

19. Dezember 2023

LG Tübingen: Cyber-Versicherer muss trotz veralteter Server zahlen

Bei einem Hacker-Angriff kann sich die Cyber-Versicherung nicht einfach auf veraltete Server und fehlende Sicherheits-Updates berufen, um die Leistung zu verweigern. So entschied das Landgericht Tübingen am 26. Mai 2023 (Az.: 4 O 193/21) im ersten Urteil in Deutschland zu einem Cyber-Versicherungsfall.

Trojaner verschlüsselt 16 von 21 Servern

Ein Mitarbeiter des Unternehmens hatte auf seinem Laptop den Anhang einer E-Mail geöffnet, der als Rechnung getarnt war und einen Verschlüsselungstrojaner (Ransomware) enthielt. Der Laptop war über einen VPN-Tunnel mit dem Unternehmensnetzwerk verbunden. So konnte sich die Schadsoftware auf 16 der insgesamt 21 Server ausbreiten. Diese wurden vollständig verschlüsselt und der Großteil der IT-Infrastruktur des Unternehmens lahmgelegt. Durch die lange Betriebsunterbrechung und die Monate andauernde Wiederherstellung der Daten entstanden Schäden von knapp 3 Millionen Euro.

Um sich gegen solche Schäden abzusichern, hatte das Unternehmen eine Cyber-Versicherung abgeschlossen. Der Versicherer bzw. der verantwortliche Assekuradeur hatte nach einer Beweisaufnahme vor Vertragsabschluss den Eindruck vermittelt, dass keine hohen Anforderungen an die IT-Sicherheit gestellt würden. Nachdem das Unternehmen jedoch den Schaden gemeldet hatte, verweigerte die Versicherung die Zahlung und erklärte zudem den Rücktritt vom Vertrag. Die Begründung: Der Versicherungsnehmer habe seine vorvertraglichen Anzeigepflichten verletzt und Risikofragen arglistig falsch beantwortet. Denn mehrere der betroffenen Server waren so alt, dass Microsoft dafür schon seit Jahren keine Sicherheits-Updates mehr anbot.

Unternehmen soll Risikofrage arglistig fasch beantwortet haben

Dem Versicherungsnehmer war vor Vertragsabschluss unter anderem die Gefahrfrage gestellt worden, ob verfügbare Sicherheits-Updates ohne schuldhaftes Zögern durchgeführt würden und für die Software des IT-Systems lediglich Produkte eingesetzt würden, für die der Hersteller Sicherheits-Updates bereitstelle (z. B. Betriebssysteme, Virens Scanner, Firewall, Router und NAS-Systeme). Das Unternehmen hatte dies bejaht. Dabei waren 11 der 21 Server zu dem Zeitpunkt veraltet und Microsoft stellte schon länger keine Sicherheits-Updates mehr dafür zur Verfügung.

Dies führte die Cyber-Versicherung als Grund an, um die Übernahme des Schadens zu verweigern. Weil das Unternehmen die Frage arglistig falsch beantwortet habe, erklärte der Versicherer zudem den Rücktritt vom Vertrag. Hilfsweise machte er Leistungsfreiheit wegen einer Gefahrerhöhung und vorsätzlicher Herbeiführung des Versicherungsfalls geltend.

LG Tübingen fällt erstes Urteil zu Cyber-Versicherung

Das Landgericht Tübingen ließ das jedoch nicht gelten. Nach Auffassung der Richter war der Versicherer weder wegen einer vorvertraglichen Anzeigepflichtverletzung noch wegen einer Gefahrerhöhung leistungsfrei geworden.

Das Gericht stellte fest, dass das klagende Unternehmen die Gefahrfrage zu den Sicherheits-Updates allenfalls fahrlässig falsch beantwortet habe. Die Versicherung bzw. der Assekuradeur habe vor Vertragsschluss den Eindruck vermittelt, dass keine besonders hohen Anforderungen an die IT-Sicherheit gestellt würden. Dieses Verhalten schließe Vorsatz und Arglist des Versicherungsnehmers aus. Es sei am Versicherer selbst gewesen, durch weitere entsprechende Risikofragen das Vorliegen zusätzlicher Sicherheitsmaßnahmen zu klären.

Außerdem habe der Versicherer von den alten Servern gewusst. Denn der Assekuradeur sei streng genommen ein Versicherungsvertreter mit besonderer Vollmacht. Dementsprechend seien dessen Äußerungen und Kenntnisse der Versicherung zuzurechnen.

Veraltete sowie moderne Server von Trojaner betroffen

Um zu klären, ob der Schaden durch die veralteten Server und fehlenden Sicherheits-Updates erst möglich gemacht bzw. das Risiko dadurch erhöht wurde, holte das LG Tübingen ein Sachverständigengutachten ein. Dieses kam zu dem Ergebnis, dass alte wie neue Server gleichermaßen von der Schadsoftware betroffen waren. Bei dem Cyberangriff sei eine vorhandene Schwachstelle von Windows ausgenutzt worden, die unabhängig von der Aktualität des jeweiligen Systems bestünde. Die fehlenden Sicherheits-Updates hätten also keinen Einfluss, weder auf Eintritt noch auf Höhe des Schadens, gehabt.

Damit gelang dem Kläger ein sog. Kausalitätsgegenbeweis in Bezug auf die Anzeigepflichtverletzung, denn er konnte gemäß § 21 Abs. 2 Satz 1 VVG nachweisen, dass eine mögliche Falschbeantwortung der Risikofragen weder die Ursache für den Eintritt des Versicherungsfalls noch für dessen Umfang war. Damit wurde auch das Argument des Versicherers entkräftigt, er sei wegen einer Gefahrerhöhung leistungsfrei.

Gefahrenlage bestand schon bei Vertragsabschluss

Auch den Einwand der Versicherung, das klagende Unternehmen habe den Versicherungsfall vorsätzlich, mindestens aber grob fahrlässig herbeigeführt, ließ das Landgericht nicht gelten. Zwar habe es technische Maßnahmen gegeben, die den Schaden trotz veralteter Software hätten verhindern oder zumindest verringern können. Das sei jedoch nicht relevant, wenn die Gefahrenlage bei Vertragsschluss bereits bestand, was hier der Fall war.

Im Schadenfall versuchen Versicherungen immer wieder, die Leistung zu verweigern und werfen den Versicherungsnehmern angebliche Vertragsverstöße vor. In der Anwaltskanzlei Lenné konnten wir schon vielen Mandanten dabei helfen, ihre Ansprüche gegenüber den Versicherern doch noch durchzusetzen. Wenn auch Ihre Versicherung die Übernahme eines Schadensfalls verweigert, beraten wir Sie gern im Zuge eines kostenlosen Erstgesprächs.

[Guido Lenné](#)

Rechtsanwalt aus der Anwaltskanzlei Lenné.

Rechtsanwalt Lenné ist auch Fachanwalt für Bank- und Kapitalmarktrecht.

Wir helfen Ihnen gerne! [Kontaktieren](#) Sie uns. Oder vereinbaren Sie [hier online einen Termin](#) für eine telefonische kostenfreie Erstberatung.

- [Facebook](#)
- [Twitter](#)
- [WhatsApp](#)
- [E-mail](#)

[Zurück](#)