Auf Risiken vorbereitet sein.

Aspekte der Strafbarkeit

Unterschiedliche Formen von Datendiebstahl

von Dr. iur. Cornel Borbély

Persönliche Daten sind inzwischen gefragte Güter. Es gibt dabei unterschiedliche Arten, an die Daten zu kommen. Der folgende Beitrag liefert eine strafrechtliche Würdigung der unterschiedlichen Delikte.

Regelmässig werden neue Fälle von Datendiebstählen bekannt. In der Bevölkerung erwecken solche Fälle Aufsehen, insbesondere wenn dadurch eine Vielzahl von Personen betroffen ist. Sei dies nun im Bereich der Finanzindustrie oder im Umfeld von sozialen Netzwerken.

Medial prominent diskutiert werden die Fälle von Bankdatendiebstahl. Dabei handelt es sich meist um Konstellationen, bei denen ein Mitarbeiter Informationen über Bankkunden kopiert und diese an Mittelsmänner weiterverkauft. Endabnehmer sind Privatpersonen, Firmen oder staatliche Behörden. Bradley Birkenfeld übergab als ehemaliger Bankmitarbeiter Kundendaten an US-Steuerbehörden und erhielt dafür von denselben eine Belohnung von über 100 Millionen USD. Bei Datendiebstählen von Industrieunternehmen ist demgegenüber an Fälle zu denken, bei denen Firmen von geheimen Forschungsergebnissen ihrer Konkurrenz profitieren wollen.

Das klassische Eindringen in ein Computersystem von ausserhalb einer Unternehmung wird als Hacking bezeichnet. Bei solchen Cyberangriffen ist das Schädigungspotenzial der Attacken bemerkenswert: Im Juni 2015 wurde bekannt, dass bei einem Hackerangriff auf das US Office of Personnel Management offenbar 19.7 Millionen Personaldossiers mit sensiblen persönlichen Daten erlangt wurden, beim Hacking von Adobe-Accounts mehr als 38 Millionen Nutzerdaten.

Heute sind Unternehmen im Umgang mit Datensätzen sensibilisierter und kennen teilweise die Risiken. Dennoch, auch Kriminelle arbeiten in ihrem Bereich hoch professionell, und der geheime Wissensschatz von Unternehmen stellt Anreiz für kriminelles Handeln dar. Es ist deshalb davon auszugehen, dass Computerdelikte zur illegalen Erlangung von Informationen über Firmenkunden und der Diebstahl von betrieblichem Know-how weiter zunehmen werden.

Datenverlust als bedingt kontrollierbares 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 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 statistisch erfasst werden. Tatsache ist, dass eine betroffene Unternehmung einem schwer 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.

Strafbarkeit von Datendieben

Eine betroffene Unternehmung kann im Falle eines Datendiebstahls zivil- und strafrechtliche Schritte einleiten. Auch können sich aufsichtsrechtliche Fragen stellen, falls eine Unternehmung einer Aufsichtsbehörde unterstellt ist – beispielsweise der Finanzmarktaufsicht. Zivilrechtlich kann ein Datendieb auf Schadenersatz belangt werden, bei einem Arbeitnehmer mit dem Instrumentarium des Arbeitsrechts. Selbstverständlich bleibt dies ein kleiner Trost, wenn eine Unternehmung von Millionenschäden bedroht ist. Griffige Massnahmen kann das Strafrecht bieten, insbesondere die Sicherstellung von gestohlenen Daten sowie die Arrestierung der Täterschaft.

Konkret steht bei einem Datendieb die Bestrafung für die Begehung folgender Delikte im Vordergrund:

Beim Tatbestand der unbefugten Datenbeschaffung gemäss Art. 143 Strafgesetzbuch (StGB) beschafft sich ein Täter elektronisch gespeicherte oder übermittelte Daten. Diese müssen gegen seinen unbefugten Zugriff besonders gesichert sein. Darin liegt gerade auch die Schwierigkeit in der Anwendung dieses Tatbestandes. Falls eine Firma, die von ihr gespeicherten Daten nicht in zumutbarer Weise schützt, wird ein Täter kaum verurteilt werden. Die unbefugte Datenbeschaffung kann sich auf verschiedene Weise manifestieren. Ein klassischer Fall ist ein Mitarbeiter, welcher interne Sicherheitsschranken überwindet, um Daten auf einen USB-Stick zu kopieren und diese später verkauft. Das Beschaffen kann auch dadurch erfolgen, dass ein Täter Daten unbefugt abfängt, welche von einer Datenübertragungsanlage gesendet werden.

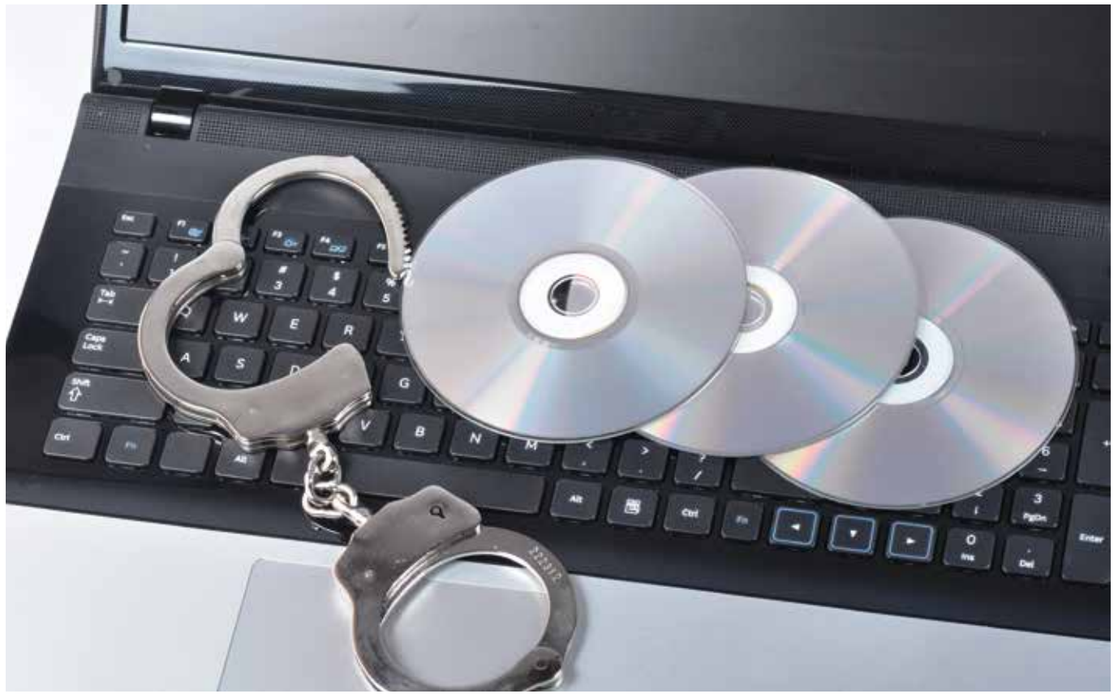
Beim Hacking dringt ein Täter unbefugt in ein für ihn fremdes Computersystem ein. Art. 143bis StGB bestimmt die Strafbarkeit von entsprechendem Verhalten. Der Gesetzgeber verlangt für eine Verurteilung, dass Daten gegen den Eindringling besonders geschützt sein müssen. Die Unternehmung ist in der Pflicht; die Anwendbarkeit dieser Bestimmung wird damit nicht möglich sein, falls eine Firma nicht über genügende Abwehrmechanismen verfügt. Hacking wird nur auf Antrag verfolgt, also nur bei Übermittlung einer Anzeige von der geschädigten Firma. Aus Sicht der Unternehmung sind vor Einreichung einer Strafanzeige verfahrenstechnische Aspekte sowie Reputationsrisiken zu berücksichtigen.

Zur Bekämpfung der Computerkriminalität hat die Schweiz die Europaratskonvention über die Cyberkriminalität ratifiziert, welche per 1. Januar 2012 in Kraft getreten ist, mit den entsprechenden Gesetzesanpassungen auf nationaler Ebene. Dementsprechend ist gemäss Art. 143bis Abs. 2 StGB auch schon als Täter strafbar, wer Passwörter, Programme oder andere Daten in Verkehr bringt, wenn er annehmen muss, dass diese als Grundlage für Hacking dienen könnten.

Das Eindringen in ein fremdes Computersystem kann ebenfalls durch heimliches Umleiten von fremden E-Mails auf eine E-Mail-Adresse des Täters geschehen. Das Bundesgericht hat dazu klar Stellung bezogen und die Strafbestimmung auch für diese Form als anwendbar erklärt (BGE 130 III 32 E. 4.2).

Ein wichtiger Bestandteil bei der Strafverfolgung von Datendieben im Umfeld von Industriediebstählen ist Art. 162 StGB, Tatbestand der Verletzung des Fabrikations- oder Geschäftsgeheimnisses. Danach wird unter anderem bestraft, wer ein Firmengeheimnis verrät, welches er aufgrund seiner arbeitsvertraglichen Pflichten erfahren hat. Häufig sind Fälle, bei denen ein ehemaliger Mitarbeiter beim Verlassen seiner Arbeitsstelle Dokumente und Pläne auf Datenspeichern mit sich nimmt, um diese später in (eigenen) Konkurrenzunternehmen zu verwenden. Meist betroffen ist das technische Know-how einer Firma, mit erheblichem Schädigungspotenzial, insbesondere wenn zur ▶

Bei der Computerkriminalität hat die Schweiz die Europaratskonvention über die Cyberkriminalität ratifiziert.



Die Daten müssen geschützt werden, sonst verlangt der Gesetzgeber eine Verurteilung.

Erarbeitung des Know-how jahrelange Entwicklungen notwendig waren. Selbstverständlich kann diese Bestimmung in Konkurrenz zu anderen Tatbeständen treten, wenn nämlich entsprechende Geheimnisse via externe Computersysteme gestohlen werden.

Im Bankenumfeld können bei einem Datendiebstahl diverse Strafbestimmungen tangiert sein. Falls ein Geheimnisträger selbst Daten entwendet, dann kann die Anwendung der klassischen Computerdelikte fraglich sein. Das Bankengesetz sanktioniert in Art. 47 BankG die Weitergabe von Bankdaten durch den Geheimnisträger selbst. Entscheidend ist nun, dass gemäss neuem Art. 47 Abs. 1 lit. c BankG auch Datenhehlerei bestraft wird; der Übermittler von Daten wird bestraft, der wissen muss, dass die Daten aus einem Bankdatendiebstahl kommen. Besonders an Widerhandlungen gegen das Bankengesetz ist, dass solche auch durch fahrlässiges Handeln begangen werden können.

Beim Datendiebstahl haben die Strafverfolgungsbehörden auch wirtschaftlichen Nachrichtendienst gemäss Art. 273 StGB zu prüfen. Wie im Fall von Art. 162 StGB wird bestraft, wer auf Datenträgern gespeicherte Fabrikations- oder Geschäftsgeheimnisse auskundschaftet. Im Unterschied zu dieser Regelung handelt hier ein Täter mit dem Ziel, Daten einer fremden amtlichen Stelle oder einer privaten Unternehmung zugänglich zu machen.

In der Schweiz werden unzulässige Eingriffe gegen den freien Wettbewerb ebenfalls durch das Bundesgesetz gegen den unlauteren Wettbewerb (UWG) reguliert. Art. 6 in Verbindung mit Art. 23 UWG bestraft den Dieb von Geschäftsgeheimnissen, jedoch nur auf Antrag einer Geheimnisträgerin.

Die aktuellen Entwicklungen zeigen, dass Gesetzgeber sowohl auf nationaler als auch internationaler Ebene die koordinierte Bekämpfung von Computerkriminalität vereinfachen wollen. Materiellrechtliche Bestimmungen sind jedoch nur so stark, wie die prozessuale Umsetzung dies zulässt und auch ein entsprechender politischer Wille dazu besteht.

Strafbarkeit von Unternehmen

Für die Strafverfolgungsbehörden stellt sich unweigerlich die Frage, ob die geschäftsführenden Organe ihre Unternehmung 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?

Falls solche Fragen nicht befriedigend beantwortet werden, kann einem geschäftsführenden Organ vorgeworfen werden, dass die Verantwortung nicht wahrgenommen und dadurch ein Computerdelikt ermöglicht wurde. Dies mit ernst zu nehmenden Konsequenzen. In zivilrechtlicher Hinsicht kann dies zu Schadenersatzansprüchen gegen einen CEO führen. Strafrechtlich können unter dem Titel der ungetreuen Geschäftsbesorgung (Art. 158 StGB) empfindliche Strafen in Aussicht stehen.

Demgegenüber sind Konstellationen, bei denen sich eine Unternehmung in Anwendung des Unternehmensstrafrechts im Sinne von Art. 102 StGB selbst strafbar macht, kaum vorstellbar. Dazu müssten diverse im Gesetz fixierte Schranken in erheblicher Weise durchbrochen worden sein, welche kausal zum Datenleck beziehungsweise -diebstahl geführt hätten. Auch die Praxis zeigt, dass Unternehmen für potenzielle Vergehen strafrechtlich nur zurückhaltend in die Pflicht genommen werden.

Betriebliches Risiko «Strafuntersuchung»

Datendiebstähle werden für Unternehmen auch in Zukunft eine erhebliche Gefahr darstellen. Aus Kosten- und Effizienzgründen wird vermehrt papierlos gearbeitet, wobei sämtlicher interner und externer Geschäftsverkehr auf Servern dokumentiert ist.

Für ein Unternehmen gilt es im Bereich von Datendiebstählen stets die aktuellen Entwicklungen zu überwachen und sich auf künftige Risiken vorzubereiten. Insbesondere ist aus Sicht einer Unternehmung das Risiko einer eskalierenden Strafuntersuchung zu minimieren. Sicherlich bestehen in solchen Fällen Wege, mit Behörden zusammenzuarbeiten. Nicht vergessen werden darf dabei nebst Reputationsrisiken die erhebliche administrative Belastung für eine Unternehmung, verursacht durch Zeugeneinvernahmen, Herausgebersuchen und andere Massnahmen von Behörden. ■

Dr. iur. Cornel Borbély

ist Rechtsanwalt in Zürich. 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.

www.ffhs.ch