

# Datendiebe begehen selten einen «Datenklau»

Daten gehen verloren – absichtlich, unabsichtlich oder durch kriminelle Energie. Die Angst davor ist gross, vor allem im Hinblick auf die eigenen Mitarbeiter. Wie sieht die Situation aber auf juristischer Ebene aus? Und was ist bei der Abwehr erlaubt? Christian Walter

«Datenklau» ist ein Thema, das in den letzten Jahren an Präsenz in den Medien gewonnen hat. Angefangen bei der erstarkten Cybermafia, die auf höchst professionelle Weise Ziele auf der ganzen Welt angeht und kommerziell ausschachtet, bis zur Bedrohung durch den eigenen Mitarbeiter, der sich bereichern will. Diverse Diebstähle von Kreditkarten sowie die Bankdaten, die verschiedenen Steuerbehörden zum Kauf angeboten wurden, mögen hier als Beispiele dienen. Mit anderen Worten: Datenklau hat viele Gesichter. Damit hört es allerdings nicht auf, denn der Begriff selbst ist mehr als nur ein bisschen schwammig, vor allem aus rechtlicher Sicht. Gerade bei der Entwendung heikler Unternehmensdaten durch die eigenen Mitarbeiter handelt es sich selten um den Tatbestand der sogenannten «unbefugten Datenbeschaffung», wie David Rosenthal, Konsulent bei Homburger und Experte für IT-Recht, vor kurzem auf einer Veranstaltung der ISSS (Information Security Society Switzerland) ausführte.

Das Schweizer Strafgesetz (Artikel 143) gibt hier eine enge Definition vor. Demnach muss es sich erstens um eine Beschaffung elektronischer Daten handeln, zweitens, die Daten dürfen nicht für den Täter bestimmt sein, drittens, der Täter will sich oder andere unrechtmässig bereichern und viertens, die Daten waren gegen den «unbefugten Zugriff» besonders geschützt. Das Gesetz erfasst also nur entweder externe Angreifer oder interne, die über keinen gültigen Zugriff verfügen.

## Altes Recht gilt

Genauso wenig greift der Tatbestand des «unbefugtes Eindringens». Im Unterschied zur unbefugten Datenbeschaffung fehlt hier die Bereicherungsabsicht. Das Gesetz richtet sich nur gegen den klassischen Hacker, der aus Spass oder Neugier in ein System eindringt. Schliesslich handelt es sich auch um keine Straftat gegen den «Geheim- und Privatbereich». Da einerseits verschlüsselt übermittelte elektronische Daten keine Schrift sind, also auch das Schriftgeheimnis nicht verletzt werden kann, und andererseits selten unbefugt Personendaten beschafft werden. Potenzielle Erpresser vergreifen sich meist nicht an



Wer Daten klaut, ist nicht unbedingt ein Datendieb nach Schweizer Recht. Bildquelle: Fotolia, Montage Netzwoche

Daten wie der Krankengeschichte der Mitarbeiter. Somit greift auch das Datenschutzgesetz nicht. «Das Recht bietet allerdings genug andere Möglichkeiten, um sich der Datendiebe zu erwehren», so Rosenthal. Es greifen unter Umständen Dinge wie die unerlaubte Bekanntgabe, Persönlichkeits- oder Vertragsverletzung, Erpressung oder sogar das Urheberrecht. Bereiche also, die auf den ersten Blick wenig mit der digitalen Welt zu tun haben, dafür aber umso wirksamer sind.

## Staaten verklagen

Somit stehen den betroffenen Unternehmen eine Reihe von Möglichkeiten zur Verfügung, die sowohl aus dem Bereich des Strafrechts als auch des Zivilrechts kommen. Jedes dieser Instrumente hat allerdings seine Vor- und Nachteile. Das Zivilrecht, ganz allgemein gesprochen, erlaubt ein höheres Mass an Kontrolle über das Verfahren, birgt aber auch ein grösseres Risiko als das Strafrecht. Wo man selbst als Kläger auftritt, muss man nämlich bei einer Niederlage selbst die Gerichtskosten tragen. Dafür bietet das Zivilrecht wieder den Vorteil, auch über die Grenzen hinaus wirksam zu sein. Es erlaubt sogar ein Vorgehen gegen andere Staaten. Beim Strafrecht muss sich zuerst der Bundesrat einschalten. Das macht er nicht gern, da so unliebsame politische Konsequenzen ausgelöst werden könnten. Als Beispiel dient hier wieder der vor kurzem erfolgte Diebstahl der Bankdaten,

die dem deutschen Fiskus angeboten wurden. Finanzminister Schäuble wurde deswegen bisher nicht angeklagt, auch wenn er als Nutzniesser des Diebstahls durchaus vom Gesetz her belangt werden könnte.

## Grenzen der Überwachung

Die Gesetze befassen sich aber nicht nur mit den Folgen für Diebe und Nutzniesser. Ein bestohlenen Unternehmen muss sich immer zwei Fragen stellen: Hat es die gesetzlichen Mindestanforderungen zum Schutz der Daten erfüllt? Erfolgte die Preisgabe der Daten für einen unbefugten, unverhältnismässigen Zweck und gegen das Gebot von Treu und Glauben? Muss mindestens eine der beiden Fragen mit Ja beantwortet werden, drohen rechtliche Konsequenzen.

Das Thema ist also alles andere als unkompliziert. Darum liegt die Schlussfolgerung nahe, dass ein ungewollter Datenabfluss möglichst verhindert werden sollte. Aus technischer Sicht nennt sich das Ganze «Data Leakage Prevention» und eine Reihe von Unternehmen bietet verschiedenste Lösungen. Eine Variante ist die Überwachung des Mitarbeiters auf Verdacht oder auch verdachtsunabhängig. Doch auch hier gelten Gesetze, deren oberste Maxime lautet: Der Persönlichkeitsschutz setzt der Überwachung von Mitarbeitenden Grenzen, betont Karin Koç vom Büro des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Die Überwachung darf nicht dem Interesse der Verhaltensüberwachung dienen. Ausserdem müssen die Arbeitnehmer einerseits bei der technischen Einrichtung der Überwachung einbezogen und andererseits darf deren Gesundheit und Bewegungsfreiheit nicht beeinträchtigt werden. Was nicht heisst, dass im Einzelfall eine geheime Überwachung über einen kurzen Zeitraum unzulässig ist. Allerdings sind diese Fälle meist heikel und sollten vorher mit dem Büro des EDÖB abgeklärt werden. In der Schweiz sind diese Dinge merkwürdigerweise nur auf Verordnungsstufe geregelt und nicht auf Gesetzesebene. Eine Tatsache, mit der auch das Bundesgericht bei einem Urteil über geheime Videoüberwachung konfrontiert wurde. <