

## Haftung und Rechtssicherheit bei der Datensicherung

Obwohl bei deutschen Unternehmen das Thema Datensicherung und Datensicherheit an Bedeutung gewonnen hat, setzen sich nur wenige mit dieser Problematik hinreichend auseinander. In einer Vielzahl deutscher Unternehmen bestehen erhebliche Sicherheitslücken im Bereich der Informationstechnik. Dies birgt nicht nur das Risiko schwerer wirtschaftlicher Einschnitte, sondern zugleich ein enormes Haftungsrisiko für die Unternehmen, deren Unternehmensführung und nicht zuletzt auch für deren Mitarbeiter.

Nur nahezu jedes zweite deutsche Unternehmen nimmt sich ausreichend Zeit, um die eigenen IT-Systeme zu sichern und eine eigene IT-Sicherheitsstrategie zu erstellen. Gerade die Budgetverantwortlichen sehen wegen mangelnder Fachkenntnisse kaum Veranlassung, Sicherheitsinvestitionen vorzunehmen und ihre IT-Manager sowie IT-Sicherheitsexperten aktiv zu unterstützen. Da aber in ca. 75% der deutschen Unternehmen die Unternehmensführung über die Ausgaben für diesen Bereich entscheidet und das Risiko- und Haftungsbewusstsein nur mangelhaft bis gar nicht ausgeprägt ist, genügt das IT-Security-Management häufig nicht einmal den gesetzlichen Anforderungen.

Bei unzureichender IT-Security und mangelhafter Datensicherung tragen die Unternehmen bzw. deren Unternehmensführung grundsätzlich die volle Verantwortung und somit das gesamte Haftungsrisiko. Daneben besteht auch für IT-Manager und IT-Sicherheitsexperten das nicht unerhebliche Haftungsrisiko, sich für eine schuldhaft Verletzung der auf ihn übertragenen Pflichten zur ordnungsgemäßen Datensicherung und Gewährleistung der IT-Security aus dem jeweiligen Vertragsverhältnis ersatzpflichtig zu machen. Hinzu kommt die Gefahr einer Abmahnung und im Wiederholungsfalle die einer Kündigung.

Letztendlich entscheidend für die IT-Security in deutschen Unternehmen ist die Konkretisierung der Anforderung einer ordnungsgemäßen Datensicherung. Die Sicherung der Daten muss täglich, die Vollsicherung mindestens einmal wöchentlich erfolgen. Zudem muss ein Backup räumlich getrennt von den IT-Systemen aufbewahrt werden, die gesicherten Daten sollten verschlüsselt sein.

Als zuverlässige und rechtskonforme Datensicherung bietet sich ein so genanntes Remote Backup, wie z.B. der Datensicherungsservice ReBack von netcos AG ([www.re-back.de](http://www.re-back.de)) an. Dabei werden die Daten verschlüsselt, über eine Internetleitung in ein sicheres Rechenzentrum übertragen und dort abgelegt. Durch die Verschlüsselung ist ein Missbrauch der Daten ausgeschlossen. Die gesicherten Daten selbst liegen getrennt vom System. Eine Sicherung kann mehrmals täglich, auf Wunsch sogar nach jeder Änderung durchgeführt werden. Da die Sicherung ganz automatisch im Hintergrund läuft, werden Arbeitsprozesse nicht beeinflusst. Damit werden alle Anforderungen des Gesetzgebers erfüllt. Auch eine Rücksicherung im Fall der Fälle gestaltet sich hier einfacher und schneller. Unsicherheitsfaktoren wie unzuverlässige Hardware, Katastrophen oder menschliche Unwägbarkeiten können weitgehend ausgeschlossen werden.