

## **Thema: Sicher vor Datenverlust**

München, September 2008: Gerade in letzter Zeit häufen sich Meldungen aus Großbritannien über verlorengegangene hochsensible Daten. So tauchte auf Ebay eine Festplatte mit detaillierten Bankkundendaten auf, ein USB-Stick mit Daten von Gefangenen verschwand spurlos. Experten schätzen, dass in der Vergangenheit bereits mehrere Millionen Datensätze abhanden gekommen sind. In den meisten Fällen befanden sich diese Daten auf mobilen Geräten wie CDs, USB-Sticks, Magnetbänder, externe Festplatten oder Laptops.

Doch auch hierzulande sind die Daten nicht sicher. Laut einer Studie von Clearswift GmbH verzeichneten rund 7,5 % der 150 befragten IT-Entscheider in den vergangenen eineinhalb Jahren mindestens einen Fall von Datenverlust in ihrer Firma. Über zwei Drittel der befragten Teilnehmer gaben an, wegen eines drohenden Imageschadens einen möglichen Datenverlust nicht zu melden. Aber nicht nur die wirtschaftlichen Folgen können erheblich sein, Schadensersatzpflicht sowie persönliche Haftung der Geschäftsführung können nach einem schwerwiegenden Datenverlust mögliche rechtliche Folgen sein.

Es ist immer riskant, hochsensible Daten unverschlüsselt auf mobile Datenträger zu speichern, egal ob diese das Haus verlassen sollen oder nicht. Dies betrifft ebenso Medien für die Datensicherung, selbst wenn der Weg zum Tresor nur ein kurzer ist. Denn auch bis dorthin können diese vergessen, verloren oder gestohlen werden. Grundsätzlich gilt, Daten sollten immer verschlüsselt sein, sobald das Medium, auf das sie gespeichert werden, theoretisch das Firmengebäude verlassen kann.

Als sichere Alternative zur herkömmlichen Datensicherung auf Speichermedien bietet sich ReBack an, der Remote Backup Service von netcos AG ([www.re-back.de](http://www.re-back.de)). Hier werden die Daten lokal hochgradig verschlüsselt, dann erst über eine Datenleitung zu einem entfernten Rechenzentrum übertragen und dort verschlüsselt abgelegt. Zum einen sind diese Daten sicher geschützt vor dem Zugriff Unberechtigter. Die verschlüsselten Daten können nur mit einem persönlichen Schlüssel, den der Anwender selbst erzeugt hat, ausgelesen werden. Zum anderen können die so gesicherten Daten bei einem Datencrash schnell, einfach und zuverlässig wiederhergestellt werden. Unsicherheitsfaktoren wie unzuverlässige Hardware, Katastrophen oder menschliche Unwägbarkeiten können hier ausgeschlossen werden. Ein Imageschaden sowie rechtliche Folgen sind in diesem Falle abgewendet.

Pressekontakt:  
Stanislaw Panow  
netcos AG  
Richard-Strauss-Straße 71  
81679 München  
089/45221622