Daten-Diebstahl kann versichert werden

Versicherungsunternehmen reagieren zunehmend auf die rasante Zunahme der Internetkriminalität. Allein im Jahr 2012 wurden in Deutschland rund 64.000 Fälle von Cybercrime registriert. Auch viele KMU sind davon betroffen. Darüber sprach Der Mittelstand. mit Natalie Kress, Cyber Practice Manager Germany & Austria der ACE Group (ACE) in Frankfurt und Tim Bormann, dem Leiter des Versicherungsmaklers DMM Deutsche Mittelstands Makler GmbH aus Osnabrück.

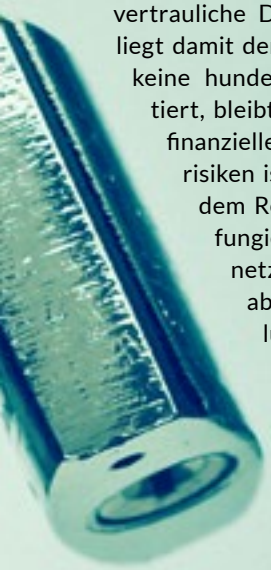
Foto: © wk1003mike - Shutterstock.com

Der Mittelstand.: Versicherungen gegen Daten-Diebstahl sind auf dem angloamerikanischen Markt bereits sehr verbreitet. Nun werden auch hierzulande Cyber-Versicherungen angeboten. Ist das wirklich notwendig?

Tim Bormann: Unbedingt. Ein erfolgreicher Hacker-Angriff auf ein Großunternehmen verursacht einen durchschnittlichen wirtschaftlichen Schaden von 1,8 Millionen Euro. Bei kleinen und mittelständischen Unternehmen liegt der Durchschnittswert bei 70.000 Euro. Der Schaden, der sich aus allen Hacker-Angriffen auf deutsche Firmen insgesamt pro Jahr ergibt, lag 2011 laut Bundeskriminalamt bei 70,2 Millionen Euro. Da die Dunkelziffern sehr hoch sind, ist zu vermuten, dass der tatsächliche wirtschaftliche Schaden jedoch um ein vielfaches höher ist.

Warum sollten Mittelständler die zusätzlichen Kosten einer Cyberpolice auf sich nehmen?

Natalie Kress: Unternehmen sind hochgradig technikabhängig, unabhängig von ihrer Größe. Heute verarbeitet so gut wie jeder sensible Daten – ob die der eigenen Mitarbeiter oder vertrauliche Datensätze Dritter – und unterliegt damit dem Bundesdatenschutzgesetz. Da keine hundertprozentige IT-Sicherheit existiert, bleibt immer ein Restrisiko – und das finanzielle Schadenpotenzial von Cyberrisiken ist enorm. Eine Cyberpolice hilft, dem Restrisiko gerecht zu werden und fungiert als zusätzliches Sicherheitsnetz, um die finanziellen Verluste abzudecken, die durch den Verlust oder die Manipulation der eigenen Daten und Programme entstanden sind. Wichtiger Teil der Cyberpolice ist auch die Unterstützung und Fachkenntnis im Schadenfalls, denn hier gilt: schnellstmöglich handeln, um weitere Schäden zu vermeiden. Denn wird ein Cybervorfall seitens des betroffenen Unternehmens nicht entsprechend gehandhabt, kann dies durchaus zur realen Gefahr werden, Gewinneinbrüche, Reputationsschäden und unter Umständen im äußersten Fall sogar die Insolvenz der Firma nach sich ziehen.



Ist eine Cyberpolice nicht eher etwas für große Unternehmen?

Tim Bormann: Kein Unternehmen ist heute mehr vor Cyberangriffen gefeit, unabhängig ob es sich um Kleinunternehmen, Mittelständler oder Großkonzerne handelt. Ein beliebtes Ziel für Cyberkriminelle sind dabei nach wie vor die klassisch hochexponierten Branchen, wie der Einzelhandel oder das Finanz- und Versicherungswesen. Aufgrund der zahllosen Transaktionen und den enormen Mengen vertraulicher Daten in jenen Geschäftsbereichen gelten diese als besonders lukrativ für Cyberkriminelle. Dennoch gilt: Ins Visier kann mittlerweile jeder geraten.

Schließen Geschäftsführer die Police möglicherweise nur deshalb ab, damit sie selbst aus der Haftung sind?

Natalie Kress: Die Absicherung von Cyberrisiken ist für Führungskräfte ein wichtiges Thema, da ihre Organisationspflicht auch den IT-Bereich umfasst. Sie müssen dafür sorgen, dass ihr Unternehmen so gut wie möglich vor IT-basierten Risiken geschützt ist, zum Beispiel indem sie bestimmte IT-Sicherheitsrichtlinien umsetzen. Kommen sie ihrer Pflicht nicht nach, und kommt es dadurch zum Cyberschaden, kann dieser als Organisationsverschulden gewertet und die Verantwortlichen dafür schadensersatzpflichtig belangt werden. Für Geschäftsführer besteht dadurch ein enormes Gefahrenpotenzial.

Was empfehlen Sie für eine Rund-Um-Absicherung bei einem größeren Mittelständler mit 500 Mitarbeitern?

Tim Bormann: Um die spezifischen Gefahren eines Unternehmens abdecken und so individuellen Schutz bieten zu können, bedarf es einer detaillierten Risikoanalyse. Nur so können Risikopotenziale erkannt, bewertet und entsprechend gehandhabt werden. Abhängig beispielsweise von der jeweiligen Qualität der IT-Sicherheit, der Größe oder auch der Branche eines Unternehmens ergibt sich daraus die individuell auf den Kunden zugeschnittene Höhe der Prämie und der Deckungslimits. ■

Tim Bormann
Leiter DMM Deutsche Mittelstands Makler GmbH (DMM)

www.mittelstandsmakler.com

Natalie Kress
Cyber Practice Manager Germany & Austria
ACE Group, Frankfurt

www.acegroup.com/de