

LEGAL UPDATE VERSICHERUNGSRECHT  
KÖLN, 24.04.2025

# Cyber-Versicherung: Kein Schutz bei unsorgfältiger Beantwortung der Risikofragen

Vladimir Krahn

Angesichts der ständig zunehmenden kriminellen Cyber-Angriffe hat sich die Cyber-Versicherung in den letzten Jahren selbst für kleine und mittlere Unternehmen zu einer Must-have-Versicherung entwickelt. Gerade Unternehmen, die mit personenbezogenen Daten ihrer Kunden arbeiten, sind auf wirksamen Schutz einer Cyber-Versicherung angewiesen. Diese kommt nach einem Cyber-Angriff nicht nur für Schäden an der eigenen Infrastruktur (etwa: Hardware) auf, sondern auch für Schäden, die Dritte gegen das Unternehmen geltend machen.

Voraussetzung für die Erlangung eines wirksamen Versicherungsschutzes ist allerdings nicht nur der Abschluss eines Versicherungsvertrags bei einem renommierten Versicherer. Vielmehr zeigt die Analyse der obergerichtlichen Rechtsprechung, dass Unternehmen im Vorfeld des Abschlusses des Versicherungsvertrags, nämlich bei der Beantwortung der Risikofragen des Versicherers, besonders sorgfältig agieren müssen. Eine aktuelle Entscheidung des Schleswig-Holsteinischen Oberlandesgerichts (Beschluss vom 8. Januar 2025 – 16 U 63/24) veranschaulicht, dass bereits die nachlässige Beantwortung von Fragen zum Sicherheitsstand des IT-Netzwerks nicht nur zu einer Kürzung, sondern zu einem vollständigen Verlust des Versicherungsschutzes führen kann.

## Welche Risikofragen des Versicherers beantwortete die Versicherungsnehmerin falsch?

Bei der Anbahnung des Vertragsabschlusses beantwortete der Leiter der IT-Abteilung der Klägerin, die einen Holzgroßhandel mit mehr als 400 Mitarbeitern und mit der Möglichkeit einer Online-Bestellung über einen Webshop betreibt, folgende Risikofragen des Versicherers mit einem „Ja“, wobei er zuvor keine näheren Erkundigungen und / oder eine Systemprüfung vornahm:

- Alle stationären und mobilen Arbeitsrechner sind mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet.
- Verfügbare Sicherheitsupdates werden ohne schuldhaftes Zögern durchgeführt und für die Software, die für den Betrieb des IT-Systems erforderlich ist, werden lediglich Produkte eingesetzt, für die vom Hersteller Sicherheitsupdates bereitgestellt werden (dies betrifft v.a. Betriebssysteme, Virens Scanner, Firewall, Router, NAS-Systeme).

Nach einem Cyber-Angriff auf die Systeme der Klägerin ließ der Versicherer eine forensische Analyse durchführen. Dabei stellte sich u. a. heraus, dass die Klägerin für den Betrieb ihres Webshops einen „End of Life“-Server eingesetzt hatte, sodass Software- und Sicherheitsupdates seit geraumer Zeit nicht mehr durchgeführt wurden. Außerdem fehlten ein Virens Scanner bzw. eine Antiviren-Software. Schließlich befand sich der von der Klägerin eingesetzte Domain-Controller, der den Zugang von über 70 Nutzern regelte, zum Zeitpunkt des Cyber-Angriffs noch im Auslieferungszustand.

Nach den Feststellungen der Forensik sah sich der Versicherer durch die Falschbeantwortung der Risikofragen arglistig getäuscht. Bei Kenntnis der wahren Sachlage, so der Versicherer, hätte er keinen Versicherungsvertrag mit der Klägerin geschlossen. Aus diesem Grund erklärte er die Anfechtung des Versicherungsvertrags und lehnte die Leistung einer finanziellen Entschädigung an die Klägerin ab.

### Die Entscheidung des Schleswig-Holsteinischen Oberlandesgerichts

Das Schleswig-Holsteinische Oberlandesgericht gab dem Versicherer Recht. Es bestätigte die erstinstanzliche Entscheidung des Landgerichts Kiel (Urteil vom 23. Mai 2024, Az. 5 O 128/21), wonach der Versicherer den Versicherungsvertrag wegen arglistiger Täuschung der Klägerin vor Vertragsschluss wirksam angefochten hat und daher keine Entschädigung an die Klägerin leisten musste.

Das OLG stellte fest, dass der IT-Leiter der Klägerin die vorgenannten Risikofragen des Versicherers objektiv falsch beantwortet hatte. Zwar verteidigte sich die Klägerin u. a. damit, dass eine der Risikofragen sich ausdrücklich nur auf Arbeitsplatzrechner und nicht auf Server bezogen habe.

Auf den Arbeitsplatzrechnern seien Virens Scanner installiert gewesen. Dieser Argumentation folgte das OLG jedoch nicht. Wer eine Cyber-Versicherung zur Sicherung seines IT-Netzwerks abschließen wolle, wird den Begriff des Arbeitsrechners weiter verstehen als den bloßen Arbeitsplatzrechner.

Ferner sah das OLG den Vorwurf der Arglist der Klägerin bei der Beantwortung der Risikofragen als begründet an. Der Klägerin helfe nicht, dass ihr IT-Leiter bei der Beantwortung der Fragen nicht positiv an die vorgenannten Sicherheitslücken dachte. Es komme insbesondere nicht darauf an, ob der IT-Leiter der Klägerin bei der Beantwortung der Risikofragen in dem Glauben gewesen sei, es sei alles in Ordnung – etwa, weil externe Unternehmer in die Gestaltung der Serverlandschaft eingebunden waren und auch im Übrigen Mitarbeiter der Klägerin mit der Sicherheit der IT-Systeme betraut waren. Gutgläubig, so das Gericht, war die Klägerin damit nicht.

Im Gegenteil: Der IT-Leiter der Klägerin habe annehmen müssen, dass der Versicherer auf seine dezidierten Fragen zu Aspekten der IT-Sicherheit keine Antworten nach Glauben oder Meinen erwartete. Daher entspreche die Erklärung zu einzelnen Aspekten der IT-Sicherheit auf „gut Glück“ ohne tatsächlich hinreichende Kenntnisse einer bewussten Unrichtigkeit; (allein) darin sah der Senat eine arglistige Täuschung des Versicherers.

### Bedeutung für die Praxis: Worauf müssen Unternehmen beim Abschluss einer Cyber-Versicherung achten?

Der Entscheidung des Schleswig-Holsteinischen Oberlandesgerichts kommt eine hohe praktische Bedeutung zu. Nach einem Cyber-Angriff wird der Versicherer im Regelfall eine forensische Analyse durchführen lassen.

Dabei wird der Versicherer nicht nur die Ursachen für den Cyber-Angriff ermitteln lassen; vielmehr wird der Versicherer auch versucht sein, bei der Systemanalyse objektiv falsche Antworten des Versicherungsnehmers auf die im Vorfeld des Vertragsschlusses gestellten Risikofragen zu identifizieren – gerade, wenn es um erhebliche Geldbeträge als Versicherungsleistung gehen sollte. Fehlerhafte Antworten zu zentralen Fragen wie der Sicherheit des IT-Netzwerks werden künftig dazu führen, dass manch ein Versicherer die Anfechtung der abgeschlossenen Cyber-Versicherungsverträge erklären wird, um keine Zahlung leisten zu müssen. Der Versicherungsnehmer wird einen jahrelangen Rechtsstreit mit ungewissem Ausgang führen müssen.

Um dem Risiko des vollständigen Verlusts des Cyber-Versicherungsschutzes vorzubeugen, raten wir den Unternehmen Folgendes:

- Sämtliche Risikofragen der Versicherer im Vorfeld des Vertragsschlusses sollten mit größtmöglicher Sorgfalt beantwortet werden.
- Soweit die mitunter offen gestalteten Fragen zu Verständnisschwierigkeiten führen oder doppeldeutig erscheinen mögen, sollte auf keinen Fall die für den Versicherungsnehmer günstigste Verständnismöglichkeit zur Grundlage der

Beantwortung gemacht werden – stattdessen müssen Rückfragen an den Versicherer gestellt werden.

- Stellt der Versicherer dezidierte Risikofragen zu Aspekten der IT-Sicherheit (wie etwa zur Verfügbarkeit von Firewalls und Virenschaltern), müssen vor der Beantwortung der Fragen konkrete Erkundigungen in Form einer Systemüberprüfung eingeholt und dokumentiert werden. Unterbleibt die Dokumentation, droht dem Versicherungsnehmer im Deckungsprozess gegen den Versicherer Beweisnot, um den Einwand der Arglist zu entkräften.
- Sollte für Ihr Unternehmen aufgrund des konkreten Geschäftsmodells eine besonders hohe Gefahr krimineller Cyber-Angriffe bestehen, lohnt sich eine anwaltliche Beratung bereits im Vorfeld des Abschlusses des Versicherungsvertrags – etwa bei der Beantwortung der Risikofragen des Versicherers.
- Unternehmen sollten vor Abschluss des Cyber-Versicherungsvertrags nicht nur die konkreten Konditionen wie Prämienleistungen und den Deckungsumfang im Auge haben. Vielmehr ist auch ein Vergleich der Komplexität der Risikofragenkataloge als Auswahlkriterium zu berücksichtigen

**Hinweis**

Dieser Überblick dient ausschließlich der allgemeinen Information und kann konkreten Rechtsrat im einzelnen Fall nicht ersetzen. Sprechen Sie bei Fragen bitte Ihren gewohnten Ansprechpartner bei GÖRG bzw. den Autor Vladimir Krahn unter +49 221 33660-418 oder VKrahn@GO-ERG.de an. Informationen zum Autor finden Sie auf unserer Homepage [www.goerg.de](http://www.goerg.de).

Wir verwenden das generische Maskulinum und sehen von einer Nennung aller Geschlechtsidentitäten ab, damit die ser Text besser lesbar ist, und meinen damit ausdrücklich jeden in jeder Geschlechtsidentität.

## Unsere Standorte

GÖRG Partnerschaft von Rechtsanwälten mbB

**BERLIN**

Kantstr. 164, 10623 Berlin  
Tel. +49 30 884503-0  
Fax +49 30 882715-0

**HAMBURG**

Alter Wall 20 - 22, 20457 Hamburg  
Tel. +49 40 500360-0  
Fax +49 40 500360-99

**FRANKFURT AM MAIN**

Ulmenstr. 30, 60325 Frankfurt am Main  
Tel. +49 69 170000-17  
Fax +49 69 170000-27

**KÖLN**

Kennedyplatz 2, 50679 Köln  
Tel. +49 221 33660-0  
Fax +49 221 33660-80

**MÜNCHEN**

Prinzregentenstr. 22, 80538 München  
Tel. +49 89 3090667-0  
Fax +49 89 3090667-90