Wenn Mitarbeitende Daten klauen: So schützt man sein Unternehmen

Datendiebstahl – ein unterschätztes Risiko

Sybille Zingg Righetti
Rechtsanwältin
Bracher & Partner, Advokatur und Notariat, Langenthal, Bern und Biel
sybille.zingg@bracherpartner.ch

Die fortschreitende Digitalisierung in einem Unternehmen bietet neben den Vorteilen auch neue Angriffsflächen. Ein unberechtigter Zugriff auf Daten bzw. deren unrechtmässige Verwendung insbesondere auch durch Arbeitnehmer ist längst keine Seltenheit mehr.

In den Medien diskutiert werden lediglich Aufsehen erregende Fälle wie beispielsweise jener der Hyposwiss (NZZ Nr. 287, 10.12.2013, S. 14). In diesem Fall lud ein ehemaliger IT-Mitarbeiter an seinem letzten Arbeitstag 32 Gigabyte Daten auf einen Memory-Stick, da er sich von seinem Chef schikaniert fühlte. Anderthalb Jahre später, als er aus den Medien von einem Streit zweier russischer Milliardäre vernahm, bei welchem dem einen Geldwäscherei über Hyposwiss vorgeworfen wurde, packte er seine Gelegenheit: Er bot Belege über kompromittierende Transaktionen für zwei Millionen Franken dem Rechtsanwalt des einen Milliardärs zum Kauf an. Dieser avisierte jedoch die Bundesanwaltschaft, womit der Plan fehlschlug und der Datendiebstahl ans Licht kam. Es gibt jedoch eine Vielzahl von Fällen, in welchen die Öffentlichkeit und gar die Strafverfolgungsbehörden nie etwas von einem erfolgten Datendiebstahl erfahren – die Dunkelziffer ist entsprechend hoch.

Geradezu typisch ist das Szenario, in welchem der Mitarbeiter kurz vor Beendigung des Arbeitsverhältnisses, beispielsweise bei einem Wechsel innerhalb der Brache, sensible Daten kopiert, welche er dann an Dritte weiter veräussern oder zu seinem eigenen Vorteil nutzen will. Besonders beliebt sind dabei Datenbanken mit Kundenkontakten, strategische Pläne oder technisches Know-how. Beim Entwenden von Daten, welche dem Unternehmen schaden könnten, steht oftmals das Motiv der Rache aufgrund empfundener Ungerechtigkeiten oder aber das Ziel der Erpressung des Unternehmens im Vordergrund. Der unberechtigte Zugriff auf Daten oder deren unrechtmässige Verwendung kann schwerwiegende Folgen für ein Unternehmen haben. Bester Schutz gegen solche Delikte durch Mitarbeiter bieten präventive Massnahmen.

Vorbeugende Massnahmen

In erster Linie schafft Aufklärung und die Sensibilisierung im Umgang mit Daten das nötige Bewusstsein bei den Mitarbeitenden, so dass die Hemmschwelle für Datendiebstahl höher ist.

Technische Massnahmen wie die Verschlüsselung von Daten, Servern und Kommunikationswegen, das Sperren von Schnittstellen und das Monitoring von Systemen sorgen dafür, dass Zugangsberechtigungen klar definiert werden, Kopiervorgänge nur beschränkt möglich sind und illegales Kopieren nachweisbare Spuren hinterlässt.

Auch **organisatorische Massnahmen,** wie insbesondere das restriktive Erteilen von Zugriffsberechtigungen, das Erstellen von Richtlinien zur Datenbearbeitung, das Vorsehen von vertraglichen Geheimhaltungsvereinbarungen mit Androhung einer Konventionalstrafe, vorbeugende Personen-Sicherheitsüberprüfungen und das kontrollierte Entsorgen sensibler Daten, können einem Datendiebstahl vorbeugen. Auch ein Überwachen der Arbeitnehmenden könnte Abhilfe schaffen, ist jedoch rechtlich nur sehr beschränkt zulässig und überdies unter Umständen mit erheblichem Aufwand verbunden.

Sollte es trotz Präventivmassnahmen zum Datendiebstahl kommen, stehen sowohl straf- als auch zivilrechtliche Möglichkeiten zur Verfügung, welche je nach den Umständen des Einzelfalls geprüft werden müssen.

Strafrechtliche Massnahmen

Das Strafrecht kann griffige Mittel bieten; dazu gehört beispielsweise die Sicherstellung der gestohlenen Daten und allenfalls die Verhaftung des Täters. Durch die Behelfe des Strafrechts wird primär Druck gegenüber dem Täter aufgebaut, zudem wirkt das Ergreifen dieser Massnahmen gegenüber potentiellen Nachahmern abschreckend.

Der unberechtigte Zugriff auf Daten oder deren unrechtmässige Verwendung kann eine Vielzahl von Straftatbeständen erfüllen. Wichtig ist, vor jeder Strafanzeige zu prüfen, welche Risiken dadurch geschaffen werden. Ein Strafverfahren kann nämlich relativ geräuschlos verlaufen, aber auch mediale Aufmerksamkeit generieren.

Ein Strafprozess kann ausserdem sehr langwierig und kostenintensiv sein und betriebliche Kapazitäten belegen. Weil die Verwendung von gestohlenen Daten unter Umständen aber zu nicht kontrollierbaren Schäden beim betroffenen Unternehmen führen kann, bleibt häufig keine andere Wahl, als sämtliche verfügbaren Massnahmen – und damit auch die Mittel des Strafrechts – zur schnellstmöglichen Schadensbekämpfung zu ergreifen. Es gilt dabei jedoch stets, das Risiko einer ausufernden und allzu umfangreichen Strafuntersuchung zu vermeiden. Eine Strafanzeige sollte deshalb immer durch einen Experten ausgearbeitet werden; von einer mündlich bei der Polizei deponierten Anzeige ist abzuraten.

Zivilrechtliche Massnahmen

Neben der strafrechtlichen Verfolgung des Täters stehen dem betroffenen Unternehmen auch diverse zivilrechtliche Mittel zur Verfügung. So können Unterlassungsansprüche (beispielsweise ein Verbot der Weitergabe oder Veröffentlichung der gestohlenen Daten) mittels vorsorglicher Massnahme rasch und bei besonderer zeitlicher Dringlichkeit mittels superprovisorischer Massnahmen sogar umgehend durchgesetzt werden. Im ordentlichen Prozess kann schliesslich die Rückgabe des Datenträgers oder Schadenersatz und Gewinnherausgabe eingeklagt werden. Schadenersatzansprüche und Ansprüche auf Gewinnherausgabe sind in der Regeln jedoch sehr schwierig zu beziffern bzw.

nachzuweisen. Im laufenden Arbeitsverhältnis stehen zudem die Instrumente des Arbeitsrechts zur Verfügung, wie beispielsweise die Abmahnung oder in schwerwiegenderen Fällen die fristlose Entlassung des Mitarbeitenden.

Haftung des Unternehmens und der Organe

Datendiebstahl stellt nebst den finanziellen Risiken und der drohenden Reputationsschäden auch eine nicht zu unterschätzende rechtliche Gefahr für das Unternehmen und dessen Organe dar.

Nach geltendem Recht ist eine strafrechtliche Haftung des Unternehmens selbst möglich, wenn eine mangelhafte Organisation vorliegt und aufgrund dessen keine Rückverfolgung der Tat auf bestimmte natürliche Personen möglich ist. Sofern also ein strafrechtlich relevanter Datendiebstahl insbesondere bei Schädigung von Drittpersonen aufgrund ungenügender Massnahmen nicht einer bestimmten Person im Unternehmen zugeordnet werden kann, könnte im Endeffekt gar das Unternehmen selbst mit einer Busse belegt werden. Schliesslich kann bei mangelhafter Sorgfalt der Geschäftsleitung, beispielsweise in der Überprüfung der Einhaltung der Datenschutzgesetzgebung, auch eine zivilrechtliche Haftung derselben entstehen. Auch unter diesem Blickpunkt sind Präventivmassnahmen gegen Datendiebstahl von zentraler Bedeutung.

Wenn trotz aller Prävention ein Datendiebstahl durch Beschäftigte erfolgt, ist es von grosser Wichtigkeit, die im konkreten Einzelfall passenden Massnahmen zu ergreifen. Es empfiehlt sich dabei in der Regel der Beizug eines Rechtsexperten, um die Schäden und Risiken zu minimieren.