WILHELM

RECHTSANWÄLTE

Obliegenheiten in der Cyberversicherung

Von Updates, Backups und problematischen Klauseln

www.wilhelm-rae.de

Juni 2023

WILHELM

RECHTSANWÄLTE

Von Dr. David Ulrich, LL.M. (Kent)

Obliegenheiten in der Cyberversicherung

Von Updates, Backups und problematischen Klauseln

Der Fluss an Meldungen über erfolgreiche Cyberangriffe auf Unternehmen in Deutschland reißt derzeit nicht ab. Richtigerweise raten deshalb Cyberversicherer ebenso wie Versicherungsmakler und Cyber-Experten zu umfassender Risikovorsorge durch IT-Sicherheitsmaßnahmen.

Versicherer belassen es jedoch nicht bei mahnenden Worten. Durch hohe Anforderungen an die IT der versicherten Unternehmen sowie vertragliche Obliegenheiten schaffen die Cyberversicherer ein Schlupfloch, um Leistungen im Schadenfall zu kürzen.

In der Cyberversicherungs-Praxis erweisen sich viele Obliegenheiten jedoch als problematisch. Zweifel an der Wirksamkeit mancher Formulierungen geben Anlass zur kritischen Auseinandersetzung mit marktüblichen Klauseln. Wenn der Cyberversicherer dem Versicherungsnehmer eine Obliegenheitsverletzung vorwirft, lohnt sich ein zweiter Blick: Ist die Obliegenheit überhaupt wirksam vereinbart? Wer hat die Obliegenheit eigentlich verletzt? Und war die vermeintliche Obliegenheitsverletzung überhaupt für den Schadeneintritt kausal?

Insbesondere die sogenannte *Update-Obliegenheit* und die *Backup-Obliegenheit* sorgen in der Praxis regelmäßig für Streit.

Beispielszenarien zeigen die Grenzen dieser Obliegenheiten auf:

1. Die Update-Obliegenheit

Beliebter Anknüpfungspunkt für eine vermeintliche Obliegenheitsverletzung ist die sog. *Update-Obliegenheit*.

Die Update-Obliegenheit kann etwa wie folgt lauten:

„Updates sind unverzüglich zu installieren."

Nicht unverzüglich installierte Updates stellen demnach eine Obliegenheitsverletzung dar, die den Versicherer zur quotalen Leistungskürzung berechtigt. In der Theorie ist diese Anforderung einleuchtend. In der Praxis können aber je nach Ausgestaltung der Obliegenheit und der Begleitumstände des Einzelfalls Zweifel an einem Leistungskürzungsrecht des Versicherers bestehen.

1.1 Vorrang der Individualvereinbarung?

Die besonderen Bedingungen oder die vorvertragliche Korrespondenz können die Update-Obliegenheit verdrängen.

Beispielszenario 1 (Kenntnis des Versicherers):

Das Unternehmen übersendet umfangreiche Unterlagen zur eigenen IT-Struktur. Aus den übersendeten Unterlagen folgt transparent, dass das Unternehmen Updates erst dann vornimmt, wenn das Update mit anderen Anwendungen kompatibel ist und deswegen zu keiner Betriebsunterbrechung führt. Der Versicherer nimmt diese Information zur Kenntnis und legt dennoch seine standardmäßigen AVB zugrunde. Diese standardmäßigen AVB enthalten die Update Obliegenheit. Nach einer Cyberattacke wendet der Versicherer ein, dass das Unternehmen ein verfügbares Update nicht unverzüglich installierte. Das Unternehmen hält dem entgegen, dass das Update zu einer Betriebsunterbrechung geführt hätte und erst nach weiteren Installationen mit anderen Anwendungen kompatibel gewesen wäre.

Dokumentierte Vereinbarungen mit dem Versicherer können vertragliche Obliegenheiten verdrängen.

Der Versicherer kann im Beispielszenario 1 keine Obliegenheitsverletzung einwenden, da er wusste, dass das Unternehmen Updates erst dann vornimmt, wenn keine Betriebsunterbrechung mehr droht. Dementsprechend ist die Update-Obliegenheit dahingehend auszulegen, dass *Updates dann durchzuführen sind, sobald das Update zu keiner Betriebsunterbrechung führt*.

Für das Unternehmen ist daher wichtig, die vorvertragliche Korrespondenz mit dem Versicherer umfassend zu dokumentieren, um ggf. die Kenntnis des Versicherers von der vorvertraglichen Risikosituation zu beweisen.

Selbst wenn ein Gericht entgegen der hier vertretenen Meinung keinen Vorrang der Individualvereinbarung und damit eine Obliegenheitsverletzung annimmt, kann die Kenntnis des Versicherers das Verschulden ausschließen und ein Leistungskürzungsrecht scheidet aus.[1]

1.2 Unangemessenheit der Update-Obliegenheit?

Weitere Voraussetzung für ein Leistungskürzungsrecht des Versicherers ist, dass die vermeintlich verletze Obliegenheit wirksam vereinbart wurde.

Der Versicherer kann daher nur dann eine Verletzung der Update-Obliegenheit vorwerfen, wenn

[1] MüKo VVG[3], § 28 VVG, Rn. 251, m.w.N.

die Update-Obliegenheit i.S.v. § 307 Abs. 1, 2 BGB angemessen ist.

Beispielszenario 2 (Inkompatibilität mit weiteren Anwendungen):

Ein Unternehmen verfügt über einen vollautomatisierten Produktionsprozess. Dem vollautomatisierten Produktionsprozess liegen verschiedene Anwendungen unterschiedlicher Anbieter zugrunde. Der Anbieter der Anwendung Y veröffentlicht am 1. November ein Update. Dieses Update führt jedoch dazu, dass die Anwendung Y nicht mehr mit den anderen notwendigen Anwendungen kompatibel ist. Das Unternehmen steht somit vor der Frage: Weiterlaufen des Betriebs ohne Update oder unversicherte Betriebsunterbrechung bis eine Komptabilität hergestellt ist?

Versicherungsnehmer sollten prüfen, ob die Obliegenheiten überhaupt angemessen sind.

Gegen eine Angemessenheit der Update-Obliegenheit spricht, dass der Versicherungsnehmer durch eine Update-Obliegenheit zu einer kostspieligen Betriebsunterbrechung verpflichtet wäre. Solche kostspieligen Betriebsunterbrechungen entstehen immer dann, wenn das Update zu einer Inkompatibilität mit anderen für den Betrieb zwingend notwendigen Anwendungen führt.

Die Update-Obliegenheit verletzt somit einseitig die Interessen des Versicherungsnehmers des Versicherungsnehmers und ist demnach i.S.v. § 307 Abs. 1, Abs. 2 BGB unangemessen und unwirksam.

2. Die Backup-Obliegenheit

Eine weitere praxisrelevante Obliegenheit ist die *Backup-Obliegenheit.*

Die Backup-Obliegenheit kann wie folgt lauten:

„Der Versicherungsnehmer ist verpflichtet, mindestens tägliche Datensicherung i.S.e. Offline-Backups durchzuführen.“

Auch hier gilt, Unternehmen sollten schon allein aus eigenem Interesse regelmäßige Backups ihrer Daten erstellen. Die Übersetzung einer sinnvollen technisch-organisatorischen Maßnahme in eine unangemessene und unbestimmte versicherungsvertragliche Obliegenheit ist jedoch problematisch:

2.1 Vorrangige Individualvereinbarung?

Insbesondere bei der Backup-Obliegenheit lohnt sich eine Prüfung vorrangiger Individualvereinbarungen.

Beispielszenario 3 (Kenntnis des Versicherers):

Im Rahmen der Vertragsanbahnung legt das Unternehmen die vorhandene IT-Struktur dar. Hierzu übersendet das Unternehmen u.a. Pläne aus denen folgt, dass das Unternehmen wöchentlich Backups durchführt. Der Versicherer versichert nach Erhalt dieser IT-Unterlagen das Cyberrisiko des

Unternehmens mit einer standardmäßigen Obliegenheit zur täglichen Durchführung von Backups. Nach einer Cyberattacke verweigert der Versicherer die Regulierung, weil das Unternehmen die Backup-Obliegenheit verletzt habe.

Im Beispielszenario kann sich der Versicherer nicht auf die Verletzung der Backup-Obliegenheit berufen. Auch hier ist eine Individualvereinbarung vorrangig.

Durch die vorvertragliche Korrespondenz war dem Versicherer bekannt, dass das Unternehmen nicht die standardmäßige Backup-Obliegenheit zur Datensicherung erfüllt. Versichert der Versicherer trotz Kenntnis von dieser Abweichung das Cyberrisiko, ist die Obliegenheit zur täglichen Datensicherung verdrängt. Das Unternehmen ist somit nur verpflichtet, die dem Versicherer bei Vertragsschluss bekannte Backupstruktur aufrechtzuerhalten. Nur wenn der Versicherer die tägliche Datensicherung mittels Auflage zur Bedingung für den Versicherungsschutz gemacht hätte, wäre die Backup-Obliegenheit wirksam vereinbart.

2.2 Unangemessene Backup-Obliegenheit?

Selbst wenn keine vorrangige Individualvereinbarung vorliegt, kann die dargestellte Backup-Obliegenheit den Versicherungsnehmer unangemessen benachteiligen und daher unwirksam sein (§ 307 Abs. 1, 2 BGB), wie folgende Szenarien zeigen:

Beispielszenario 4 (Datensicherung auch an Sonn- und Feiertagen):

Der Versicherungsnehmer ist ein mittelständischer Betrieb und arbeitet ausschließlich Werktags. Deswegen fallen sonntags keine neuen Daten an und der Betrieb führt sonntags keine Backups durch. Nach einer Cyberattacke verweigert der Versicherer die Leistung, weil der Versicherungsnehmer die Obliegenheit zur täglichen Datensicherung verletzt habe.

Eine Obliegenheit zur täglichen Datensicherung unabhängig davon, ob überhaupt neue Daten angefallen sind, verursacht beim versicherten Betrieb Kosten, ohne einen höheren Schutz zu schaffen. Deshalb benachteiligt eine solche Backup-Obliegenheit zur täglichen Datensicherung den Versicherungsnehmer unangemessen und ist unwirksam.[2]

Obliegenheiten, die nur höhere Kosten, aber keinen höheren Cyber-Schutz bringen, können unangemessen sein.

[2] In diese Richtung: *Klimke* in Prölss/Martin[31], A1-16 AVB Cyber, Rn. 15.

Beispielszenario 5 (Datensicherung auch unwichtiger Daten):

Beim versicherten Unternehmen fallen eine Fülle von Daten an. Neben der für die Geschäftstätigkeit zwingend notwendigen Daten entstehen auch viele Daten, die die Geschäftstätigkeit nicht beeinflussen („unwichtige Daten"). Diese unwichtigen Daten sichert das Unternehmen nur wöchentlich. Im Anschluss an eine Cyberattacke wendet der Versicherer ein, der Versicherungsnehmer habe die Obliegenheit zur täglichen Sicherung aller Daten verletzt.

Eine solche Obliegenheit zur täglichen Datensicherung unterschiedslos aller Daten belastet den Versicherungsnehmer unangemessen und ist deswegen gem. § 307 BGB unwirksam. Der Versicherer hat kein schützenswertes Interesse an der täglichen Sicherung unwichtiger Daten, da sich diese nicht auf seine Leistungspflicht auswirken.

2.3 Offline-Backups – zu unbestimmt?

Des Weiteren ist die dargestellte Backup-Obliegenheit wegen der Verpflichtung zur Offline-Datensicherung unbestimmt und damit unwirksam (§ 307 Abs. 1 S. 2 BGB).

Beispielszenario 6 (Online-Backup):

Das Unternehmen möchte seine Daten über die Cloud eines vertrauenswürdigen weltweit agierenden Backup-Anbieters sicher und kostengünstig speichern. Jedoch fragen sich die Entscheidungsträger, ob ein solches Online-Backup mit der versicherungsvertraglichen Obliegenheit zu Offline-Backups vereinbar ist.

Die Datensicherung über Online-Backups ist zulässig, da die Obliegenheit zu Offline-Backups zu unbestimmt und damit unwirksam ist.

Auch unbestimmt formulierte und somit mehrdeutige Klauseln sind häufig unwirksam.

Unklar ist nämlich, wann ein Offline-Backup vorliegt. Zum einen könnte ein Offline-Backup nur dann vorliegen, wenn die Daten auf einer physisch getrennten Festplatte gesichert sind. In einem solchen Fall wäre die Obliegenheit wohl schon wegen den mindestens gleichsicheren Online-Backups unangemessen und deswegen unwirksam. Zum anderen könnte ein Offline-Backup schon dann vorliegen, wenn die Angreifer das Backup nicht unmittelbar sperren können. In diesem Fall wären auch sichere Online-Backups zulässig. Diese Unsicherheit bei der Auslegung führt zur Unbestimmtheit und damit zur Unangemessenheit der Offline-Backup-Obliegenheit.

3. Weitere Verteidigungslinien

Selbst wenn der Versicherer sich mit seiner Ansicht durchsetzt, dass der Versicherungsnehmer eine wirksame Obliegenheit aus dem Cyberversicherungsvertrag verletzte, verbleiben dem Versicherungsnehmer weitere Verteidigungslinien.

3.1 Verletzung durch Repräsentanten

Eine Obliegenheitsverletzung liegt immer nur dann vor, wenn ein Repräsentant des Unternehmens die Obliegenheit verletzte.

Eine Repräsentantenklausel kann etwa wie folgt lauten:

„Dem Versicherungsnehmer wird die Kenntnis, das Verhalten und das Verschulden folgender Personen (Repräsentanten) zugerechnet:

*bei Aktiengesellschaften die **Mitglieder des Vorstandes […]“***

Beispielszenario 7 (Der autonom agierende IT-Mitarbeiter):

Die AVB enthalten eine wirksame Backup-Obliegenheit sowie eine Repräsentantenklausel. Entgegen den internen Vorgaben stellt ein IT-Mitarbeiter des Unternehmens das automatische Backup aus, weil das automatische Backup die Performance störe. Eine Cyberattacke führt zur vollständigen Verschlüsselung aller Daten. Ein aktuelles Backup liegt nicht vor. Der Versicherer verweigert nun die Zahlung, weil der Versicherungsnehmer gegen die Backup-Obliegenheit verstoßen habe.

Dem Versicherer steht jedoch kein Leistungskürzungs- oder -verweigerungsrecht zu, da kein Repräsentant des Versicherungsnehmers die Backup-Obliegenheit verletzte.

Eine enge Repräsentantenklausel kann Versicherungsschutz wahren. Die Repräsentanten sind daher sorgsam zu bestimmen und ausdrücklich auf die Organe des Versicherungsnehmers (etwa Geschäftsführer oder Vorstände) zu begrenzen.

3.2 Fehlende Ursächlichkeit (Kausalitätsgegenbeweis)

Sollte der Versicherer eine Obliegenheitsverletzung durch einen Repräsentanten nachweisen, kann der Versicherungsnehmer gegen eine Leistungsfreiheit des Versicherers einwenden, dass die Obliegenheitsverletzung nicht kausal für den Umfang der Leistungspflicht ist (§ 28 Abs. 3 S. 1 VVG).

Beispielszenario 8 (Irrelevanz der Obliegenheitsverletzung):

Das Unternehmen sichert die Backups trotz wirksamer Obliegenheit unzureichend. Die Angreifer sperren daher die Backups und entziehen vertrauliche Unternehmens- und Kundendaten. Um eine Wiederherstellung zu ermöglichen und eine Veröffentlichung der entzogenen Daten zu verhindern, zahlt das Unternehmen das Lösegeld. Der Versicherer verweigert nun den Ersatz des Lösegelds mit Verweis auf die verletzte Backup-Obliegenheit.

Die Verweigerung des Versicherers ist unzulässig. Ein Backup kann einer Verschlüsselung von Daten entgegenwirken, aber keinen Datenabfluss und anschließende Veröffentlichung verhindern. Das Lösegeld dient aber insbesondere auch dazu, der Veröffentlichung vertraulicher und versicherter

Daten vorzubeugen. Dementsprechend ist die Verletzung der Backup-Obliegenheit für die Leistungspflicht des Versicherers irrelevant.

4. Fazit

Obliegenheitsverletzungen stellen ein ständiges Risiko für versicherte Unternehmen dar, ihren Cyber-Versicherungsschutz zu verlieren. Nicht nur im eigenen Interesse sollten Unternehmen ihre IT-Standards fortwährend überprüfen und dabei auch mit den Anforderungen aus dem Versicherungsvertrag abgleichen. Für problematisch formulierte Klauseln gilt, diese frühzeitig mit dem Versicherer und dem Versicherungsmakler zu besprechen. Treffen die Parteien dann eine abweichende Individualvereinbarung, so sollte das versicherte Unternehmen diese gut dokumentieren.

Wendet der Cyber-Versicherer im Schadenfall eine Obliegenheitsverletzung ein, muss dies nicht zwingend den Verlust des Versicherungsschutzes bedeuten. Berechtigte Zweifel an der Wirksamkeit einer Klausel können den Versicherungsschutz in vielen Fällen retten. Um auch nach einem Cyberangriff die eigenen Rechte gegenüber dem Cyberversicherer ohne Kostenrisiko durchzusetzen, bietet sich der Abschluss einer Cyberrechtsschutzversicherung an.

Diesen Beitrag veröffentlichte die Zeitschrift *Die VersicherungsPraxis* in ihrer Ausgabe 06/2023.

Für Rückfragen steht Ihnen der Autor gern zur Verfügung:

Dr. David Ulrich, LL.M. (Kent)
Rechtsanwalt

WILHELM Partnerschaft von Rechtsanwälten mbB

Tel: +49 30 8172732-40
david.ulrich@wilhelm-rae.de