

Kundeninformation zu **Cyber**risiken in der D&O-Versicherung

Cyber als elementares Geschäftsrisiko

Cyberrisiken sind aus unserer heutigen Geschäftswelt nicht mehr wegzudenken. Sie sind zu einem elementaren Geschäftsrisiko geworden, das ohne einen angemessenen Versicherungsschutz die Existenz Ihres Unternehmens bedrohen kann. Insbesondere in Fällen, in denen Cyberereignisse zu Vermögensschäden führen, können Cyberrisiken bereits teilweise über Ihre klassischen Versicherungspolizen, wie z. B. die D&O-Versicherung, gedeckt sein. Wie bei der D&O-Versicherung ist hierfür jedoch Voraussetzung, dass eine versicherte Person für den eintretenden Schaden haftbar gemacht werden kann. Da uns Transparenz und Ihre Sicherheit sehr am Herzen liegen, haben wir Ihnen einen Überblick darüber erstellt, welche Cyberrisiken in der D&O-Versicherung der Allianz gedeckt sind und welche nicht.

Bitte beachten Sie, dass dieses Informationsblatt lediglich einen Überblick über wesentliche cyberrelevante Deckungen und Ausschlüsse gibt und nicht vollständig ist. Es ist unverbindlich und nicht Teil der Vertragsunterlagen.

Versicherte Cyberschäden

Die D&O-Versicherung der Allianz ist als Haftpflichtversicherung zugunsten der versicherten Personen ausgestaltet. Voraussetzung ist, dass eine versicherte Person für den eingetretenen Schaden haftpflichtig gemacht werden kann,

da sie eine bestehende Pflicht schuldhaft verletzt hat und kein Deckungsausschluss wie z. B. wesentliche Pflichtverletzung greift. Auch Cyberrisiken können vom Versicherungsschutz umfasst sein:



Beschädigung bzw. Verlust von Daten oder Software infolge eines Cyberereignisses ohne Zerstörung der Hardware: Wurden Daten zerstört bzw. beschädigt, ohne dass dem Datenverlust eine Zerstörung der Infrastruktur (Hardware) zugrunde liegt, besteht Versicherungsschutz für die versicherte Person.

Beispiel: Durch einen Cyberangriff werden Daten des Unternehmens oder Dritter vernichtet/beschädigt und eine versicherte Person trägt dafür die Verantwortung.



Durch ein Cyberereignis kommt es zu Datenschutzverletzungen: Aufgrund eines Cyberereignisses werden datenschutzrelevante Daten widerrechtlich an Dritte weitergeleitet. Falls eine versicherte Person schuldhaft gehandelt hat, ist der hierdurch entstehende Vermögensschaden versichert.

Beispiel: Mittels eines Cyberereignisses werden sensible Kundendaten veröffentlicht und eine versicherte Person trägt hierfür die Verantwortung.

Nicht versicherte Cyberschäden

Voraussetzung für den D&O-Versicherungsschutz für Schadenersatzansprüche im Zusammenhang mit einem Cyberereignis ist die Verursachung eines Vermögensschadens.



Funktionsunfähigkeit und Beschädigung von Hardware und Datenträgern: Die D&O-Versicherung der Allianz deckt weder Sachschäden noch die sich aus Sachschäden ergebenden Vermögensschäden.

Beispiel: Durch ein Cyberereignis werden Computer und Speichermedien physisch beschädigt und unbrauchbar.

Voraussetzung für den D&O-Versicherungsschutz für Schadenersatzansprüche im Zusammenhang mit einem Cyberereignis ist ein vorwerfbares, d. h. schuldhaftes Verhalten einer über die D&O-Police versicherten Person.



Hackerangriffe sind häufig erfolgreich, obwohl die Sicherheitsvorkehrungen den Standards entsprechen. Da die Voraussetzungen für ein Verschulden einer versicherten Person nicht vorliegen, wehren wir den Haftpflichtanspruch für die versicherte Person ab. In diesem Fall verbleibt dann der Schaden bei Ihrem Unternehmen.

Beispiel: Aufgrund eines Cyberereignisses wird unbefugt auf sensible Kundendaten zugegriffen. Da ausreichende Vorkehrungen von den versicherten Personen getroffen wurden, sind die Voraussetzungen für einen versicherten Haftpflichtanspruch nicht gegeben.



Beispiel: Trotz ausreichender Vorkehrungen zur IT-Sicherheit seitens einer versicherten Person, erfolgt ein Cyberangriff. Dieser verursacht einen Betriebsunterbrechungsschaden im Unternehmen sowie Wiederherstellungskosten für Dateien etc.

„Nice to know“

Was ist eigentlich ein „Cyberereignis“?

Unter einem Cyberereignis versteht man insbesondere einen unbefugten Eingriff auf ein Computersystem mit dem Ziel, die Verfügbarkeit, Vertraulichkeit oder Echtheit von Daten zu manipulieren. Zu einem Computersystem gehören auch Maschinensteuerungen und mobile Endgeräte. Ziel eines Eingriffs ist es i. d. R., Daten abzugreifen, zu veröffentlichen und/oder zu verschlüsseln.



Wie kann sich Ihr Unternehmen gegen cyberbedingte Vermögensschäden versichern?

Wir bieten Ihrem Unternehmen gerne unseren Allianz CyberSchutz an, der speziell dazu konzipiert wurde, Ihr Unternehmen umfassend vor Risiken der Informationstechnologie zu schützen. Haben Sie Interesse? Bitte sprechen Sie Ihren Vermittler an.