnen trotz zumutbarer Sorgfalt nicht möglich gewesen sein soll, diese Noven frühzeitig und konzentriert vorzutragen, was die Parteien jedoch nicht getan haben. Ohnehin ist nicht ersichtlich, weshalb es den Parteien nicht möglich gewesen sein soll, ihre Tatsachenbehauptungen betreffend dem entscheidrelevanten Konnex zwischen der *P.*_____ und *K.*_____ einerseits und dem Cyberangriff auf die Klägerin andererseits konzentriert in einer einzigen Eingabe – anstatt über mehrere Eingaben verteilt – vorzutragen.

7.2.3.4. Zusammenfassend sind einzig das vor Aktenschluss eingereichte Cyber-Gutachten vom 5. Mai 2022 der Beklagten sowie das nach Aktenschluss eingereichte klägerische Cyber-Gutachten vom 13. Juni 2022 prozessrechtlich zulässig. Sämtliche weiteren Cyber-Gutachten sind nicht zu berücksichtigen.

7.3. Würdigung

7.3.1. Die Beklagte muss mit dem Beweismass der *preponderance* aufzeigen, dass die sanktionierte *P.*_____ am Angriff gegen die Klägerin ein rechtlich relevantes Interesse hatte. Einen direkten Nachweis der Beteiligung der *P.*_____ am Angriff offeriert die Beklagte nicht. Sie stützt ihre Behauptungen vielmehr auf Indizienbeweise (d.h. Tatsachen, die einen Schluss auf das Vorhandensein der entscheidenden Tatsache erlauben, RÜETSCHI, Sven, in: Hausheer/Walter (Hrsg.), Berner Kommentar zur Zivilprozessordnung, Bern 2012, N 7 zu Art. 168). Kern ihrer Argumentation ist dabei die Annahme, dass sich die Beteiligung der *P.*_____ am Angriff gegen die Klägerin aus der (behaupteten) *Urheberschaft* der *P.*_____ betreffend den Quellcode von *K.*_____ und den beim Angriff beobachteten *Modus Operandi* ableiten lasse. Wenn feststehe, dass die beim Angriff auf die Klägerin verwendete Ransomware *K.*_____ von der *P.*_____ programmiert worden sei, liege der Schluss nahe, dass diese hinter dem Cyber-Angriff gegen die Klägerin

gestanden oder zumindest ein rechtlich relevantes Interesse im Sinne des U.S.-Sanktionsrechts an dem Angriff gehabt habe. Die Beklagte möchte die Urheberschaft der *P._____* anhand eines Vergleichs der beim Angriff verwendeten Ransomware *K._____* mit den älteren Ransomwares *Q._____*, *AB._____* und *AC._____* nachweisen, die alle der *P._____* zuzuschreiben seien.

7.3.2. Die Programmcodes der verschiedenen Ransomwares – insbesondere auch von *K._____* – reicht die Beklagte nicht ein. Weder in den Rechtsschriften noch in den Cyber-Gutachten der Beklagten werden die Programmcodes näher dargestellt. Die Beklagte behauptet zwar einige Übereinstimmungen zwischen den Ransomwares sowie der *Modi Operandi* (vgl. act. 32 Rz. 29, Rz. 32). Es bleibt aber bei (bestrittenen, vgl. act. 38 Rz. 72 ff.) Behauptungen, die ohne zusätzliche Ausführungen samt entsprechenden Beweisofferten unsubstanziiert und unbewiesen bleiben. Insbesondere fehlen *konkrete Ausführungen* zum Angriff auf die Klägerin. Es reicht nicht, allfällige Gemeinsamkeiten zwischen verschiedenen Ransomwares aufzuzeigen. Vielmehr sind der Ablauf und die Eigenschaften des konkreten Cyber-Angriffs vom tt.mm.Tatjahr gegen die Klägerin darzulegen und nachzuweisen. Die Behauptung einer gewissen "Verwandtschaft" zwischen den verschiedenen Programmcodes genügt nicht, um einen sanktionsrelevanten Konnex zwischen der *P._____* und dem Cyber-Angriff gegen die Klägerin nachzuweisen (vgl. zutreffend auch act. 38 Rz. 83 f.; act. 39/1 Rz. 24 f.). Nicht auszuschliessen ist, dass andere Nutzer einen Programmcode der *P._____* für die Entwicklung ihrer eigenen Ransomware verwendet haben, ohne Wissen der *P._____*. Somit vermöchte der Nachweis der blossen Urheberschaft der *P._____* betreffend den Programmcode von *K._____* für sich allein noch kein Interesse einer SDN im Sinne des U.S.-Sanktionsrecht darzutun (vgl. Erw. 6.3.13). Der Vergleich der Programmcodes basiert nämlich auf der Prämisse, dass die Ransomwares – auch nachdem sie bereits im Umlauf sind – exklusiv von der Cybercrime-Gruppe eingesetzt und weiterentwickelt werden, die sie auch ursprünglich programmiert hat. Die Klägerin hat aber nicht aufgezeigt, dass neuere Ransomwares, deren Programmcode Ähnlichkeiten mit dem Programmcode einer früher zirkulierenden, älteren Ransomware aufweist, nur bzw. stets von derselben Gruppe entwickelt und eingesetzt werden, die die ältere Ransomware programmierte. Die Prämisse der Beklagten bleibt unbewiesen. Selbst der Gutachter der Beklagten führt aus, dass

die verschiedenen cyberkriminellen Gruppen Programmteile anderer Gruppen kopieren, unter anderem im Versuch, ihre Identität zu verschleiern. Somit bestehen Zweifel daran, ob die Verwendung von Ransomware mit ähnlichen Programmcodes nur durch den ursprünglichen Urheber des Programmcodes oder mit dessen Zustimmung erfolgen kann (vgl. auch Erw. 7.3.6.6). Auch der klägerische Gutachter weist überzeugend darauf hin, dass *K._____* – auch in Bezug auf die Art und Weise der Verbreitung – Eigenschaften aufweist, die sich auch in anderen Ransomwares finden und die nicht proprietär der *P._____* zugeordnet werden können (vgl. act. 38 Rz. 83 ff.; act. 39/1 Rz. 17). Selbst wenn der Quellcode der für den Cyberangriff auf die Klägerin verwendeten Ransomware somit gewisse Übereinstimmungen mit dem Programmcode einer von der *P._____* verwendeten Ransomware aufgewiesen hätte, könnte der Angriff auf die Klägerin vorliegend nicht der *P._____* zugeordnet werden.

7.3.3. Das OFAC hat zudem nie dargelegt, aufgrund welcher Tatsachen und Überlegungen es die cyberkriminellen Gruppen konkret identifiziert und sanktioniert, sondern diese jeweils ohne Veröffentlichung der eigenen forensischen Abklärungen in ihre SDN-Liste aufgenommen. Die Kriterien einer allfälligen Zuordnung von *einzelnen* Cyber-Angriffen zu bestimmten cyberkriminellen Gruppen bleiben entsprechend unbekannt. Auch besteht betreffend das Cyber-Sanktionsrecht keine Praxis des OFAC in Bezug auf Verstösse gegen das Sanktionsrecht, da das OFAC bis heute in diesem Bereich noch keine Entscheide veröffentlicht hat (vgl. bereits Erw. 6.3.11). Es lässt sich somit nicht ohne weiteres feststellen, aufgrund von welchen Voraussetzungen das OFAC einen Verstoss gegen das Cyber-Sanktionsrecht annehmen würde. Die Ausführungen des OFAC, die *P._____* habe Lösegeldzahlungen von über [Hoher Betrag] erpresst (vgl. act. 29/15 S. 3), lassen darauf schliessen, dass das OFAC gestützt auf *konkrete* Zahlungsflüsse die *P._____* als Täterin identifizierte und die Zuordnung der einzelnen Cyber-Angriffe zu einer SDN – neben Hinweisen technischer Natur – insbesondere (auch) anhand der Zahlungsflüsse erfolgt. Die Urheberschaft betreffend eine Ransomware mag zwar Grundlage für die Aufnahme in die SDN-Liste sein, weil sie eine "*significant malicious cyber-enabled activit[y]*" sein kann (vgl. auch 31 CFR § 578.315). Aber sie stellt für sich allein *kein Interesse einer SDN* dar; ebenso wenig lässt sich *allein gestützt auf sie* ein *bestimmter Cyber-Angriff*

einer bestimmten cyberkriminellen Gruppierung zuordnen. Aus der Urheberschaft der Ransomware allein lässt sich nicht ableiten, ob diese auch diesen *bestimmten* Angriff ausgeführt hat und/oder diese überhaupt ein Interesse am Angriff hatte. Daran ändert das Beweismass der *preponderance* nichts. Hinsichtlich der Zahlungsflüsse ist vorliegend einzig erstellt, dass die Klägerin (bzw. die *N.*_____ im Auftrag der Klägerin) die Lösegeldzahlung in Bitcoins an eine Krypto-Wallet-Adresse zahlte, die bis heute vom OFAC *keiner* SDN zugeordnet wurde (vgl. act. 29 Rz. 79; act. 32 Rz. 262). Die Beklagte äussert sich nicht weiter zu konkreten Zahlungsflüssen im Zusammenhang mit dem Cyber-Angriff gegen die Klägerin. Dass die *P.*_____ finanziell von der Lösegeldzahlung profitierte, ist damit weder substanziiert behauptet noch sonst wie erstellt.

7.3.4. Auch das bisherige Verhalten des OFAC betreffend den streitrelevanten Cyber-Angriff untermauert, dass eine bloss mögliche Urheberschaft betreffend die Ransomware nicht ausreicht, um ein Interesse der *P.*_____ am Cyber-Angriff gegen die Klägerin nachzuweisen. Das OFAC hatte bereits vor Rechtshängigkeit des vorliegenden Verfahrens Kenntnis vom Angriff auf die Klägerin und der dabei eingesetzten Ransomware *K.*_____. Zum einen wurde über den Angriff auf die Klägerin weltweit in den Medien berichtet (vgl. auch act. 17 Rz. 78 f.; act. 28 Rz. 68). Zum anderen informierte die Klägerin das FBI und hatte das OFAC Kenntnis von der Lösegeldzahlung (vgl. act. 1 Rz. 57, Rz. 66; act. 28 Rz. 92). Die Beklagte beantragte beim OFAC sodann am 29. Oktober 2021 – im Verlauf des vorliegenden Verfahrens – eine Einzellizenz, welche die streitgegenständliche Zahlung im Voraus genehmigen sollte (vgl. act. 28 Rz. 131; act. 32 Rz. 68 ff.; der aktuelle Stand des Lizenzverfahrens ist unbekannt, wobei sich diesbezüglich weder aus der klägerischen Noveneingabe vom 10. Februar 2023 (vgl. act. 62; act. 63/1A–B) noch aus der Stellungnahme vom 23. Februar 2023 der Beklagten (vgl. act. 65) neue, entscheidrelevante Erkenntnisse ergeben). Unbestrittenermassen hat das OFAC bis heute weder gegen die Klägerin (oder einer mit dieser verbundenen U.S.-Gesellschaft) noch gegen die mit der Ausführung der Bitcoin-Lösegeldzahlung beauftragten (*U.S.-Person*) *N.*_____ ein *Enforcement*-Verfahren durchgeführt. Auch gegen andere Cyber-Versicherungsunternehmen, die an die Klägerin im Zusammenhang mit dem streitrelevanten Cyber-Angriff Leistungen erbrachten, wurden soweit bekannt keine *Enforcement*-Verfahren durchgeführt

oder gar Strafen ausgesprochen. Dieses Verhalten des OFAC muss vorliegend in die Würdigung einfliessen, geht es doch gerade darum einzuschätzen, ob das OFAC eine Täterschaft der *P.*_____ im Zusammenhang mit dem Cyber-Angriff gegen die Klägerin bejahen würde. Zusammenfassend ist auch das Verhalten des OFAC ein gewichtiger Faktor, um eine Täterschaft oder ein Interesse der *P.*_____ im Zusammenhang mit dem Cyber-Angriff gegen die Klägerin zu verneinen.

7.3.5. Die Beweisführung der Beklagten scheitert damit bereits in ihrem Ansatz. Die blosse Urheberschaft der *P.*_____ hinsichtlich der Ransomware *K.*_____ würde – wenn sie denn überhaupt nachgewiesen wäre –, nicht ausreichen, um die Sanktionsklausel zu aktivieren. Als blosser Indizienbeweis müssten neben der Urheberschaft weitere Anhaltspunkte vorliegen, wie namentlich konkrete Zahlungsflüsse im Zusammenhang mit dem Cyber-Angriff vom tt.mm.Tatjahr, um ein Interesse der *P.*_____ am Angriff zu erstellen. Die Beklagte behauptet indes keine weiteren Hilfstatsachen. Da die behauptete Urheberschaft der *P.*_____ betreffend den Programmcode von *K.*_____ für sich allein betrachtet nicht entscheidrelevant ist, wäre auch das von der Beklagten beantragte Gerichtsgutachten betreffend die Urheberschaft der *P.*_____ hinsichtlich *K.*_____ (vgl. act. 17 Rz. 96, act. 32 Rz. 22) nicht zielführend. Ausserdem scheitert der Beweisantrag auch daran, dass die Beklagte damit ihre Substanziierungspflicht an den Gutachter delegieren würde, hat sie doch hinsichtlich der notwendigen Tatsachen (namentlich die relevanten Programmcodes oder die Zahlungsflüsse) keine hinreichend substanziierten Behauptungen aufgestellt. Eine gerichtliche Expertise dient nur dazu, hinreichend substanziierte Tatsachenbehauptungen in tatsächlicher Hinsicht zu prüfen. Fehlt es an substanziierten Behauptungen, kann dies nicht durch einen Beweisantrag nachgeholt werden (vgl. Urteil des Bundesgerichts, 4A_447/2018, vom 20. März 2019, E. 5.2.4). Die beantragte Einholung des Gutachtens hat darum zu unterbleiben.

7.3.6. Der Vollständigkeit halber wird nachfolgend aufgezeigt, dass die Beklagte auch die von ihr behauptete Urheberschaft von *P.*_____ betreffend *K.*_____ *nicht* nachzuweisen vermag. Selbst wenn man der Argumentation der Beklagten hinsichtlich der behaupteten Entscheidrelevanz der Urheberschaft im Ergebnis zu-

stimmen würde, bliebe der Tatsachenvortrag der Beklagten unsubstanziiert und unbewiesen:

7.3.6.1. Die Beklagte beginnt ihre Beweiskette betreffend die Urheberschaft der *P.*_____ mit dem Schadprogramm *Q.*_____ (vgl. act. 32 Rz. 24). *Q.*_____ wurde vom OFAC der *P.*_____ zugeschrieben (vgl. 29/15 S. 3), weshalb die Urheberschaft der *P.*_____ hinsichtlich *Q.*_____ erstellt ist.

7.3.6.2. Die Beklagte sieht einen direkten Konnex von *Q.*_____ zur Ransomware *AB.*_____. Beide seien derselben Urheberin zuzuordnen (vgl. act. 32 Rz. 27 mit Verweis auf act. 33/34 S. 4). Diese gemeinsame Urheberschaft stützt sie auf eine (behauptete) Ähnlichkeit zwischen den Programmierungscodes der Ransomwares *Q.*_____ und *AB.*_____. Die beiden Schadprogramme seien zudem zur selben Zeit programmiert worden, was nahelege, dass beide von der *P.*_____ stammen würden (vgl. act. 32 Rz. 26 f.; act. 33/34 S. 4). Die Programmcodes der beiden Schadprogramme hat die Beklagte, wie erwähnt, nicht eingereicht. Das OFAC hat die Schadsoftware *AB.*_____ bis heute *nicht* der *P.*_____ zugeordnet, weshalb bereits die behauptete Verbindung zwischen diesen Schadsoftwares zu verneinen ist. Es ist nicht anzunehmen, dass das OFAC über mehrere Jahre sanktionsrelevante Anknüpfungspunkte verschweigen würde, ist es doch dafür bekannt, die sanktionsrelevanten Informationen regelmässig zu aktualisieren. Die Beklagte verweist in ihren Gutachten zwar mehrmals auf Online-Beiträge, in welchen eine Autorschaft von *P.*_____ betreffend *AB.*_____ bejaht wird. Die Beiträge enthalten hingegen keine vertiefte Auseinandersetzung mit der Frage, wer die *AB.*_____-Ransomware entwickelt hat, sondern sie halten vielmehr pauschal fest, hinter *AB.*_____ stehe die *P.*_____. Das genügt vorliegend nicht, um die Autorschaft von *P.*_____ nahezulegen, zumal die Beklagte ohnehin *in toto* auf die Beiträge verweist, ohne sich mit diesen genauer auseinanderzusetzen. Richtig ist immerhin, dass das *U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)* in einem Bericht die zahlreichen Übereinstimmungen zwischen den Programmcodes von *Q.*_____ und *AB.*_____ erwähnte, und dass verschiedene Cyber-Sicherheitsexperten sowohl *Q.*_____ als auch *AB.*_____ der *P.*_____ zuordnen würden. Entscheidend sei dabei insbesondere,

dass beide Schadprogramme *nahezu gleichzeitig im Umlauf* gesetzt wurden (vgl. act. 32 Rz. 27; act. 33/34 S. 4 mit Verweis auf den *CISA* Report). Diese Gleichzeitigkeit erhöht die Wahrscheinlichkeit eines gemeinsamen Urhebers, weil die zeitgleiche Entwicklung der Schadprogramme die Möglichkeit mindert, dass eine andere cyberkriminelle Gruppe Programmteile von *Q._____* übernehmen konnte, um anschliessend *AB._____* zu entwickeln. Insofern wäre eine Urheberschaft von *P._____* hinsichtlich *AB._____* gestützt auf das Beweismass der *preponderance* nicht ausgeschlossen. Gleichwohl haben weder die CISA noch das OFAC *AB._____* der *P._____* zugeordnet, was letztlich entscheidend ist.

7.3.6.3. Im Cyber-Gutachten der Beklagten finden sich sodann Ausführungen zur Ransomware *AC._____*, die gemäss der Beklagten grosse Teile des Programmcodes von *AB._____* übernommen habe (vgl. act. 33/34 S. 4; die Klägerin bestreitet eine Verbindung zwischen der *P._____* und *AC._____*, vgl. act. 38 Rz. 75 mit Verweis auf act. 39/1 Rz. 12). Die Beklagte macht in der Duplik allerdings keine Ausführungen zu *AC._____* und es finden sich entsprechend auch keinerlei Verweise auf ihr Cyber-Gutachten im Zusammenhang mit *AC._____*. Damit genügt die Beklagte den bundesgerichtlichen Anforderungen an einen Verweis auf eine Beilage nicht, wonach Verfahrensparteien ihrer Behauptungs- und Substanziierungslast in den Rechtsschriften nachkommen müssen (vgl. BGer 4A_443/2017 vom 30. April 2018, E. 2.2.1 und E. 2.2.2 m.w.H.). In Bezug auf die Ransomware *AC._____* ist das Cyber-Gutachten der Beklagten, dessen diesbezüglichen Ausführungen sich teilweise mit denjenigen zu *AB._____* überschneiden, demnach nicht zu beachten. Selbst wenn man aber die Ausführungen im Parteigutachten betreffend *AC._____* berücksichtigen würde, könnte die Beklagte daraus nichts zu ihren Gunsten ableiten. Der Gutachter der Beklagten räumt nämlich selbst ein, dass nicht klar gewesen sei, ob *AC._____* von der *P._____* programmiert und eingesetzt oder nicht vielmehr von einer anderen kriminellen Gruppe gestützt auf *AB._____* programmiert worden sei (vgl. act. 33/34 S. 5). Der Gutachter möchte diese Unsicherheit betreffend die Urheberschaft damit ausräumen, dass sowohl *AC._____* einerseits als auch *Q._____* und *AB._____* andererseits in der Cyber-Crime-Szene allgemein verbreitete *Botnets*, wie namentlich *AD._____*, verwendet hätten (vgl. act. 33/34 S. 5). Unter Botnets versteht man miteinander über das Internet verbundene und mit Malware infizierte Geräte, die von einem Hacker kon-

trolliert und für Angriffe auf noch nicht infizierte Systeme verwendet werden (vgl. Was ist Malware? abrufbar unter https://www.ibm.com/de-de/topics/malware, Stichwort "Botnets"). Die Behauptung der Beklagten lässt sich nicht überprüfen, da die Beklagte keinerlei weitere Informationen betreffend den angeblich verwendeten Botnets liefert. Zudem würden gemäss eigenen Angaben der Beklagten die *Botnets* auch von anderen kriminellen Organisationen verwendet (vgl. act. 33/34 S. 5), womit die Beklagte gleich selbst ihren Standpunkt unterläuft. Darauf weist auch der Gutachter der Klägerin hin, der ausführt, die von der Beklagten angerufenen Übereinstimmungen hätten keinen exklusiven Charakter (vgl. act. 39/1 Rz. 17).

7.3.6.4. Der Gutachter der Beklagten behauptet sodann finanzielle Verflechtungen zwischen "*AC._____ ransomware groups*" und der sanktionierten *P._____*. Die Angreifer (im Original: *threat actors*), die *AB._____* und *AC._____* eingesetzt hätten, hätten einen "*common apparatus of cryptocurrency wallets*" verwendet, um die Lösegeldzahlungen entgegenzunehmen (vgl. act. 33/34 S. 5). Verwirrend ist bereits, dass der Gutachter unversehens von "*AC._____ ransomware groups*" und von *threat actors* spricht. Damit suggeriert er, dass es verschiedene kriminelle Gruppen gibt, welche die Ransomware *AC._____* einsetzten. Die Verbindung der *P._____* zu *AC._____* erscheint damit umso beliebiger. Der Gutachter führt weiter folgendes aus: "*Specifically, by tracking ransomware payments, AE._____ found commonality in the cryptocurrency flow used by both AB._____ and AC._____, which indicated that both strains of malware contributed to a singular crime syndicate facilitated by P._____*" (vgl. act. 33/34 S. 5). Diese Ausführungen sind zudem unsubstanziiert (worauf auch der Gutachter der Klägerin hinweist, vgl. act. 39/1 Rz. 39). Welcher *common apparatus of cryptocurrency wallets to receive payments* wurde verwendet? Welche Lösegeldzahlungen wurden verfolgt und wie? Welche Gemeinsamkeiten im Zahlungsfluss der Kryptowährungen wurden vorgefunden? Wie konkret beziehen sich diese angeblichen Befunde auf den *gegen die Klägerin* mit *K._____* ausgeführten Cyber-Angriff? Die Beklagte hat es versäumt, all diese Umstände, welche die Herstellung einer Verbindung des Cyber-Angriffs zur *P._____* beitragen könnten, näher auszuführen. In ihrer Duplikschrift macht die Beklagte keinerlei Ausführungen zu AC._____. Entsprechend beantwortet die Beklagte weder diese sich ohne weiteres stellenden Fragen noch

offeriert sie auch nur eine einzige Quelle für die Behauptungen im Cyber-Gutachten vom 5. Mai 2022.

7.3.6.5. Insgesamt vermochte die Beklagte die Urheberschaft der *P.*_____ betreffend *AB.*_____ und *AC.*_____ – ausgehend von *Q.*_____ – nicht hinreichend darzutun Kommt hinzu, dass das OFAC weder *AB.*_____ noch *AC.*_____ der *P.*_____ zuordnete.

7.3.6.6. Damit misslingt der Beklagten auch der Nachweis dass hinter *K.*_____ die P._____ als Urheberin stehe, weil *K.*_____ eine nahe Verwandtschaft zu früheren Ransomwares aufweise, die der P._____ zuzurechnen seien. Die Beklagte sowie ihr Gutachter behaupten ohnehin, *K.*_____ sei der Versuch der *P.*_____ gewesen, ihre Identität zu verschleiern, indem sie unter anderem Ransomwares anderer, nicht sanktionierter Gruppen übernommen habe (vgl. act. 32 Rz. 25 und Rz. 29; act. 33/34 S. 6, vgl. auch act. 52 Rz. 17). Das vermag aber eine Urheberschaft der *P.*_____ nicht nachzuweisen. Im Gegenteil: Wenn die *P.*_____ zwecks Verschleierung ihrer Identität Programmteile von Ransomwares anderer Gruppen übernommen haben soll, stellt sich umso mehr die Frage, wie gestützt auf den Programmcode eine Beteiligung der *P.*_____ am Cyber-Angriff gegen die Klägerin überhaupt nachgewiesen werden soll. Damit stünde einzig fest, dass die verschiedenen cyberkriminellen Gruppen auch "fremde" Ransomwares (zumindest teilweise) übernehmen, was eine klare Identifizierung der Urheberschaft allein anhand des Programmcodes weiter erschwert, wenn nicht gar verunmöglicht.

7.4. Fazit

Die Beklagte weist nicht nach, dass hinter dem Cyber-Angriff auf die Klägerin die sanktionierte *P.*_____ stand oder dass diese ein rechtlich relevantes Interesse am Angriff hatte. Eine Beteiligung der *P.*_____ ist nicht *more than likely* dargetan.

8. Höhe und Fälligkeit der Versicherungssumme sowie Verzugszins

8.1. Höhe der Forderung

Die Beklagte konnte kein Interesse der sanktionierten *P.*_____ am Angriff gegen die Klägerin nachweisen. Eine Bestrafung der Klägerin durch das OFAC ist demnach höchst unwahrscheinlich. War die Lösegeldzahlung der Klägerin unter sanktionsrechtlichen Gesichtspunkten nicht zu beanstanden, ist auch die Versicherungsleistung der Beklagten an die Klägerin rechtlich zulässig. Die vertragliche Sanktionsklausel greift nicht. Damit entfällt die einzige Einrede der Beklagten gegen die Forderung der Klägerin, und die Beklagte schuldet die Versicherungssumme. Die vertraglich geschuldete Versicherungssumme beträgt unstreitig [ca. 10 % des versicherten Schadens] (vgl. Erw. 2.1). Die Beklagte ist in Gutheissung der Klage zu verpflichten, der Klägerin [ca. 10 % des versicherten Schadens] zu bezahlen.

8.2. Fälligkeit der Forderung

8.2.1. Parteivorbringen

8.2.1.1. Die Klägerin macht geltend, sie habe mit Schreiben vom tt.mm.Tatjahr der Beklagten eine letztmalige Frist von 14 Tagen zur Bezahlung der Versicherungsleistung angesetzt. Mit unbenutztem Ablauf dieser Frist befinde sich die Beklagte seit dem tt.mm.Tatjahr in Verzug i.S.v. Art. 102 Abs. 1 OR. Mangels abweichender vertraglicher Regelung sei seither ein Verzugszins von 5 % geschuldet (vgl. act. 1 Rz. 135–137).

8.2.1.2. Die Beklagte bestreitet die Fälligkeit der Forderung (und damit auch den verlangten Verzugszins), weil die Klägerin ihren Obliegenheiten gemäss Police und VVG nicht nachgekommen sei. Gemäss Police werde der Anspruch vier Wochen nach Erhalt der Schadenanzeige zur Zahlung fällig, wenn sich das Versicherungsunternehmen von der Richtigkeit des Anspruchs habe überzeugen können,

was der Regelung gemäss Art. 41 Abs. 1 VVG entspreche. Die Police sehe ausdrücklich vor, dass auf Aufforderung des Versicherers hin die Polizei, das FBI oder eine andere zuständige Strafverfolgungsbehörde vom Versicherungsnehmer über die Cyber-Erpressung benachrichtigt werden müsse. Eine solche Aufforderung zur Benachrichtigung sei in der E-Mail vom tt.mm.Tatjahr von der Beklagten an *T._____ Ltd.* (*Coverholder*) zu erblicken. Ein Vertreter des Brokers der Klägerin (*U._____*), AF._____, habe diese E-Mail in Kopie erhalten. Daraus gehe hervor, dass die Beklagte um nähere Informationen über die Freigabe des OFAC ersucht habe. Die Beklagte habe somit deutlich gemacht, dass gemäss der Police eine Meldung an das OFAC zu erfolgen habe. Eine Meldung sei trotz der Aufforderung vom tt.mm.Tatjahr ausgeblieben. Darum könne die Fälligkeit noch gar nicht eingetreten sein (act. 17 Rz. 299–308).

8.2.2. Rechtliches

Gemäss dem anwendbaren Art. 41 Abs. 1 VVG wird die Forderung aus dem Versicherungsvertrag mit dem Ablaufe von vier Wochen, von dem Zeitpunkte an gerechnet, fällig, in dem das Versicherungsunternehmen Angaben erhalten hat, aus denen es sich von der Richtigkeit des Anspruches überzeugen kann. Voraussetzung für den Eintritt der Fälligkeit sind eine gehörige Anspruchsbegründung sowie die Erfüllung allfälliger Obliegenheiten (vgl. SÜSSKIND, Marcel, in: Grolimund/Loacker/Schnyder (Hrsg.), Basler Kommentar zum Versicherungsvertragsgesetz [BSK-VVG], 2. Aufl., Basel 2023, Art. 41 N 8 ff. und N 14 ff.). Zu den Obliegenheiten des Anspruchsberechtigten gehört namentlich die Auskunftspflicht sowie vertraglich vereinbarte Obliegenheiten. Nach der Prüfung der Sachverhalts durch das Versicherungsunternehmen offen bleibende Rechtsfragen vermögen die Fälligkeit nicht hinauszuschieben (vgl. SÜSSKIND, Marcel, in: BSK-VVG, a.a.O., N 21 zu Art. 41).

8.2.3. Würdigung

8.2.3.1. Die Beklagte wendet gegen die Fälligkeit der Forderung einzig eine angebliche Verletzung einer vertraglichen Obliegenheit durch die Klägerin ein. Die

Klägerin hätte – nachdem sie die Beklagte entsprechend aufgefordert habe – das OFAC über den Vorfall informieren müssen. Als Aufforderung sieht die Beklagte eine E-Mail vom tt.mm.Tatjahr (gemeint ist act. 18/4). Es trifft zwar zu, dass in der Police festgehalten wird, dass die Klägerin auf Verlangen der Versicherer verschiedene, von dieser zu bezeichnende Behörden hätte informieren müssen (vgl. act. 18/1 S. 51 von 84 unter C. 1). Wie die Beklagte aber selbst ausführt, richtete sich ihre E-Mail vom tt.mm.Tatjahr gar nicht an die Klägerin oder an dessen Broker. Letzterer erhielt die E-Mail nur in Kopie. Eine direkte Aufforderung an die Klägerin (bzw. an ihren Broker) liegt demnach nicht vor. Auch kann die E-Mail vom tt.mm.Tatjahr ohnehin nicht als Aufforderung verstanden werden, das OFAC zu informieren. Die Beklagte richtete die E-Mail an die *T._____* als *Coverholder* (die *T._____* war letztlich Vertreterin der Beklagten). Sie teilte der *T._____* mit, gestützt auf die Sanktionsklausel dürfe die *T._____* die Beklagte nicht in dieser Sache vertreten (vgl. act. 18/4 S. 1, E-Mail vom tt.mm.Tatjahr, gesendet von AG._____"*Therefore, and pursuant to the sanctions clause at paragraph 34.4 on the coverholder appointment agreement, T._____ may not agree or settle this claim on B._____s behalf*"). Die Beklagte fragte die *T._____* ausserdem an, ob das OFAC eine Freigabe für die Lösegeldzahlung erteilt habe und die Beklagte eine Kopie dieser Freigabe erhalten könnte (vgl. act. 18/4; act. 17 Rz. 306). Diese Anfrage hat mit der Obliegenheit der Klägerin gemäss Police, bestimmte Behörden auf Verlangen der Versicherer zu informieren, nichts zu tun.

8.2.3.2. Die Klägerin (bzw. ihre Vertreter) informierte die Versicherer vorab am tt.mm.2022 über den Cyber-Angriff und am tt.mm.Tatjahr formell (act. 1 Rz. 48; act. 28 Rz. 60 f., Rz. 64 f.). In den bereits erwähnten Schreiben vom tt.mm.Tatjahr und vom tt.mm.Tatjahr behielten sich die Versicherer zwar die Einrede der Sanktionsklausel vor. Sie machten aber nicht geltend, dass die Klägerin ihnen nicht ausreichende Informationen für die Prüfung der Versicherungsdeckung gegeben habe. Im Gegenteil hielten sie fest, dass der Cyber-Angriff grundsätzlich von der Versicherungspolice gedeckt sei. Mithin verfügten die Versicherer über genügende Informationen, um die Versicherungsdeckung im Grundsatz zu bejahen. Die Deliberationsfrist von vier Wochen gemäss Art. 41 VVG begann somit bereits Ende mm.Tatjahr zu laufen, spätestens aber Ende mm.Tatjahr. Die rechtliche Unsicherheit im Zusammenhang mit der Sanktionsklausel ändert daran nichts. Damit

trat nach Ablauf der Deliberationsfrist spätestens im mm.Tatjahr auch die Fälligkeit der Versicherungsleistung ein.

8.3. Verzugszins

8.3.1. Die Klägerin verlangt mit ihrem Rechtsbegehren in der Klageschrift Verzugszins zu 5% auf [ca. 10 % des versicherten Schadens] seit dem tt.mm.Tatjahr+1 mit dem Replikbegehren hingegen seit dem tt.mm.Tatjahr, wobei die Klägerin in der Replik von einem unveränderten Rechtsbegehren ausgeht und sich entsprechend nicht zu dieser "Änderung" äussert (vgl. act. 1 S. 2 und act. 28 S. 2; auch in den zusätzlichen Stellungnahmen nach Aktenschluss beantragt die Klägerin Verzugszins seit tt.mm.Tatjahr, wobei sie stets von einem "unveränderten Rechtsbegehren" ausgeht).

8.3.2. Rechtsbegehren sind wie alle Prozesshandlungen nach Treu und Glauben und im Lichte der Begründung auszulegen (BGE 137 II 313, E. 1.3; BGE 137 III 617, E. 6.2; BGE 135 I 119, E. 4; BGer 5A_140/2020 vom 25. März 2020 E. 1.2; BGer 5A_818/2019 vom 31. Januar 2020, E. 2).

8.3.3. Sowohl aus der Klageschrift als auch aus der Replik geht hervor, dass für die Klägerin weder der tt.mm.Tatjahr (RB Klage) noch der tt.mm.Tatjahr (RB Replik), sondern der tt.mm.Tatjahr massgebend ist (vgl. act. 1 Rz. 28 und act. 28 Rz. 381). Auch aus dem zum Beweis offerierten Mahnschreiben vom tt.mm.Tatjahr geht hervor, dass die Klägerin der Beklagten eine *Zahlungsfrist von 14 Tagen ab Datum des Schreibens*, mithin bis zum tt.mm.Tatjahr, ansetzte, womit der Verzug frühestens am tt.mm.Tatjahr eintreten konnte (vgl. act. 3/21 S. 6). Massgebender Beginn der Laufzeit des Verzugszinses ist damit der tt.mm.Tatjahr.

8.3.4. Unbestritten blieb, dass sich die Beklagte seit dem tt.mm.Tatjahr in Verzug befindet, sofern die klägerische Forderung fällig geworden ist (die Beklagte bestreitet einzig die Fälligkeit der Forderung, jedoch nicht die klägerischen Berechnungen betreffend den Verzugszins für den Fall, dass die Forderung fällig geworden ist, vgl. act. 17 Rz. 299 ff.). Damit befindet sich die Beklagte seit dem tt.mm.Tatjahr in Verzug und schuldet Verzugszins zu 5% auf [ca. 10 % des versicherten Schadens] seit dem tt.mm.Tatjahr.

9. Zusammenfassung der Tat- und Rechtsfragen

9.1. Die Klägerin wurde am tt.mm.Tatjahr Opfer eines Cyberangriffs, der ihre Daten verschlüsselte und ihre Systeme lahmlegte. Erst nach Zahlung eines Lösegelds in Höhe von … [hohe Summe] (damals rund … [grosser Schaden]) erhielt sie wieder Zugriff auf ihre Systeme. Die Parteien hatten einen Versicherungsvertrag betreffend eine Cyberversicherung abgeschlossen, der unbestrittenermassen auch den Schaden aus dem Vorfall vom tt.mm.Tatjahr erfasste. Gemäss der Versicherungspolice steht der Beklagten die Einrede der Sanktionsklausel zu, wenn die Beklagte mit der Zahlung der Versicherungssumme unter anderem gegen U.S. Sanktionsrecht verstossen würde. Die Beklagte verzichtete nicht auf die Einrede der Sanktionsklausel. Ebenso wenig ist die Sanktionsklausel als ungewöhnlich im Sinne der AGB-Rechtsprechung zu qualifizieren, weshalb sie Vertragsinhalt wurde.

9.2. Nach U.S. Sanktionsrecht gilt die Beklagte als sog. *non-U.S.-Person*. Eine *non-U.S.-Person* kann wegen Verstosses gegen das Sanktionsrecht bestraft werden, wenn sie einen Verstoss durch eine *U.S.-Person* verursacht. Ein Verstoss kann unter anderem darin liegen, dass eine Zahlung in U.S. Dollar erfolgt, weil aufgrund des *Clearing-und-Settlements* der Zahlung zwingend ein U.S. Finanzdienstleiter an der Transaktion beteiligt wird. Voraussetzung für einen Verstoss ist allerdings, dass ein Interesse einer sanktionierten Person (SDN) berührt wird. Die blosse Urheberschaft betreffend eine Ransomware stellt kein solches Interesse dar. Hingegen stellt ein Profit der SDN im Zusammenhang mit einer Lösegeldzahlung ein Interesse im Sinne des U.S. Sanktionsrechts dar. Dieses Interesse erfasst auch eine Versicherungsleistung, welche den Schaden aus der Lösegeldzahlung ersetzt, unabhängig davon, ob die Versicherungsleistung an die SDN oder an den Versicherungsnehmer ausbezahlt wird.

9.3. Vorliegend vermag die Beklagte nicht nachzuweisen, dass die von der U.S. Regierung sanktionierte *P.*_____ Urheberin des Cyberangriffs war bzw. vom Cyberangriff gegen die Klägerin profitierte und damit ein Interesse daran hatte. Damit besteht kein Anknüpfungspunkt zum U.S. Sanktionsrecht und eine Bestrafung der Beklagten wegen Verstosses gegen das Sanktionsrecht ist höchst unwahrscheinlich. Entsprechend greift auch die von der Beklagten angerufene Sankti-

onsklausel nicht. Die Klage ist gutzuheissen und die Beklagte zu verpflichten, der Klägerin die Versicherungssumme samt Zinsen zu bezahlen. Damit erübrigt es sich, auf den Eventualantrag der Klägerin (vgl. act. 28 S. 9) einzugehen.

10. Kosten- und Entschädigungsfolgen

10.1. Gerichtskosten

Die Höhe der Gerichtsgebühr bestimmt sich nach der Gebührenverordnung des Obergerichts vom 8. September 2010 (GebV OG; Art. 96 ZPO i.V.m. § 199 Abs. 1 GOG) und richtet sich in erster Linie nach dem Streitwert (§ 2 Abs. 1 lit. a GebV OG). Der Streitwert beträgt [ca. 10 % des versicherten Schadens]; Wechselkurs per Datum Klageeinleitung [25. Januar 2021, act. 1]; Kurs gemäss www.oanda.com). Die Grundgebühr beträgt rund …. Sie kann unter Berücksichtigung des Zeitaufwandes des Gerichts und der Schwierigkeit des Falls ermässigt oder um bis zu einem Drittel, in Ausnahmefällen bis auf das Doppelte, erhöht werden. Die Bearbeitung des vorliegenden Prozesses erwies sich als aufwändig. Die Parteien reichten insgesamt neun Rechtsschriften und 13 Gutachten (sieben Rechtsgutachten zum ausländischen Recht und sechs Gutachten betreffend Ransomware) ein. Weiter hatte sich das Gericht vertieft mir ausländischem Recht auseinanderzusetzen. Die Gerichtsgebühr ist um circa 50 % auf rund … zu erhöhen. Die Gerichtskosten sind ausgangsgemäss der Beklagten aufzuerlegen und vorab aus dem von der Klägerin geleisteten Kostenvorschuss zu beziehen. Der Klägerin ist gegen die Beklagte das entsprechende Rückgriffsrecht zu gewähren.

10.2. Parteientschädigungen

10.2.1. Die Klägerin hat Anspruch auf eine Parteientschädigung für ihre berufsmässige Vertretung. Die Höhe der Parteientschädigung ist nach der Verordnung über die Anwaltsgebühren vom 8. September 2010 zu bemessen (AnwGebV; Art. 105 Abs. 2 ZPO). Grundlage ist auch hier der Streitwert (§ 2 Abs. 1 lit. a AnwGebV). Bei einem Streitwert von [ca. 10 % des versicherten Schadens] beträgt die Grundgebühr rund .... Sie ist mit der Begründung bzw. Beantwortung der Klage verdient. Für die Teilnahme an zusätzlichen Verhandlungen und für weitere notwendige Rechtsschriften wird ein Zuschlag von je höchstens der Hälfte der

Grundgebühr berechnet (§ 11 Abs. 1 und 2 AnwGebV i.V.m. § 4 Abs. 1 AnwGebV). Vorliegend ist aufgrund der Vergleichsverhandlung und der zusätzlichen Rechtsschriften sowie unter Berücksichtigung des Aufwands eine Erhöhung der Grundgebühr um rund 50 % angemessen. Dies führt in Anwendung von §§ 4 und 11 AnwGebV zu einer Parteientschädigung in der Höhe von rund … an die Klägerin.

10.2.2. Die Klägerin verlangt die Parteientschädigung zuzüglich der Mehrwertsteuer. Weder behauptet sie noch weist sie die fehlende Berechtigung zum Vorsteuerabzug nach. Entsprechend ist die Parteientschädigung ohne Mehrwertsteuer zuzusprechen (vgl. Kreisschreiben der Verwaltungskommission des Obergerichts vom 17. Mai 2006 Ziffer 2.1.1 S. 3 unten; abrufbar unter <http://www.gerichte-zh.ch/kreis-schreiben/kreisschreiben.html>; Urteil des Bundesgericht 4A_552/2015 vom 25. Mai 2016, E. 4.5; KassGer ZH vom 19. Juli 2005, ZR 104 [2005] Nr. 76, E. III.2.g S. 293-294 = SJZ 101 [2005] 531).

Das Handelsgericht erkennt:

1. Die Beklagte wird verpflichtet, der Klägerin [ca. 10 % des versicherten Schadens] nebst Zins zu 5% seit dem tt.mm.Tatjahr zu bezahlen.

2. Die Gerichtsgebühr wird festgesetzt auf ….Die Kosten werden der Beklagten auferlegt und teilweise aus dem von der Klägerin geleisteten Kostenvorschuss bezogen. Der Klägerin wird in Höhe des bezogenen Kostenvorschusses das Rückgriffsrecht auf die Beklagte gewährt. Der Fehlbetrag wird direkt von der Beklagten nachgefordert.

3. Die Beklagte wird verpflichtet, der Klägerin eine Parteientschädigung von … zu bezahlen.

4. Schriftliche Mitteilung an die Parteien, an die Klägerin unter Beilage der Doppel von act. 65 und act. 66.

5. Eine bundesrechtliche **Beschwerde** gegen diesen Entscheid ist innerhalb von **30 Tagen** von der Zustellung an beim Schweizerischen Bundesgericht, 1000 Lausanne 14, einzureichen. Zulässigkeit und Form einer solchen Be-

schwerde richten sich nach Art. 72 ff. (Beschwerde in Zivilsachen) oder Art. 113 ff. (subsidiäre Verfassungsbeschwerde) in Verbindung mit Art. 42 und 90 ff. des Bundesgesetzes über das Bundesgericht (BGG). Der Streitwert beträgt ….

Zürich, 9. März 2023

Handelsgericht des Kantons Zürich

Vorsitzende:	Gerichtsschreiber:
Dr. Claudia Bühler	Dr. Giulio Donati