Vieldiskutiertes Phänomen

Datendiebstahl in einem KMU: Strafrechtliche Aspekte

Von Dr. iur. Cornel Borbély

Datendiebstahl ist für die meisten Unternehmen eine alarmierende, wenn auch abstrakte Gefahr – der gestohlene Gegenstand ist immateriell und nicht ‹greifbar›, die Tatwaffe nicht vorhanden.

Datendiebstahl kann in einem Unternehmen zu einem erheblichen Schaden führen, verbunden mit Reputationsverlust. Die Geschäftsleitung ist sich dabei oft nicht bewusst, dass mangelhafte Sicherungsmassnahmen auch zu persönlicher Verantwortlichkeit führen können.

Interne Mitarbeiter als Datendiebe

Fälle von *Datendiebstahl* bzw. *Datenklau* werden in den Medien breit diskutiert. Insbesondere ist an die Berichterstattung über Entwendungen von ganzen Kundenstämmen bei Banken zu denken. Meist handelt es sich um Konstellationen, bei denen ein Mitarbeiter Informationen über Bankkunden kopiert, um diese später via Mittelsmänner zu verkaufen. Empfänger sind Privatpersonen, Firmen oder ausländische (Steuer-)Behörden. Ebenfalls kommt vor, dass eine bestohlene Firma zum Rückkauf von entwendeten Daten erpresst wird – wobei ein kopierter Datensatz später trotz Rückkauf dennoch in Umlauf kommt. Bei Industrieunternehmungen ist zudem an Konkurrenzfirmen zu denken, welche auf diese Weise von geheimen Forschungsergebnissen profitieren wollen. Im Bankenumfeld war der *Fall Bradley Birkenfeld* besonders prominent. Als ehemaliger Mitarbeiter der UBS übergab er Kundendaten an US-Steuerbehörden und erhielt dafür von denselben eine Belohnung von über 100 Mio. USD[1].

Abgesehen von diesem Modus Operandi sind ebenfalls weitere Möglichkeiten der illegalen Datenbeschaffung bekannt. Zu denken ist an das klassische Eindringen in ein Computersystem *von ausserhalb einer Unternehmung* (sogenanntes *Hacking*). Diese Cyberangriffe führten jüngst vermehrt zu medialen Berichterstattungen. Hier ist insbesondere das Schädigungspotential der Attacken bemerkenswert:

- Hackerangriff auf das U.S. Office of Personnel Management (Erlangen von 19.7 Mio. Personaldossiers mit sensiblen persönlichen Daten),[2]
- Hacking von 150 Mio. Adobe-Accounts (Erlangen von mehr als *38 Mio. Nutzerdaten*).[3]

Abzugrenzen ist der Datendiebstahl schliesslich von einer *missbräuchlichen Verwendung* von erlangten Daten, bei welcher Daten vom Endempfänger in unlauterer Weise zum eigenen Nutzen verwendet werden. Der Datendiebstahl stellt dazu eine Vorstufe deliktischen Handelns dar. Sehr verbreitet ist auch die *Datenbeschädigung* mittels Virenprogrammen, welche durch Anhänge in E-Mails oder Download von Dateien übertragen werden.

Computerdelikte

Unter Experten gibt es keine einheitliche Ansicht, ob und in welchem Ausmass Unternehmungen von Computerdelikten, insbesondere von einer internen unbefugten Datenbeschaffung, betroffen sind. Im Kanton Zürich geht die polizeiliche Kriminalstatistik von einer abnehmenden Tendenz aus[4]. Auf der anderen Seite betonen Ermittlungsfirmen das zunehmende Risiko eines Datendiebstahls für KMU[5].

Nach der Erfahrung des Autors ist *keine Abnahme von Computerdelikten* festzustellen. Es werden bei Weitem nicht alle Fälle von Datendiebstählen der Polizei angezeigt, nicht zuletzt, um Publizität infolge einer Strafuntersuchung zu meiden. Hier herrscht für die Strafverfolgungsbehörden eine *erhebliche Dunkelziffer*, welche nicht in deren Statistik einfliesst. Zudem können Computerdelikte nicht immer dem gleichen Tatbestand des Strafgesetzbuches (StGB) zugeordnet werden, was zu einer Verzerrung der Statistik führen kann. Zu berücksichtigen ist ebenfalls, dass betroffenen KMUs eine Vielzahl von Delikten nie oder erst nach Jahren bekannt werden.

Unkontrollierbares Risiko

Daten sind kein klassisches Tatobjekt. Bei Tötungsdelikten gibt es die Tatwaffe, bei einem Autodiebstahl das Fahrzeug. Daten auf der anderen Seite sind *beliebig und schnell reproduzierbar.* Sie können weltweit innert Sekundenbruchteilen ausgetauscht werden. Täter nutzen dabei Proxy-Server, welche auf der ganzen Welt verteilt sind. Die Endlagerung kann rein virtuell auf Clouds erfolgen, auch kann die Beute in kleine Dateneinheiten aufgeteilt und an beliebigen Orten gelagert werden. Besonders gravierend ist die Tatsache, dass selbst aufgefundene Datensätze

Dr. Cornel Borbély, ist Rechtsanwalt in Zürich. Als ehemaliger Staatsanwalt und Gruppenleiter für Strafrecht im Kanton Zürich hat er langjährige Erfahrung in der Begleitung und Führung von nationalen und internationalen Verfahren. Nebst seiner Tätigkeit als Rechtsanwalt ist Cornel Borbély in diversen Gremien sowie in der Militärjustiz engagiert. Daneben doziert er an verschiedenen Universitäten und Fachhochschulen in den Bereichen Wirtschaftsstrafrecht und Compliance, unter anderem an der Fernfachhochschule FFHS.

Fussnoten

1 *‹UBS-Whistleblower›, NZZ vom 11. September 2012.*
2 *‹Fatale IT-Sicherheitslücke in den USA›, NZZ vom 10. Juli 2015.*
3 *‹Hackerangriffe werden immer bedrohlicher›, NZZ vom 20. Februar 2015.*
4 *Polizeiliche Kriminalstatistik des Kantons Zürich 2014, S. 9.*
5 *Siehe dazu kritisch KILLIAS et al., ‹Wirtschaftskriminalität wird dramatisiert› in NZZ vom 28. Juli 2014.*

keine Garantie bieten, dass nicht etliche *Kopien* im Besitz von kriminellen Händen sind.

Vor diesem Hintergrund relativiert sich die Frage, ob und wie viele Computerdelikte von den Behörden gezählt werden. Tatsache ist, dass eine betroffene KMU einem *nicht kontrollierbaren Risiko* ausgesetzt ist, das in Datensätzen festgehaltene Know-how für immer zu verlieren – mit entsprechendem Risiko für Reputation und Marktfähigkeit. Gerade bei internationalen Sachverhalten stossen *Strafverfolgungsbehörden an faktische und rechtliche Grenzen* und können das Tatgut ‹Daten› nicht mehr sichern.

Strafrechtliche Einordnung der deliktischen Verhaltensweise

Eine betroffene Unternehmung kann im Falle eines Datendiebstahls zivil- und strafrechtliche Schritte einleiten. Auch können sich aufsichtsrechtliche Fragen stellen, falls eine KMU einer Aufsichtsbehörde unterstellt ist (bspw. der Finanzmarktaufsicht). Zivilrechtlich kann ein Datendieb auf *Schadenersatz belangt* werden, bei einem Arbeitnehmer mit dem ganzen Instrumentarium des Arbeitsrechts. Selbstverständlich bleibt dies ein kleiner Trost, wenn eine Unternehmung von Millionenschäden bedroht ist.

Strafrechtliche Verantwortung (der Organe einer bestohlenen Unternehmung)?

Für die Strafverfolgungsbehörden stellt sich unweigerlich die Frage, ob die geschäftsführenden Organe ihre KMU so organisiert haben, dass das Risiko von Delikten minimiert wird. Waren Daten jedem Mitarbeiter frei zugänglich? Wurden Datenverkehrskontrollen eingeführt? Sind sensible Daten verschlüsselt, wie wird ein Backup gelagert?

Massnahmen gegen Datendiebstähle

Griffige Massnahmen kann das Strafrecht bieten, insbesondere die Sicherstellung von gestohlenen Daten sowie die Arrestierung der Täterschaft. Im Falle eines Datendiebstahls durch Mitarbeiter steht in strafrechtlicher Hinsicht insbesondere die Verletzung der folgenden Straftatbestände im Vordergrund:

- Unbefugte Datenbeschaffung (Art. 143 StGB). Es droht eine Freiheitsstrafe von bis zu fünf Jahren. Ein Täter stiehlt hier Datensätze, welche gegen seinen Zugriff besonders gesichert und nicht für ihn bestimmt sind.
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143^{bis} StGB). Hier handelt es sich um den klassischen Hackertatbestand, bei dem via Datenübertragungseinrichtungen ein unberechtigter Zugriff erlangt wird.
- Im Bereich von Industrieunternehmungen besonders relevant ist die Verletzung von *Fabrikations- oder Geschäftsgeheimnissen (Art. 162 StGB)*. Danach wird mit Freiheitsstrafe bis zu drei Jahren bestraft, wer ein solches Geheimnis unrechtmässig verrät. Zu beachten ist, dass dieses Delikt *nur auf Antrag* verfolgt wird; es ist die Willenserklärung der geschädigten KMU nötig, dass eine Behörde aktiv werden soll.
- Das Pendant im Bereich der Finanzbranche ist *Art. 47 des Bankengesetzes (BankG)*. Ein Dieb von Bankkundendaten wird mit Freiheitsstrafe bis zu drei Jahren bestraft, ein Datenhehler verschärft (Art. 47 Abs. 1 lit. c BankG).
- Eine Entwendung von Datensätzen kann diverse andere Bestimmungen des Strafgesetzbuches bzw. seiner Nebengesetzgebung tangieren. Zu erwähnen sind die Bestimmungen des *Bundesgesetzes gegen den unlauteren Wettbewerb (Art. 6 UWG)* sowie *Wirtschaftsspionage (Art. 271 bzw. 273 StGB)*. Ebenfalls sind erweiterte Sachverhaltskonstrukte denkbar, bei denen diverse andere Tatbestände erfüllt sind.

Falls solche Fragen nicht befriedigend beantwortet werden können, kann *dem Geschäftsführer der Vorwurf* gemacht werden, dass er seine Verantwortung nicht wahrgenommen und dadurch ein Computerdelikt ermöglich hat. Dies mit ernstzunehmenden Konsequenzen.

In zivilrechtlicher Hinsicht kann dies zu *Schadenersatzansprüchen gegen einen CEO* führen. Strafrechtlich können unter dem Titel der *ungetreuen Geschäftsbesorgung (Art. 158 StGB) empfindliche (Freiheits-)Strafen* in Aussicht stehen.

Chancen und Risiken einer Strafanzeige

Vor jeder Strafanzeige ist genau zu prüfen, welche Risiken dadurch geschaffen werden. Dabei ist zu berücksichtigen, dass die Strafverfolgungsbehörden eine Straftat im Rahmen ihrer eigenen Planungen untersuchen. Ein Strafverfahren kann relativ geräuschlos ablaufen oder auch mediale Aufmerksamkeit wecken sowie langwierige und kostenintensive Prozesse verursachen. Andererseits kann die illegale Verwendung von Datensätzen zu nicht kontrollierbaren Schäden in KMUs führen. Häufig bleibt diesen aufgrund von Verantwortlichkeits- bzw. aufsichtsrechtlichen Bestimmungen keine andere Wahl, als sämtliche Massnahmen zur Schadensbekämpfung zu ergreifen.

Damit gilt es, das *Risiko einer eskalierenden Strafuntersuchung zu minimieren*. Es bestehen Wege, mit Behörden zusammenzuarbeiten. Verhandlungsspielraum gibt, dass bei Antragsdelikten nach einer zivilrechtlichen Einigung mit einer Gegenpartei auf die weitere Durchführung eines Strafverfahrens verzichtet werden kann (Rückzug des Strafantrags bzw. Desinteresseerklärung). Als Vorbereitung zu einem Strafverfahren und zwecks Grobsteuerung einer Untersuchung sollte eine Strafanzeige durch einen Experten ausgearbeitet werden. Diese ist zu fokussieren, wobei die Balance zwischen Kürze und Substantiierung der Vorwürfe gefunden werden muss. Von einer mündlich zu erstattenden Strafanzeige ist abzuraten; die Erfahrung zeigt, dass die Kernbotschaft so nur erschwert zu platzieren ist. Nicht vergessen werden darf das Risiko, dass eine Strafuntersuchung auch für die eigene Unternehmung eine erhebliche administrative Belastung verursachen kann (Zeugenbefragungen, Editionen von betrieblichen Unterlagen etc.).

Zukunft des Datendiebstahls

Der Diebstahl von Datenstämmen wird für eine KMU eine erhebliche Gefahr bleiben. Aus Kosten- und Effizienzgründen wird vermehrt papierlos gearbeitet, wobei sämtlicher interner und externer Geschäftsverkehr auf Servern dokumentiert ist.

Unternehmen sind für Risiken im Umgang mit Datensätzen sensibilisierter. Dennoch, auch Kriminelle arbeiten in ihrem Bereich hochprofessionell, und der geheime Wissensschatz von KMUs stellt einen Anreiz für kriminelles Handeln dar. Es ist damit davon auszugehen, dass Computerdelikte zur illegalen Erlangung von Informationen über Kunden und betriebliches Know-how von KMUs weiter zunehmen werden. ■