Crowdstrike-Vorfall – Erhalten betroffene Unternehmen eine Entschädigung aus ihrer Cyber-Versicherung?

Frankfurt am Main, 23.07.2024

Ein fehlerhaftes Update des US-amerikanischen IT- Sicherheitsdienstleisters Crowdstrike hat am Freitag zu weitreichenden Störungen geführt. Experten sprechen vom größten, nicht durch einen Cyber-Angriff verursachten IT-Ausfall aller Zeiten. Unzählige Unternehmen waren betroffen und etliche mussten den Betrieb oder Teile davon zeitweise komplett einstellen. Auch wenn Crowdstrike den Fehler zwischenzeitlich behoben hat und die meisten Unternehmen wieder voll einsatzfähig sind, bleibt eine große Frage: Wer erstattet den betroffenen Unternehmen die Kosten und Umsatzausfälle, die aufgrund des Vorfalls entstanden sind? Ferner, ob Versicherungsschutz im Rahmen einer Cyber-Police besteht?

Klassische deckungsauslösende Ereignisse in der Cyber-Versicherung

Die Frage lässt sich nicht ohne weiteres mit einem einfachen Ja oder Nein beantworten. Vielmehr kommt es – wie so oft – auf die Umstände des Einzelfalls und insbesondere auf die konkreten Bedingungen der zugrundeliegenden Cyber-Deckung an.

Eine Cyber-Versicherung bietet grundsätzlich Versicherungsschutz für Schäden, die versicherten Unternehmen infolge eines deckungsauslösenden Ereignisses entstehen. Was der einzelne Versicherungsvertrag unter einem solchen Ereignis versteht, unterscheidet sich von Deckungskonzept zu Deckungskonzept. In sämtlichen Cyber-Versicherungen werden deckungsauslösende Ereignisse aber durch Cyber-Angriffe ausgelöst. Grob skizziert sind dies Vorfälle der unbefugten Nutzung versicherter IT, wie zum Beispiel insbesondere klassische „Hackerangriffe", aber auch die Sabotage versicherter IT durch eigene Mitarbeiter. Weitere mögliche Deckungsauslöser sind Datenschutzrechtsverletzungen sowie die Androhung eines Cyber-Angriffes in erpresserischer Weise. Da es sich vorliegend – zumindest nach derzeitigen Erkenntnissen – jedoch um ein fehlerhaftes Update eines Cyber-Dienstleisters handelte und nicht um einen Cyber-Angriff im klassischen Sinne, greifen die oben angesprochenen einschlägigen Trigger der Cyber-Versicherung nicht.

Fehlbedienung und technische Probleme als deckungsauslösende Ereignisse

In vielen Versicherungsverträgen werden daneben aber auch sogenannte Bedienfehler und technische Probleme als deckungsauslösende Ereignisse definiert. Entweder ist dies im Katalog der deckungsauslösenden Ereignisse standardmäßig enthalten oder kann als optionale Deckungserweiterung gegen Mehrprämie vom Versicherungsnehmer dazugebucht werden.

Bei der Erweiterung des Gefahrenkataloges um die Fehlbedienung wird diese meist als eine fehlerhafte (unsachgemäße) Bedienung des IT-Systems eines versicherten Unternehmens durch fahrlässiges Handeln oder Unterlassen beschrieben. Hier kommt es dann auf die weiteren Details des Wordings an: Sind nur Fehlbedienungen durch eigenes Personal des Versicherten umfasst oder sind auch Fehlbedienungen durch IT-Dienstleister in die Gefahrenbeschreibung eingeschlossen?

Zählt auch ein fehlerhaftes Update zu den versicherten Bedienfehlern? Ist es für das Auslösen der Deckung erheblich, ob die Fehlbedienung an IT des Versicherungsnehmers vorgenommen wurde?

Eine weitere Möglichkeit, einen passenden Deckungsauslöser für das vorliegende Szenario zu finden, bietet eventuell die Mitversicherung von technischen Problemen.

Definiert werden technische Probleme in den Bedingungen zum Beispiel als Fehlfunktionen des informationstechnischen Systems eines versicherten Unternehmens, die weder durch eine Fehlbedienung noch durch eine Netzwerksicherheitsverletzung verursacht werden. Die Erweiterung der Deckung wird in der Regel auf Basis sogenannter „benannter Gefahren" angeboten, das heißt der Umfang der Deckung wird durch Konkretisierung der genau in den Versicherungsschutz fallenden Szenarien präzisiert und weiter eingeschränkt. So ist häufig auch bei Mitversicherung technischer Probleme der Deckungsumfang auf Fälle der Über- und Unterspannung, Ausfall der eigenen Stromversorgung oder Klimatechnik und Ähnliches begrenzt. Teils sind aber auch fehlerhafte Updates ausdrücklich in den Anwendungsbereich des Bausteines einbezogen.

Auch etwaige Bausteine, die die Nichtverfügbarkeit externer IT-Dienstleister, Softwarefehler oder fehlerhafte Updates als deckungsauslösende Ereignisse vorsehen, können hier einschlägig sein.

Ob es sich beim Crowdstrike-Vorfall um einen Fall für die Cyber-Versicherung handelt, ist nach alldem individuell zu bestimmen und hängt entscheidend von den vereinbarten Bedingungen ab.

Versicherungsumfang der Cyber-Versicherung

Liegt ein deckungsauslösendes Ereignis vor, bietet der Cyber-Versicherungsvertrag für versicherte Unternehmen – neben Assistance-Leistungen durch eine Notfallhotline und diverserer Netzwerkpartner – insbesondere einen Kostenschutz (zum Beispiel Schadenermittlungskosten, Wiederherstellungskosten, Rechtsanwaltskosten, Lösegelder), einen Verfahrensschutz (zum Beispiel Abwehrkosten in OwiG- oder Bußgeld-Verfahren) sowie Schutz vor Schadenersatzansprüchen (Abwehr und/oder Freistellung). Darüber hinaus bieten die Policen Versicherungsschutz für Verluste aufgrund einer Betriebsunterbrechung.

Schäden aufgrund des Crowdstrike-Vorfalls

Im Rahmen des Crowdstrike-Vorfalls sind vor allem Kosten oder Mehraufwendungen denkbar, die bei betroffenen Unternehmen für die Wiederherstellung der Systeme angefallen sind (zum Beispiel weil ein externer IT-ler eingeschaltet werden musste oder weil Mitarbeiter Überstunden machen mussten) und Umsatzverluste aufgrund einer Betriebsunterbrechung.

Sowohl Kosten als auch ein Verlust durch Betriebsunterbrechung sind im Rahmen der Cyber-Versicherung grundsätzlich versichert, wenn die Schäden kausal auf einem der in der konkreten Police versicherten deckungsauslösenden Ereignisse beruhen.

Unternehmen, denen Schäden aufgrund des Crowdstrike-Vorfalls entstanden sind, sollten daher unbedingt einen genauen Blick in ihre Versicherungspolice werfen. Insbesondere wenn der Vertrag eine Klausel enthält, die Fehlbedienungen durch externe IT-Dienstleister oder eine Verfügbarkeitsbeeinträchtigungen infolge technischer Probleme als deckungsauslösendes Ereignis definiert, könnten entstandene Kosten versichert sein.

Ausschlüsse, Sublimite und zeitlicher Selbstbehalt

Beachtet werden müssen hierbei aber etwaige Ausschlüsse, die einschlägig sein könnten (zum Beispiel ein Ausschluss für Schäden durch Softwarefehler) und individuelle Sublimite, die die Entschädigung zu bestimmte Deckungsbausteinen auf einen Maximalbetrag beschränken. Darüber hinaus kommt für eine Entschädigung eines etwaigen Betriebsunterbrechungsschadens in aller Regel ein sogenannter zeitlicher Selbstbehalt zur Anwendung. Dieser beträgt in vielen Versicherungsverträgen 12 Stunden. Das heißt, erst wenn eine Betriebsunterbrechung länger als der vereinbarte Selbstbehalt andauerte, wird der Versicherer eintrittspflichtig. Ist der zeitliche Selbstbehalt überschritten, gilt in vielen Spezialkonzepten dann sogar eine Eintrittspflicht rückwirkend ab der 1. Minute.

Fazit

Sollten Sie beziehungsweise einer Ihrer Kunden vom Crowdstrike-Vorfall betroffen sein und sind Kosten oder ein Schaden aufgrund einer Betriebsunterbrechung entstanden, sollte vom Unternehmen oder dem betreuenden Makler geprüft werden, ob gegebenenfalls ein Anspruch auf Entschädigung gegen den Cyber-Versicherer besteht.

Finlex Blogpost 07/2024

Sprechen Sie uns gerne an.

Finlex GmbH

Finlex Support
E-Mail: support@finlex.de

finlex.io