

Neue Risiken wirksam absichern

«Legt ein Virus die IT für längere Zeit lahm, steht im schlimmsten Fall die Existenz der Firma auf dem Spiel. Eine Cyberversicherung bewahrt Unternehmen vor diesem Schicksal.»

Caroline Voigt

Geschäftsführende Präsidentin des
Liechtensteinischen Versicherungsverbandes (LVV)

Neue Technologien und Entwicklungen bieten neue Chancen, bringen aber auch mögliche neue Gefahren mit sich, die sich dynamisch entwickeln. Sie sind nur bedingt erkennbar, aber versicherungstechnisch bewertbar. Diese Gefahren haben ein grosses Schadenpotenzial und werden als «Emerging Risks» bezeichnet. Ein ganz zentrales Risiko aus dieser Kategorie sind Angriffe auf die Cybersicherheit eines Unternehmens.

Diese Informationssicherheit umfasst unter anderem den Schutz der Vertraulichkeit von Informationen und Daten, den Schutz vor unbefugter Veränderung von Daten und die Gewährleistung der Verfügbarkeit von kritischen IT-Systemen wie beispielsweise Zahlungssystemen. Als Risikobereiche lassen sich Ausfälle von Systemen genauso identifizieren wie Datenverlust, Informationsspionage, Datendiebstahl und Cyber-Terrorismus.

Entschädigung, Schadenersatz, Service

Private Firmen sind heute in allen Bereichen ihrer Geschäftstätigkeit genauso auf IT-Systeme angewiesen wie öffentliche Verwaltungen und staatsnahe Betriebe. Ohne einen Computer kommen selbst kleinere Unternehmen und Selbständige kaum noch aus. Das gilt für eine Arztpraxis genauso wie für einen Schreiner, für ein Hotel oder eine Spedition. Je abhängiger die Betriebe von der Technik sind, desto gravierender können die Folgen eines Hackerangriffs sein. Legt ein Virus die IT für längere Zeit lahm, steht im schlimmsten Fall die Existenz der Firma auf dem Spiel. Eine Cyberversicherung bewahrt Unternehmen vor diesem Schicksal. Sie zahlt eine vereinbarte Entschädigung, wenn eine Attacke den Geschäftsbetrieb ganz oder teilweise zum Erliegen bringt, und springt für Schadenersatzforderungen von Kunden für Datenmissbrauch oder Lieferverzug ein. Eine Cyberversicherung ist aber mehr als eine reine Schadensversicherung: Weil nach einem Angriff jede Minute zählt, um die Auswirkungen zu begrenzen, und weil auch die Rechte von Dritten berührt sein können, bietet eine Cyberpolice je nach Anbieter zugleich wichtige Serviceleistungen. Diese helfen gerade kleineren Unternehmen, denen das entsprechende Know-how oft fehlt, mit einer solchen schwierigen Situation besser umzugehen.

Ein Umdenken findet statt

Die Komplexität der Informationssicherheit ist zwar häufig noch nicht vollständig erkannt, und das entsprechende Gefahrenpotenzial wird noch zu oft unterschätzt. Die Nachfrage nach umfassenden Cyberversicherungen hat jedoch auch in Liechtenstein deutlich zugenommen. Die globalen Cyberangriffswellen im Jahr 2020 und die verschärften Datenschutzgesetze haben zu einem Umdenken in den Unternehmen geführt.

Bevor eine Versicherungslösung in Betracht gezogen wird, müssen Unternehmen aber auf jeden Fall ihr individuelles Cyber-Restrisiko kennen. Damit ein Betrieb eine Cyberversicherung abschliessen kann, muss seine IT ein Mindestmass an Schutz aufweisen. Das ist bei Versicherungen nichts Ungewöhnliches: Auch seinen Hausrat kann beispielsweise niemand versichern, der keine abschliessbare Wohnungstür hat. Für eine Cyberversicherung müssen Betriebe zum Beispiel einen Virenschutz installiert haben, ihre Unternehmensdaten mit individualisierten Zugängen für Mitarbeiter sichern und eine regelmässige Datensicherung durchführen.

Gut investierte Zeit

Viele Versicherer haben Cyberversicherungen in ihrem Portfolio. Es empfiehlt sich daher für Geschäftsführer oder -inhaber, die sich gegen die Folgen von Cyberangriffen absichern möchten, Kontakt mit dem Versicherungsberater oder -broker ihres Vertrauens aufzunehmen und ein Beratungsgespräch zu vereinbaren. Ein oder auch mehrere solcher Gespräche sind gut investierte Zeit, verglichen mit dem Schaden, den ein Cyberangriff verursachen kann.