CENTRE DE DROIT
BANCAIRE ET FINANCIER

Cyberangriff

Der Versicherer muss zahlen

Par Célian Hirsch le 23 Oktober 2023

Wie kann sich ein Versicherer dagegen wehren, dass er ein börsennotiertes Unternehmen für einen geschätzten Schaden von fast einer Million nach einem erfolgreichen Cyberangriff entschädigen muss ? Mit der Begründung, die Zahlung würde gegen die US-Sanktionen verstoßen, da der Cyberangriff von russischen Hackern durchgeführt worden sei, gegen die Sanktionen verhängt wurden. Das Handelsgericht Zürich und anschließend das Bundesgericht ließen sich von dieser Argumentation jedoch nicht überzeugen (4A_206/2023).

Im Juli 2020 wurde ein an der NYSE notiertes Unternehmen von der Ransomware Wasted-Locker angegriffen, die unter anderem seine Kundendaten verschlüsselt. Die Angreifer forderten ein Lösegeld von 1’500 Bitcoins (damals rund CHF 13,5 Millionen) für die Herausgabe des Entschlüsselungsschlüssels. Das Unternehmen zahlt den Cyberangreifern schließlich einen Betrag von wahrscheinlich 10 Millionen, um den Schlüssel zu erhalten.

Das Unternehmen verklagt einen seiner Versicherer in Großbritannien, der sich weigert zu zahlen. Der Versicherer behauptet, der Angriff sei von der Evil Corp ausgegangen, russischen Hackern, die auf der Specially Designated Nationals and Blocked Persons-List (SDN-Liste) des Amtes für Auslandsvermögenskontrollen (OFAC) des U.S. Treasury Department (US-Finanzministerium) aufgeführt sind. Die Auszahlung der Versicherungsleistung würde somit gegen die US-Sanktionen verstoßen. Der Versicherer beruft sich insbesondere auf die folgende Vertragsklausel :

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 in 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.

Das von der Gesellschaft angerufene Handelsgericht Zürich gibt der Klage auf Zahlung von fast einer Million US-Dollar statt. Das Gericht ist der Ansicht, dass es dem Versicherer nicht gelungen ist, zu beweisen, dass der Angriff von Evil Corp ausging bzw. dass Evil Corp finanziell von dem Angriff profitiert hätte. Es sei daher höchst unwahrscheinlich, dass der Versicherer bei Zahlung der Versicherungssumme vom OFAC bestraft würde.

Der Versicherer rief das Bundesgericht an, das die vom Versicherer geltend gemachte Klausel zu prüfen hatte.

Erstens reicht die bloße Tatsache, dass die verwendete Software von Evil Corp stammt, d. h. von einem Unternehmen, das auf der SDN-Liste steht, nicht aus, um die Zahlung der Entschädigung zu verweigern. Wie die Vertragsklausel besagt, muss der Versicherer nämlich ein Risiko nachweisen, dass er wegen der Verletzung von US-Sanktionen gerügt wird.

Zweitens überprüft das Bundesgericht, ob es, wie vom Handelsgericht angenommen, höchst unwahrscheinlich war, dass der Versicherer im Falle der Auszahlung der Versicherungssumme vom OFAC bestraft werden würde. Das Bundesgericht nimmt diese Prüfung nur unter dem Aspekt der Willkür vor, da es sich um die Anwendung ausländischen Rechts in einer Geldangelegenheit handelt.

Im kantonalen Urteil stellte das Handelsgericht erstens fest, dass nicht bewiesen sei, dass der Angriff von Evil Corp. ausgegangen sei. Zweitens stellte es fest, dass nicht jeder Einsatz der Wasted-Locker-Software zwangsläufig ein „Interesse“ von Evil Corp im Sinne des US-amerikanischen Sanktionsrechts (property or interests in property) darstellt. Denn selbst wenn Evil Corp der Urheber dieser Software sein sollte, ist nicht auszuschließen, dass sie nun auch von anderen Cyberangreifern verwendet wird, ohne dass Evil Corp ein finanzielles Interesse daran hat. Schliesslich hat das OFAC bislang weder gegen die börsenkotierte Gesellschaft noch gegen die amerikanische Gesellschaft, die das Lösegeld ausgehandelt und bezahlt hat, noch gegen die anderen Versicherer, die ihre Leistungen im Zusammenhang mit diesem Cyberangriff bezahlt haben, ein Verfahren eröffnet.

Das Bundesgericht ist der Ansicht, dass diese Argumentation der Willkür standhält. Es weist insbesondere das Argument des Versicherers zurück, dass jede Nutzung von Wasted-Locker (auch durch Dritte) zu einer verbotenen Transaktion führe, da Evil Corp entweder direkt oder indirekt über Wasted-Locker an dieser Transaktion beteiligt sei. Daher wies das Bundesgericht die Klage des Versicherers ab.

Dieses Urteil ist aus mehreren Gründen interessant und bedarf einiger kurzer Bemerkungen.

Erstens handelt es sich um das erste Urteil des Bundesgerichts zur Zahlung von Lösegeld nach einem Cyberangriff. Diese Problematik war Gegenstand neuerer doktrinärer Veröffentlichungen, in denen insbesondere untersucht wird, ob die Zahlung des Lösegelds durch das Opfer oder den Versicherer eine strafrechtlich relevante Handlung darstellt (vgl. Benhamou Yaniv/Wang Louise, Cyberattaque et ransomware : risques juridiques à payer et assurabilité des rançons, RSDA 2023 S. 80 ff ; Sarrasin Delphine/Pangrazzi Sara/Meyer Pauline, The Legal Risks of Ransomware Payments, PJA 2023 S. 1077 ff.).

Zweitens erinnert das Urteil an den sehr weiten Anwendungsbereich der US-Sanktionen (vgl. auch Emmenegger Susan/Zuber Florence, To Infinity and Beyond : U.S. Dollar-Based Juristiction in the U.S. Sanctions Context, RSDA 2022 S. 114 ff.). In diesem Zusammenhang betonte das Handelsgericht in seinem Urteil, dass das OFAC noch keine Entscheidung zu Cybersanktionen veröffentlicht habe, was die Praxis des OFAC in diesem Bereich nicht verständlich mache.

Schließlich scheiterte der Versicherer in casu daran, den Beweis für die Zurechenbarkeit des

Angriffs an Evil Corp. zu erbringen. Die Beweislast war jedoch geringer als im Schweizer Recht, da als lex causae das Recht der Vereinigten Staaten galt. Dieses sieht jedoch ein „more likely than not“-Kriterium vor (Beweisgrad der Präponderanz). Zum Pech des Versicherers wurden mehrere von ihm vorgelegte Cyberexpertisen vom Handelsgericht als verspätet eingereicht und somit als unzulässig eingestuft (vgl. Art. 229 Abs. 1 lit. b ZPO).
