Haftung aus Life-Science-Risiken – Teil 5: Versicherungsschutz gegen Internetkriminalität

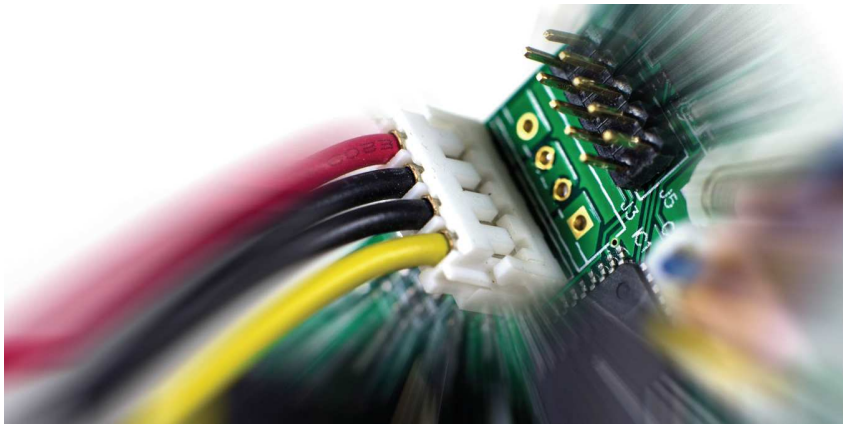
Marcus H. Rexfort

Als Dienstleistungsunternehmen für die Arzneimittel- und Medizintechnik-Industrie erbringen Auftragsforscher eine mit weitreichenden finanziellen Implikationen versehene Leistung. Ihre sensible Tätigkeit macht Auftragsforscher zu einem bevorzugten Angriffsziel von unlauteren Wettbewerbern und von staatlich gelenkter Industriespionage. Im Kontext steigender Internetkriminalität sind „Viruserkrankungen" von EDV-Systemen existenzielle Risiken, zumal sie oft mit teuren Vertragsstrafen in Folge von Vertraulichkeitsverletzungen einhergehen. Versicherungsschutz gegen diese Gefahren ist deshalb wichtiger denn je!

2017 gab es über 500 Mio. Attacken mit Viren, Trojanern und sonstiger Schadsoftware, Tendenz stark steigend. Ob IT-Sicherheitslücken, Abhörskandale oder Datenschutzverstöße: Täglich gibt es neue Berichte über reale Bedrohungen für die Nutzer des Internets. Das Beunruhigende: Auch die beste Schutz-Software für Computer kann trotz regelmäßiger Aktualisierungen Sicherheitslücken aufweisen.

Drei wesentliche Gefahren gibt es:
- Den Cyber-Angriff mit dem Ziel, die eigne IT zu unterbrechen und zu blockieren.
- Den Cyber-Eingriff, um Daten oder Programme zu stehlen, zu verändern oder zu zerstören.
- Die Cyber-Infektion mit Schadsoftware, um die kompromittierte eigene IT für Cyber-Angriffe auf Dritte – wie beispielsweise den Auftraggeber – zu nutzen.

Die Internetnutzung birgt also erhebliche Risiken, die von Cyber-Mobbing durch die Verletzung von Persönlichkeitsrechten, Identitätsdatendiebstahl, Zahlungsmitteldatendiebstahl durch die Entwendung von Bank- und Kreditkartendaten bis hin zu Urheberrechtsverletzungen und Konflikten mit den Auftraggebern oder der Justiz reichen.



R_K_B_by_Rainer Sturm_pixelio

Versicherungsschutz benötigen IT-Systeme, Programme und elektronische Daten. Privatnutzern genügt meist die Absicherung von Eigenschäden. Bei gewerblichen Anwendern kommen zusätzlich Haftpflichtansprüche aus Verletzung des Datenschutzrechts hinzu, ferner Strafgelder aufgrund des Bundesdatenschutzgesetzes oder der Weitergabe von Viren, Kosten durch Betriebsausfälle und aus der Verletzung von Geheimhaltungsverpflichtungen in Gestalt von Zahlungen vereinbarter Vertragsstrafen.

Vertraulichkeitsverletzungen sind in fast jedem Rahmenvertrag ge-regelt – das Gefährliche daran: Es entsteht ein Schadenersatzanspruch unabhängig davon, ob ein Vermögensschaden einhergegangen ist. Manche Verträge sehen kumulierende Strafen je nach Dauer des Vergehens vor, die sich schnell als existenzgefährdend erweisen können. Eine gute Cyberpolice sollte mindestens fünf Leistungskategorien umfassen:

- Beistand durch eine Notfallberatung,
- Schutz vor Identitäts- und Zahlungsmitteldatendiebstahl,
- Überprüfung des Schadens durch Fall-Analyse und Web-Check,
- Hilfe bei der Löschung gestohlener persönlicher Daten und Rechtsberatung,
- Kostenübernahme bzw. Erstattung von Schäden, die durch betrügerische Absicht oder vertragswidriges Verhalten von Vertragspartnern entstehen.

Die optimierte Police bietet darüber hinaus Versicherungsschutz bei Beschädigung, Zerstörung, Veränderung oder Missbrauch der IT-Systeme und Programme. Mitversichert werden sollte eine Cyber-Betriebsunterbrechung. Zusätzlich sollten die Kosten der Datenforensik-, Datenwiederherstellung und die Informationskosten der betroffenen privaten und juristischen Personen enthalten sein. Ganz wichtig ist die Vereinbarung von bedarfsgerechten Leistungen für Vertragsstrafen, die sich aus Vertraulichkeitsverletzungen ergeben können. Leistungen bei erpresserischen Cyber-Geldforderungen können ebenfalls versichert werden.

Jedes Unternehmen ist gut beraten, einen Cyber-Notfallplan vorzuhalten. Dazu zählt auch, im Schadensfall möglichst sofort die Cyber-Hotline des Versicherers zu wählen: Je nach Servicequalität des Versicherers ist die Erreichbarkeit 24 Stunden an 365 Tagen gewährleistet. Der Versicherer organisiert umgehend die IT-Forensik, erste Abwehrstrategien und weitere Sicherungsmaßnahmen. In dieser Situation sind aber nicht nur die Versicherungsbedingungen wichtig, sondern besonders die Expertise des vertraglich mit dem Versicherer verbundenen IT-Dienstleisters. Versicherer mit nur überschaubaren Kundenzahlen können hier oftmals nicht mithalten. Jedoch sind gerade die mitversicherten Assistance-Leistungen für Auftragsforscher häufig entscheidend, um einen Cyberangriff und die einhergehende Kriese zu überstehen. Eine kluge Beratung hilft den Entscheidern, die richtige Wahl des Versicherungspartners zu treffen.

Zum Autor:
Marcus H. Rexfort ist Inhaber des Rheinisches Versicherungskontors in Ratingen. Neben der Versicherung von klinischen Studien berät er Auftragsforscher zu deren betrieblicher Risikoabsicherung
Website:
www.medizinische-forschung.info

Korrespondenzadresse:
Marcus H. Rexfort
RhVk – Rheinisches
Versicherungskontor e.K.
Josef-Schappe-Str. 21
40882 Ratingen
Tel.: + 49 (0) 2102-709077
Fax: + 49 (0) 2102-709076
E-Mail: mail@rhvk.info
Internet: www.rhvk.info

Marcus H. Rexfort