It und Internet – das unsichtbare Risiko

Der Ausfall eines Rechners oder ein Programmabsturz können erhebliche Schäden verursachen. Große Bedeutung haben in den letzten Jahren aber die Schäden erlangt, die durch Cyber-Kriminalität entstehen können. Dabei geht es nicht nur um Datenklau, sondern auch um Schäden, die durch den gezielten Angriff auf die Daten des Unternehmens entstehen.

Udo Giesen
Geschäftsführer der
Profinanz Versicherungsmakler GmbH

Aus der weltweiten Vernetzung der Informationstechnologie ergeben sich weitere Risiken, die unter dem Begriff Cyber-Risiken Bedeutung erlangt haben. Jeder mit dem Internet verbundene Nutzer ist angreifbar. Hackerangriffe auf Sony, Google, TARGET, Amazon, TV5 Monde, die Nato und den Deutschen Bundestag zeigen die Dimensionen auf. IT-Sicherheitsexperten weisen darauf hin, dass es unmöglich geworden sei, Datenschutzverletzungen zu verhindern. Gehen Sie davon aus, dass Ihr Netzwerk bereits kompromittiert ist. Es gibt heute nur noch zwei Arten von Unternehmen: Solche, die bereits gehackt wurden und solche, die noch gehackt werden.

Vielen Unternehmen ist nicht bewusst, dass es versicherbare Risiken gibt. Eine Reihe von Versichererungsmaklern bieten Absicherungsmöglichkeiten und unterstützen Unternehmen bei der Risikoanalyse

Bedrohungspotenziale
Die digitale Vernetzung erhöht die Anfälligkeit für Angriffe. Cyber-Attacken steigen im gleichen Maße, wie auch die Abhängigkeit der Beteiligten von den IT-Strukturen zunimmt. Sie ist für Unternehmen nicht nur vorteilhaft, sondern birgt auch Risiken. IT-Systeme ohne Schwachstellen gibt es leider nicht. Angreifer sind ständig auf der Suche nach solchen Schwachstellen.

Typische Schwachstellen sind:
- Programmierfehler
- Konfigurationsfehler
- Konzeptionsfehler in Programmiersprachen
- Menschliches Fehlverhalten, wenn z. B. ein IT-Anwender aufgrund einer Phishing Mail seine Pin in falsche Hände gibt.

Dabei wird unterschieden, ob Schäden von außen oder intern durch Mitarbeiter verursacht werden. Kosten resultieren beispielsweise aus Betriebsunterbrechungen und Umsatzausfall, weil Systeme nicht funktionieren, Drittschäden durch Abfluss von Kundendaten, durch Analyse des Vorfalls für Anwälte oder auch Systemtechniker und vieles mehr.

IST-Analyse des Risikos
Um ein Risiko bewerten zu können, steht am Anfang die Frage, von welchen Cyber-Risiken das Unternehmen bedroht ist, insbesondere durch:

- Datenverluste und Datenschutzverletzungen
- Hackerangriffe oder auch Erpressungen dadurch
- Persönlichkeitsverletzungen
- Ausspähen von Daten und Geschäftsgeheimnissen
- Ertragsausfälle durch Betriebsunterbrechungen usw.

Der Ermittlung möglicher Risiken und speziellen und individuellen Aspekten des eigenen Unternehmens hinsichtlich Schadenverhütung, Prävention und Risikotragung sollte angemessene Zeit zugestanden werden.

Die analysierten Risiken gilt es entweder durch Risikoverbesserungen oder durch Risikotransfer abzusichern.

Bei dem Risikotransfer auf Versicherungen ist die jeweilige Analyse die Basis für einen richtigen Schutz. Vorhandene Anbieter bieten sehr differenzierte Policen an, die miteinander verglichen werden sollten.

Praxistipp
Zur Absicherung gehört neben der Risikovermeidung auch der richtige Versicherungsschutz für die Kosten, die aus Cyber-Schäden entstehen. Kosten der Analyse des Schadens, der Betriebsunterbrechung, der Informationspolitik können schnell sechs- bis siebenstellig werden. Daher ist es um so wichtiger, die richtige Absicherung zu finden.


Foto: flown_pixelio.de