NACHRICHTEN AG

22. August 2024

Gericht in Kiel: Cyberversicherung weicht wegen arglistiger Täuschung

Ein norddeutsches Unternehmen verliert Rechtsstreit um Cyberversicherung wegen arglistiger Täuschung und falscher Sicherheitsangaben.

In einem bedeutenden Rechtsstreit hat ein Unternehmen in Norddeutschland kürzlich den Kürzeren gezogen: Das Landgericht hat entschieden, dass die Cyberversicherung des Unternehmens nicht zahlen muss. Der Grund dafür ist eine arglistige Täuschung seitens des Versicherungsnehmers. Bei der Antragstellung gab das Unternehmen falsche Angaben zu den Sicherheitsprotokollen seines IT-Systems an, was zu der Entscheidung des Gerichts führte, die Versicherung von ihrer Zahlungspflicht zu entbinden.

Das besagte Unternehmen, das an 16 Standorten aktiv ist, hatte eine Cyberversicherung bei der Beklagten abgeschlossen. In den Risikofragen des Antrags versicherte es, dass alle Computer mit aktueller Sicherheitssoftware und regelmäßigen Updates ausgestattet seien. Diese Aussagen erwiesen sich als falsch. Bei einer Überprüfung stellte sich heraus, dass im IT-System mehrere gravierende Mängel vorlagen, unter anderem veraltete Server und fehlender Virenschutz, die die Anfälligkeit für Cyberangriffe deutlich erhöhten. Diese unzureichenden Sicherheitsvorkehrungen wurden vom Unternehmen verschwiegen oder zumindest unzureichend dargestellt.

Die Details des Urteils

Das Gericht befand, dass die falschen Angaben als arglistige

Täuschung gewertet werden mussten. Ein Mitarbeiter des Unternehmens ließ sich dazu hinreißen, die Fragen ohne fundierte Kenntnisse zu beantworten und täuschte damit den Versicherer hinsichtlich des tatsächlichen Risikos, das das Unternehmen darstellte. Infolgedessen erklärte die Versicherung ihren Rücktritt vom Vertrag und stellte die Zahlung von Schadensersatz in Höhe von mehr als 424.000 Euro ein. Es ist jedoch wichtig zu betonen, dass das Urteil des Landgerichts Kiel (5 O 128/21) bisher nicht rechtskräftig ist, was potenziell juristische Folgen für beide Parteien haben könnte.

Der Sachverhalt wirft grundlegende Fragen zur Verantwortung von Unternehmen auf, die Cyberversicherungen abschließen. Sicherheit ist in der heutigen digitalen Landschaft entscheidend, und ein Versäumnis in der richtigen Darstellung von Risiken kann nicht nur teuer werden, sondern auch das gesamte Geschäft gefährden. Die Entscheidung des Landgerichts Kiel könnte als abschreckendes Beispiel für andere Unternehmen dienen, die mit den Gedanken spielen, ungenaue Informationen bei Versicherungsanträgen anzugeben.

Vergleich mit einem anderen Gerichtsurteil

Interessanterweise gibt es Parallelen zu einem Fall, den das Landgericht Tübingen behandelt hat. Auch dort wurde der Versicherer von seiner Leistungspflicht befreit, weil auch dort veraltete Server und fehlende Sicherheitsupdates im Einsatz waren. Bei näherer Betrachtung stellte ein Gutachten jedoch fest, dass die alten und neuen Server gleichermaßen durch die heruntergeladene Schadsoftware gefährdet waren. Zudem kamen die Richter in Tübingen zu dem Schluss, dass die fehlenden Sicherheitsupdates weder den Eintritt noch die Höhe des Schadens wesentlich beeinflussten.

Diese unterschiedlichen Urteile verdeutlichen die Komplexität im Umgang mit Cyberversicherungen und den jeweiligen Pflichten der Versicherten. Die wesentlichen Erkenntnisse aus Kiel und Tübingen werden möglicherweise im künftigen

Versicherungsrecht diskutiert werden, insbesondere in Bezug auf die Verantwortung von Unternehmen und die Beweislast im Falle von Cybervorfällen.

Wichtige Implikationen für Unternehmen

Die jüngsten Entwicklungen rund um Cyberversicherungen und die damit verbundenen rechtlichen Auseinandersetzungen sind ein klares Signal für Unternehmen, die ihren digitalen Schutz stärken wollen. Die Notwendigkeit, präzise und ehrliche Angaben in Versicherungsanträgen zu machen, könnte nicht klarer sein. Jedes Unternehmen, unabhängig von Größe oder Branche, muss sich der Risiken bewusst sein und diese proaktiv managen.

Unternehmen sind gut beraten, ihre IT-Sicherheitsvorkehrungen regelmäßig zu überprüfen und gegebenenfalls anzupassen. In einer Zeit, in der Cyberangriffe zunehmend an Häufigkeit und Komplexität zunehmen, ist es nicht nur ratsam, eine Cybersicherheitsstrategie zu implementieren, sondern auch sicherzustellen, dass diese Ansprüche in den Versicherungsanträgen transparent und korrekt dargestellt werden.

Cyberversicherungen sind in den letzten Jahren aufgrund der steigenden Anzahl von Cyberangriffen und Datendiebstählen zunehmend in den Fokus von Unternehmen gerückt. Immer mehr Firmen in Deutschland, besonders im Mittelstand, sichern sich gegen die finanziellen Folgen solcher Angriffe ab. Laut einer Studie des Digitalverbands Bitkom schätzen 90 Prozent der Unternehmen die Gefahr von Cyberangriffen als hoch ein, jedoch lediglich 25 Prozent nutzen überhaupt eine Cyberversicherung. Dies zeigt, dass trotz eines hohen Bewusstseins für die Risiken oft keine adäquate Absicherung getroffen wird.

Im aktuellen Fall gibt es einige grundlegende Faktoren, die in der Diskussion um Cyberversicherungen und deren Wirksamkeit entscheidend sind. Neben den rechtlichen Aspekten, wie sie in

dem Urteil des Landgerichts Kiel behandelt wurden, spielen auch die technischen Sicherheitsvorkehrungen eine zentrale Rolle. Einrichtungen müssen sicherstellen, dass ihre IT-Systeme stets auf dem neuesten Stand sind, um im Schadensfall nicht in ähnliche Schwierigkeiten wie das betroffene Unternehmen zu geraten.

Sicherheitsstandards und rechtliche Rahmenbedingungen

Der rechtliche Rahmen für Cyberversicherungen in Deutschland ist durch das Versicherungsvertragsgesetz (VVG) geregelt. Demnach müssen Versicherungsnehmer die Wahrheitsgemäßigkeit ihrer Angaben sicherstellen. Im vorliegenden Fall hatte das Unternehmen die Anforderungen nicht erfüllt, was zu den rechtlichen Konsequenzen führte. Eine präventive Herangehensweise, also die regelmäßige Überprüfung und Aktualisierung der IT-Sicherheitsstandards, könnte viele rechtliche Probleme im Vorfeld vermeiden.

Darüber hinaus ist der europäische Datenschutzrecht, insbesondere die Datenschutz-Grundverordnung (DSGVO), zu beachten. Unternehmen sind gesetzlich verpflichtet, angemessene technische und organisatorische Maßnahmen zu ergreifen, um den Schutz personenbezogener Daten zu gewährleisten. Hierzu zählen regelmäßige Sicherheitsupdates und die Anwendung neuester Sicherheitssoftware. Versäumnisse in diesen Bereichen können nicht nur zu finanziellen Einbußen durch Schadensersatzforderungen führen, sondern auch zu erheblichen Bußgeldern.

Fazit und Ausblick

Die Konsequenzen solcher Urteile können weitreichend sein und Unternehmen dazu anregen, ihre Sicherheitsstandards zu verbessern sowie die Wahrhaftigkeit ihrer Angaben gegenüber Versicherungen ernst zu nehmen. Eine hohe Sensibilisierung für

Cyberrisiken, gepaart mit einer transparenten Kommunikation mit Versicherern, kann dazu beitragen, zukünftige Streitigkeiten zu vermeiden. Gleichzeitig müssen Versicherungsunternehmen ihre Policen so gestalten, dass sie den aktuellen Bedrohungen gerecht werden und sowohl den Unternehmen als auch den Versicherern einen klaren und fairen Rahmen bieten.

Details