/ Versicherungsschutz für Cyber-Risiken im Home-Office in Corona-Zeiten

4/8/2020

Versicherung & Rückversicherung | Haftung & Versicherung | Corona Crisis Center

Home-Office ist gerade in Corona-Zeiten das Gebot der Stunde. Unter dem Gesichtspunkt der IT-Sicherheit begründet die Arbeit im Home-Office allerdings auch erhöhte Risiken. In vielen Fällen kann nämlich davon ausgegangen werden, dass die Heimnetzwerke der Mitarbeiter nicht denselben Sicherheitsstandard bieten, wie das Unternehmensnetzwerk. Viele Unternehmen lassen ihre Mitarbeiter zudem private Geräte verwenden, vom privaten Notebook bis hin zu privaten Netzwerkdruckern oder anderen Storage-Geräten (z.B. USB-Sticks, externe Festplatten). Dazu kommt, dass immer mehr in Privathaushalten eingesetzte Alltagsgegenstände softwaregesteuert und mit dem Internet verbunden sind. Dadurch entstehen zusätzliche Angriffsvektoren, wenn derartige Geräte – häufig mit bekannten Sicherheitslücken – in denselben Netzwerken eingesetzt werden, wie die mobilen Arbeitsgeräte. Es besteht die Gefahr, dass Cyberkriminelle die Schwächen von Heimnetzwerken gerade in der aktuellen Situation vermehrt und gezielt ausnutzen, um in Unternehmensnetzwerke zu gelangen und dort personen- und/oder unternehmensbezogene Daten abzugreifen oder in Erpressungsabsicht zu verschlüsseln.

Neben diesen eher technisch bedingten Risiken ist zu beobachten, dass Cyberkriminelle vermehrt die Corona-Krise auch für Angriffe auf die Schwachstelle „Mensch“ ausnutzen. So hat das Bundesamt für Sicherheit in der Informationstechnik in einer Pressemitteilung vom 02.04.2020 mitgeteilt, dass eine Zunahme von Cyber-Angriffen mit Bezug zum Corona-Virus zu beobachten sei. So werden Unternehmen z.B. per E-Mail durch Cyberkriminelle aufgefordert, persönliche oder unternehmensbezogene Daten auf gefälschten Webseiten preiszugeben, Nutzer werden auf Webseiten mit vermeintlichem Informationsangebot zum Corona-Virus zum Download kompromittierter Dateien aufgefordert und betrügerische Online-Shops machen sich die derzeit erhöhte Nachfrage nach Schutzbekleidung und Atemmasken zunutze.

Unternehmen, die eine Versicherung zum Schutz gegen Cyber-Risiken abgeschlossen haben, können im Fall einer Cyber-Attacke auf das Home-Office in vielen Fällen auf Entschädigung hoffen. Gleichzeitig haben die Unternehmen allerdings auch auf gegebenenfalls bestehende Anzeigeobliegenheiten zu achten, um ihren Versicherungsschutz nicht zu gefährden.

1. Versicherungsschutz für Home-Office-Tätigkeit

Für die Frage, ob und in welchem Umfang Versicherungsschutz besteht, wenn Cyberkriminelle über Sicherheitslücken im Home-Office Zugriff auf das Unternehmensnetzwerk erhalten, muss danach differenziert werden, ob es sich bei den mobilen Arbeitsgeräten für die Home-Office-Tätigkeit um Privatgeräte der Mitarbeiter handelt oder diese vom Unternehmen zur Verfügung gestellt werden.

Während im letzteren Fall – vorbehaltlich besonderer Vereinbarungen – in der Regel Versicherungsschutz besteht, hängt dies bei der Nutzung privater Informations- und Telekommunikationsgeräte häufig von einer besonderen Vereinbarung im Versicherungsvertrag ab. Je nach konkreter Vereinbarung besteht mitunter nur eingeschränkter Versicherungsschutz (z.B. besondere Deckungslimite). Zu beachten ist auch, dass der Versicherungsschutz teilweise davon abhängig gemacht wird, dass den Mitarbeitern die Nutzung aufgrund einer vertraglichen oder generellen, schriftlichen Erlaubnis des Versicherungsnehmers gestattet ist.

Fehlt es an besonderen Deckungsbausteinen, kann sich der Versicherungsschutz auch aus der allgemeinen Beschreibung des versicherten Risikos ergeben. Besteht danach Versicherungsschutz ausschließlich für Angriffe auf IT-Systeme des Versicherungsnehmers, kommt es zunächst darauf an, ob und falls ja, wie die Versicherungsbedingungen den Begriff des IT-Systems definieren. Fehlt es an einer Definition, ist für die Reichweite des Versicherungsschutzes auf die

Verständnismöglichkeiten eines durchschnittlichen Versicherungsnehmers abzustellen.

Einfacher zu bestimmen ist der Versicherungsschutz in der Regel, soweit die jeweiligen Klauseln nicht auf *„informationsverarbeitende Systeme“*, *„Computer-Systeme“*, oder *„IT-Systeme“* des Versicherungsnehmers, sondern der „Versicherten“ Bezug nehmen. In diesem Fall lässt sich der Deckungsumfang für Home-Office Tätigkeiten relativ einfach über den Kreis der Versicherten bestimmen. Soweit nämlich die Mitarbeiter des Versicherungsnehmers zum definierten Personenkreis der Versicherten gehören, besteht Versicherungsschutz in der Regel im selben Umfang wie der des Versicherungsnehmers. Auslegungsfragen ergeben sich weiterhin dann, wenn unter den Begriff der „Versicherten“ – wie dies teilweise im Markt üblich ist – nur der Versicherungsnehmer selbst, sowie mitversicherte Unternehmen gefasst werden, nicht aber auch mitversicherte Personen.

2. Obliegenheiten

Nicht in Vergessenheit geraten sollte allerdings, dass auch im Home-Office die Einhaltung eines vergleichbaren IT-Sicherheits- und Datenschutzniveaus sichergestellt sein muss. Unternehmen sollten deshalb zurückhaltend damit sein, Lockerungen im Umgang mit der IT-Sicherheit und dem Datenschutz mit Verweis auf die aktuell bestehende Ausnahmesituation zuzulassen. Die Corona-Krise befreit den Versicherungsnehmer nicht von der Einhaltung seiner vertraglichen Obliegenheiten. Auf der anderen Seite ist allerdings auch dem Umstand Rechnung zu tragen, dass das Unternehmen selbst in tatsächlicher Hinsicht nur begrenzte Einflussmöglichkeiten auf den IT-Sicherheitsstandard der privaten Heimnetzwerke der Mitarbeiter hat.

Um den eigenen Versicherungsschutz nicht zu gefährden, ist den Unternehmen dringend zu empfehlen, klare und verbindliche Regeln für die Arbeit im Home-Office zu definieren. Gerade mit Blick auf die aktuell zunehmende Bedrohung durch den Anstieg sog. Phishing-Angriffe via E-Mail sollte dabei auch ein verstärkter Fokus auf entsprechenden Schulungs- und Aufklärungsmaßnahmen liegen, um die Mitarbeiter für diese Risiken zu sensibilisieren.

3. Anzeigeobliegenheiten des Versicherungsnehmers aufgrund Gefahrerhöhung

Einige Versicherer fragen im Rahmen der vorvertraglichen Risikoprüfung explizit nach der Nutzung privater Geräte zu beruflichen Zwecken oder der Anzahl der regelmäßig im Home-Office tätigen Mitarbeiter. Verneint der Versicherungsnehmer diese Frage bei Abschluss des Vertrages, so liegt in der nachträglichen Gestattung eine Risikoerhöhung, die den Versicherungsnehmer gemäß § 23 Abs. 1 VVG zur Anzeige gegenüber dem Versicherer verpflichtet. Dasselbe gilt, wenn sich die Anzahl der im Home-Office tätigen Mitarbeiter gegenüber der Situation bei Abschluss des Cyberversicherungsvertrags verändert hat und der Versicherer danach gefragt hat.

Ob eine Anzeigeobliegenheit auch unabhängig davon besteht, ob der Versicherer vor Abschluss des Vertrags nach der Home-Office-Nutzung gefragt hat, lässt sich nicht pauschal beantworten. Im Einzelfall müsste geprüft werden, ob bloß eine nach § 27 VVG als mitversichert anzusehende Gefahrerhöhung vorliegt. Zur Vermeidung von Auseinandersetzungen im Schadenfall dürfte der sicherste Weg darin liegen, dem Versicherer eine verstärkte Home-Office-Nutzung vorsorglich anzuzeigen.

4. Handlungsempfehlungen

- Cyberversicherungen bieten häufig Versicherungsschutz für Risiken aus Home-Office Tätigkeiten. Umfang und Grenzen des Versicherungsschutzes lassen sich allerdings stets nur anhand einer Auslegung des jeweiligen Vertragswerkes bestimmen. Unternehmen sollten ihre Verträge deshalb genauestens prüfen, um nicht erst im Schadenfall bislang unerkannte Deckungslücken in ihren Verträgen festzustellen.
- Daneben ist festzuhalten, dass versicherungsvertragliche Obliegenheiten prinzipiell unverändert gelten. Unternehmen sollten deshalb klare und verbindliche Regeln für die Arbeit im Home-Office definieren.

- Darüber hinaus müssen bei verstärkter Home-Office-Nutzung auch entsprechende Anzeigeobliegenheiten gegenüber dem Versicherer im Blick behalten werden.

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. Thomas Heitzer , Dr. Oliver Sieg , Dr. Dan Schilbach

Praxisgruppen: Litigation, Arbitration & ADR , Insurance & Reinsurance

Contact Person

Dr. Thomas Heitzer
Co-Leiter Finanzdienstleistungsaufsicht
Leiter Versicherung & Rückversicherung
Rechtsanwalt

T +49 211 49986170

Dr. Oliver Sieg
Leiter Haftung & Versicherung
Mitglied der Practice Group Aktien- & Kapitalmarktrecht
Rechtsanwalt

T +49 211 49986220