Dr. Heiko A. Haller, RA, und Dr. Holger Lutz, RA

Datendiebstahl als neues Prozessrisiko

Wir leben in einer Welt immer größerer Transparenz. Allerdings wird nicht nur die Welt um uns herum transparenter, sondern auch wir werden für andere transparent. Der Beitrag widmet sich dem zunehmend auftretenden Datendiebstahl aus einer zivilrechtlichen Haftungsperspektive. Hierauf bezogen meint Transparenz, dass „Diebe" immer leichter sensible Informationen über uns erlangen können. Der Beitrag analysiert die zivilrechtliche Risikolage für Unternehmen, insbesondere im Hinblick auf mögliche Schadensersatzansprüche, und zeigt Möglichkeiten der Risikominimierung auf.

I. Einleitung

In jedem Wirtschaftszweig verarbeiten Unternehmen große Mengen an Daten von und über ihre Geschäftspartner und Kunden. Bei einem Großteil dieser Informationen handelt es sich um Daten, die vertraglich und/oder gesetzlich einem besonderen Schutz unterliegen. In Betracht kommt vor allem ein (vertraglicher) Schutz der Daten als vertrauliche Informationen oder ein gesetzlicher Schutz derselben als Geschäfts- oder Betriebsgeheimnisse der Geschäftspartner oder Kunden (vgl. § 17 UWG). In vielen Fällen umfassen die Informationen auch personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG oder nach anderen datenschutzrechtlichen Vorschriften geschützte Daten (z. B. TKG, TMG).[1]

In den geschützten Daten liegt ein wertvolles Wirtschaftsgut für das jeweilige Unternehmen. Dennoch berichtet die Presse immer häufiger darüber, dass Unternehmen solche Daten (z. B. Kreditkartendaten, Passwörter und vergleichbar sensible Daten) abhandenkommen.[2]

Der Umgang mit geschützten Daten birgt unweigerlich das Risiko, dass es zu Sicherheitslücken kommt und geschützte Daten gezielt von Dritten ausgespäht werden. Statistisch gesehen gehen meist Laptops verloren oder Hacker verschaffen sich unbefugt Zugang zum Computersystem des Unternehmens. In anderen Fällen gehen Datenträger auf dem Transport verloren oder werden unvorsichtig entsorgt (ohne endgültige Löschung der Daten). In einem sehr bekannten Fall aus den USA wurden in einem Lebensmitteldiscounter Kreditkartendaten der Kunden per WLAN unverschlüsselt von den Kassen in die Buchhaltung übertragen. Kriminelle lasen die Daten mit (in einem Auto auf dem Kundenparkplatz) und sammelten im Weihnachtsgeschäft auf dieser Weise 45 Mio. (!) Kreditkartendatensätze.

In Deutschland wird das Risiko eines Datendiebstahls meist aus datenschutzrechtlicher Sicht betrachtet.[3] In der Tat existieren in Deutschland – wie auch in den anderen EU-Mitgliedstaaten – strenge Datenschutzvorschriften. Dies korreliert mit der hohen Sensibilität der (deutschen) Öffentlichkeit für den Datenschutz. Die Gefahr einer zivilrechtlichen Haftung vernachlässigen Unternehmen aber häufig, da ein substanzieller ersatzfähiger Schaden für unrealistisch gehalten wird. Dabei liegt das eigentliche (Haftungs-)Risiko für den Fall, dass geschützte Daten abhandenkommen, gerade hier: Eintrittswahrscheinlichkeit eines Schadens und Schadenshöhe sind in vielen Fällen hoch und stellen so ein kumuliertes erhebliches Risiko dar. Hinzu kommt, dass solche Schadensereignisse meist ein großes Medienecho finden.

Das Beispiel des Lebensmitteldiscounters macht das (zivilrechtliche) Haftungsrisiko deutlich: Zwar wird den meisten der 45 Mio. betroffenen Kunden kein (erheblicher) Schaden entstanden sein, weil sie ihre Kreditkarte rechtzeitig sperren ließen oder nicht für einen Missbrauch hafteten. Anders sieht es aber mit Blick auf die kartenausgebenden Kreditinstitute aus. Diese haben die Gefahr gesehen, dass die Daten ihrer Kunden missbraucht werden (und sie ihre Kunden nicht für entsprechende Abbuchungen verantwortlich machen können), und daher die Kreditkarten ihrer Kunden ausgetauscht. Während die Kosten für das Ausstellen einer einzelnen Kreditkarte überschaubar bleiben, summieren sich diese Mikroschäden bei einer Vielzahl betroffener Kunden rasch auf mehrstellige Millionenbeträge: Auch wenn pro neuer Kreditkarte „nur" ein Schaden von US$ 25 entsteht; auf 45 Mio. betroffene Kunden hochgerechnet, handelte es sich um eine erschreckend hohe mögliche Schadensersatzforderung von US$ 1,1 Mrd.

Dabei dürften die tatsächlichen Kosten regelmäßig sogar einiges höher liegen, weil ein Datendiebstahl einen hohen Beratungsbedarf bei den betroffenen Kunden auslöst. Als der Karstadt-Quelle-Bank 2009 Kundendaten abhandenkamen, erhöhten sich die Anrufe im Call Center von zuvor durchschnittlich 2000–2500 pro Tag auf 100 000 pro Tag um den Faktor 40! Hinzu kamen weitere Schadensersatzpositionen, weil die Bank ihre Kunden benachrichtigen musste und ihnen ein sogenanntes Credit Monitoring anbieten oder ähnliche Schadensbegrenzungsmaßnahmen/vorbeugende Maßnahmen ergreifen musste. Zu diesen rein monetären Ansprüchen tritt der Reputationsverlust des Unternehmens, Kosten für Mitteilungen an die betroffenen Kunden, eventuell Kulanzleistungen etc. Aber auch von staatlichen Stellen können je nach Fall Sanktionen drohen (Untersuchungen, Bußgelder, Abhilfeverlangen und im schlimmsten Fall sogar strafrechtliche Sanktionen).

Mögliche Geschädigte und damit potentielle Anspruchssteller gibt es viele: Andere Unternehmen kommen ebenso in Betracht wie Kunden und staatliche Stellen. Da eine Klage gegen die eigentlichen Datendiebe nicht erfolgversprechend ist, weil diese entweder nicht zu fassen oder mittellos sind, bleibt als Haftungsgegner nur das vom Datendiebstahl betroffene Unternehmen. Hat es den Datendiebstahl durch eigene Fahrlässigkeit ermöglicht, droht eine Haftung für alle entstehenden Schäden. Das „Opfer" des Datendiebstahls wird so wegen der

1 Diese Daten werden im Folgenden insgesamt als „geschützte Daten" bezeichnet.

2 Zum Beispiel: „Gmail statt GS: Goldman Sachs schickt vertrauliche Daten an falsche Mail-Adresse", Manager Magazine online, 3.7.2014, abrufbar unter www.manager-magazin.de/lifestyle/artikel/a-978913.html (Abruf: 3.7.2014); „Cyberkriminalität: Fahnder entdecken 18 Millionen gestohlene E-Mail-Passwörter", Spiegel Online, 3.4.2014, abrufbar unter www.spiegel.de/netzwelt/netzpolitik/e-mail-passwoerter-gestohlen-18-millionen-daten saetze-a-962419.html (Abruf: 3.7.2014).

3 Z. B. *Hornung*, NJW 2010, 1841 (Informationen über „Datenpannen" – Neue Pflichten für datenverarbeitende Unternehmen).

Ermöglichung der Tat schnell zum „Täter" und sieht sich hohen Ansprüchen ausgesetzt.

Der vorliegende Beitrag analysiert zunächst die Risikolage wie sie sich unter deutschem Recht insbesondere hinsichtlich möglicher Schadensersatzansprüche darstellt. Wir kommen zu dem Ergebnis, dass ein Unternehmen, dem geschützte Daten abhandenkommen, Ersatzansprüchen ausgesetzt ist. Zwar ist es nicht einfach, die entstehenden Schäden dem Unternehmen zuzurechnen. Doch führen bereits die eindeutig erstattungsfähigen Schadenspositionen zu einem erheblichen Risiko für das betroffene Unternehmen. Zu diesen Schäden kommen Reputationsschäden und freiwillige Leistungen, die das betroffene Unternehmen erbringt, um Vertrauen von Geschäftspartnern und Kunden wiederzugewinnen. Schließlich zeigt dieser Beitrag auch auf, wie Unternehmen ihre entsprechenden Risiken minimieren können.

II. Das unterschätzte Risiko: Schadensersatzhaftung für abhanden gekommene Daten

Obwohl in Deutschland der Datenschutz als sensibles Thema gilt, beschäftigt sich die juristische Literatur erstaunlich wenig mit den zivilrechtlichen (Haftungs-)Folgen eines Verstoßes.

Dies ist umso verwunderlicher als es immer wieder zum Verlust geschützter Daten kommt. Die Gründe für den Datenverlust sind sehr unterschiedlicher Natur. Statistisch am häufigsten handelt es sich um gestohlene Laptops oder um Angriffe durch einen Hacker, der sich unbefugt Zugang zum Computersystem und damit zu den geschützten Daten verschafft. Aber es kommt auch vor, dass Datenträger beim Versand verloren gehen oder dass Datenträger entsorgt werden, ohne dass die Daten zuvor endgültig gelöscht wurden. In allen Fällen geht es um den Verlust nicht nur eigener Daten wie z. B. eigener Geschäfts- oder Betriebsgeheimnisse, sondern auch um den Verlust von geschützten Daten der Geschäftspartner und Kunden des betroffenen Unternehmens.

Ein unwahrscheinliches Szenario? In Deutschland kam es (soweit ersichtlich) noch nicht zu einem erheblichen Schadensersatzprozess aufgrund eines Datendiebstahls. Der Blick in die USA lässt indes Schlimmes erahnen. Beispiele für abhanden gekommene Daten gibt es zuhauf und mit steigender Tendenz. Genannt seien lediglich die kürzlich aufgetretenen Fälle bei einem internationalen Spielenetzwerk und einem der größten Softwareunternehmen aber auch der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erst kürzlich aufgedeckte Diebstahl von 18 Mio. Passwörtern zu E-Mail-Konten.[4] Stets stand das betroffene Unternehmen zu Recht oder zu Unrecht am öffentlichen Pranger. Die Medien berichteten in aller Ausführlichkeit über die Fälle. Der Imageschaden war erheblich. Zu diesen nur schwer zu beziffernden Schäden traten weitere: Die Kunden mussten über den Datenverlust informiert werden und Rückfragen der Kunden mussten beantwortet werden. Während sich der Schaden pro Kunde auf wenige Euro belief, addierten sich die Gesamtschäden angesichts der hohen Zahl betroffener Kunden auf beträchtliche Summen. Hinzu kam das Risiko öffentlich-rechtlicher Folgen (Untersuchungen, Bußgelder, Abhilfeverlangen oder strafrechtliche Sanktionen).

Kunden können ihre Ansprüche auf vertragliche Grundlagen stützen: Ihr Vertragspartner – etwa der Supermarkt, in dem die Kreditkarte zum Einsatz kam – hat die vertragliche Nebenpflicht, mit den ihm anvertrauten Daten sorgfältig umzugehen (vgl. § 241 Abs. 2 BGB). Bedient er sich eines Dienstleisters für die Datenverarbeitung, haftet der Supermarkt auch für dessen Pflichtverletzungen (vgl. § 278 BGB). Kommt es zum Datendiebstahl, kann der Kunde geltend machen, dass sein Vertragspartner die vertraglichen Sorgfaltspflichten verletzt hat, und alle ihm entstehenden (Folge-)Schäden ersetzt verlangen. Schäden entstehend jedoch häufig nicht nur bei den Kunden. Aufgrund der hohen Sensibilität der Kunden bei Datenverlusten und des Risikos, dass einzelne Abbuchungen dem Kunden nicht mehr zugerechnet werden können, tauschen die meisten Banken Kreditkarten freiwillig aus und tragen gegenüber dem Kunden die hiermit verbundenen Kosten. Wie das Beispiel des Lebensmitteldiscounters zeigt, sind Kundenklagen aber nicht auszuschließen, wobei diese mangels „Sammelklagen" in Deutschland weniger gefährlich sind als in den USA.

Wirtschaftlich relevanter sind Ansprüche der Banken gegen ihre Vertragspartner, die Bezahlvorgänge mit Hilfe von Kreditkarten abwickeln und denen Kreditkartendaten entwendet worden sind. Auch in diesem Rechtsverhältnis hat der Vertragspartner Sorgfaltspflichten zu beachten und muss mit den anvertrauten Daten so umgehen, dass unberechtigte Dritte keine Kenntnis davon erhalten. An dieser Stelle stellt sich die (rechtliche) Frage nach dem Sorgfaltsmaßstab: Wie muss ein Unternehmen die ihm anvertrauten Daten schützen, damit ihm keine Fahrlässigkeit vorgeworfen werden kann? Unternehmen können sich insoweit an Industriestandards orientieren. Es ist zum Beispiel üblich, Kreditkartendaten nur verschlüsselt zu übertragen und hierfür eine anerkannte Verschlüsselungsmethode zu verwenden. Dies hatte der Lebensmitteldiscounter im Beispielsfall nicht beachtet und Kreditkartendaten unverschlüsselt in einem offenen WLAN übertragen, das so zum einfachen Ziel für den Hacker-Angriff wurde. Industriestandards sind zwar kein verbindlicher Maßstab, sie helfen in der Praxis aber, das Pflichtenprogramm von Unternehmen zu konkretisieren.

Schwierig ist die Schadensberechnung, also die Frage, für welche Kosten das Unternehmen aufkommen muss, das den Datendiebstahl durch eigene Fahrlässigkeit ermöglicht hat. Die Schadenspositionen sind vielfältig. Beim Diebstahl von Kreditkartendaten steht der Austausch der Kreditkarte, deren Daten ausgespäht wurden, im Vordergrund. In den USA wurden die Austauschkosten in einigen Fällen mit ungefähr US$ 25 pro Kreditkarte pauschaliert. Die tatsächlichen Kosten dürften einiges höher liegen, weil der Datendiebstahl einen hohen Beratungsbedarf bei den betroffenen Kunden auslöst. Nicht zuletzt ersetzen Banken ihren Kunden zumindest einen Großteil eines durch Missbrauch der Kartendaten eingetretenen Schadens. Angesichts dieser unterschiedlichen Schadenspositionen muss abgegrenzt werden, welche dieser Kosten sich das den Datendiebstahl fahrlässig ermöglichende Unternehmen zurechnen lassen muss. Nicht jeder vermeintliche Datendiebstahl führt schließlich dazu, dass Kreditkarten zwingend ausgetauscht werden müssen. Oft handelt es sich dabei um eine Vorsorgemaßnahme oder Kulanzleistung der Bank, die einen Vertrauensverlust bei ihren Kunden oder einen eigenen Imageverlust vermeiden möchte. Hinzu kommt, dass die Banken durch den Austausch

4 „Sony-Chef Stringer entschuldigt sich", Handelsblatt, 6.5.2011, abrufbar unter www.handelsblatt.com/unternehmen/it-medien/datenpanne-sony-chef-stringer-entschuldigt-sich/4142032.html (Abruf: 3.7.2014); „Cyberkriminalität: Fahnder entdecken 18 Millionen gestohlene E-Mail-Passwörter", Spiegel Online, 3.4.2014, abrufbar unter www.spiegel.de/netzwelt/netzpolitik/e-mail-passwoerter-gestohlen-18-millionen-datensaetze-a-962419.html (Abruf: 3.7.2014).

eigene Kosten sparen, weil so der turnusmäßige Austausch der Karten aufgrund Verschleißes entfällt.

Unternehmen, die eine große Menge an geschützten Daten verarbeiten, müssen angesichts der hohen Schadensrisiken aus einem Datendiebstahl ein effektives Risikomanagement installieren und so ihre Haftungsrisiken reduzieren, *bevor* es zu einem Datendiebstahl mit möglichen Haftungsansprüchen kommt. Sie müssen analysieren, welche Informationen wie verarbeitet werden und dann gegebenenfalls ihren Sicherheitsstandard anpassen. So können Unternehmen ihre Prozessrisiken z. B. dadurch reduzieren, dass sie entsprechende Sicherungseinrichtungen vorhalten und dokumentieren. Zudem können Unternehmen Risiken verlagern, etwa auf Versicherungen oder auf externe Dienstleister. Für den Schadensfall können Unternehmen bereits im Vorfeld „Notfallpläne" aufstellen und darin festlegen, wie sie auf Datenverluste reagieren werden. Solche Notfallpläne sollten immer auch Überlegungen zur raschen Information der Vertragspartner und zur Kooperation mit öffentlichen Stellen enthalten. Auf Rechtsfolgenseite ist es wichtig, schon im Vorfeld zu wissen, welche Schäden drohen.

All dies setzt voraus, dass Unternehmen präventiv tätig werden und nicht erst, wenn ein Datenverlust festgestellt wird. Wer eine rasche („raus aus den Schlagzeilen") und günstige Konfliktlösung möchte, muss Konflikte antizipieren. Auf diese Weise kann er Konflikte entweder ganz vermeiden oder wenigstens den Ablauf des Konflikts in seinem Sinne strukturieren und die Auswirkungen abfedern. Weil die wirtschaftliche Bedeutung sowie die tatsächliche wie rechtliche Komplexität der Fälle hoch sind, kann ein Unternehmen jedenfalls nicht nur zuwarten. Vielmehr gilt es, aus den praktischen Fällen in den USA zu lernen und die Konsequenzen für das eigene Unternehmen rechtzeitig zu ziehen. Die drastischen Konsequenzen trafen die Unternehmen in den USA vor allem, weil sie unvorbereitet waren – in tatsächlicher aber gerade auch in rechtlicher Hinsicht.

III. Vertragliche Haftungsrisiken

Haftungsrisiken ergeben sich für das betroffene Unternehmen zunächst aus einer möglichen vertraglichen Haftung wegen der Verletzung vertraglicher Pflichten. Während sich eine Pflichtverletzung recht leicht begründen lässt, ist dies hinsichtlich der erstattungsfähigen Schäden schwieriger.

1. Typische Ausgangskonstellation

In jedem Fall eines Datendiebstahls gibt es neben dem Datendieb mindestens zwei weitere Beteiligte: den „Eigentümer" der Daten (z. B. der Kunde oder Geschäftspartner eines Unternehmens) sowie den Empfänger der Daten (z. B. das Unternehmen, das an den Kunden Güter oder Leistungen veräußert). Der „Eigentümer" überlässt dem Empfänger entweder gezielt seine Daten als Teil der Hauptleistungspflicht, z. B. bei der Verwahrung einer DVD mit geschützten Daten, oder die Daten werden lediglich benötigt, um damit nicht zusammenhängende Vertragspflichten abzuwickeln, z. B. Kontoverbindungsdaten oder Kreditkartendaten beim Kauf von Möbeln. In diesem Fall sind die Daten nicht selbst Vertragsgegenstand.

Häufig sind zudem Banken als weitere Beteiligte eingebunden (sowohl auf Seiten des Kunden als auch auf Seiten des Unternehmens). Die Banken stehen zwischen Kunden und Unternehmen und wickeln den Zahlungsvorgang ab. So stellt z. B. die kartenausstellende Bank dem Kunden eine Kreditkarte zur Verfügung und verspricht gegenüber der Akzeptanzstelle (z. B. dem Supermarkt), die fälligen Beträge auszugleichen.[5] Es liegt also ein Mehrpersonenverhältnis vor.

Der Datendieb greift in dieses Mehrpersonenverhältnis ein. Maßgeblich ist dabei zunächst, welche Vertragsbeziehung der Datendiebstahl berührt. So macht es einen Unterschied, ob die Daten „gestohlen" werden, weil das Unternehmen damit unsorgfältig umgeht oder ob im Interbankenverkehr Daten abhandenkommen. Entsprechend können im Falle eines Datendiebstahls Schäden bei allen betroffenen Personen entstehen. So kann es zu Schäden unmittelbar beim Kunden kommen, wenn seine Kontodaten entwendet werden und der „Dieb" diese missbraucht. Zudem hat der Kunde ggf. zusätzlichen Aufwand, um eine neue Kreditkarte zu besorgen. In aller Regel wird sich hier indes die Bank in der Pflicht sehen, sodass diese Schäden im Ergebnis nicht vom Kunden getragen werden müssen. Die Schäden verlagern sich damit faktisch auf die Banken, die Karten austauschen und ein aufwendiges Credit Monitoring betreiben müssen. Die Banken werden dann allerdings versuchen, die bei ihnen entstandenen „Schäden" auf das betroffene Unternehmen zu verlagern. Der Datendieb selbst wird in der Regel nicht als Anspruchsgegner in Betracht kommen, da er nicht über die erforderliche Liquidität verfügen wird oder nicht zu fassen ist.

Gefährlich und für Unternehmen von besonderem Interesse sind vor allem diejenigen Fälle, in denen sich das Risiko an einer Stelle kumuliert, d. h. wo Personen in eine (Massen-)Transaktion eingeschaltet sind, z. B. mehrere betroffene Kunden eines Supermarkts. Da in Deutschland keine Sammelklagen zulässig sind, ist die Situation weniger gefährlich als in den USA. Gehen einem Unternehmen Kundendaten verloren, ist bei den betreffenden Kunden der eigentliche Schaden eher gering. In der Regel werden die meisten Kunden eventuell bestehende Ansprüche nicht durchsetzen. Allerdings kumulieren sich Schäden der Kunden bei Banken oder anderen Unternehmen zu ganz erheblichen Forderungen.

2. Pflichtverletzung

Ansprüche auf Schadensersatz des Kunden oder der zwischengeschalteten Bank können sich zunächst aus dem Gesichtspunkt der Vertragsverletzung ergeben (§ 280 Abs. 1 BGB). Wer Kundendaten hält und verarbeitet muss dafür Sorge tragen, dass unberechtigte Dritte darauf nicht zugreifen können. Die Vertragsparteien haben auf die Interessen der jeweiligen anderen Seite Rücksicht zu nehmen und alles zu unterlassen, was die Rechtsgüter und Interessen des Vertragspartners schädigt.[6] Zudem sind Ansprüche aus unerlaubter Handlung möglich, weil meist zugleich Schutzgesetze verletzt sein werden. Sofern es sich bei den geschützten Daten um personenbezogene Daten handelt, kommt auch die spezialgesetzliche Anspruchsgrundlage in § 7 BDSG in Betracht.

Die Bank hat als kartenausgebende Stelle mit dem Unternehmen zwar keinen direkten Vertrag geschlossen. Allerdings können hier – abhängig vom Einzelfall – die Grundsätze des Vertrages mit Schutzwirkung zu Gunsten Dritter[7] oder der Drittschadensliquidation[8] zur Anwendung kommen. Auch im Verhältnis zwischen Kunden/Geschäftspartner des Unternehmens sowie dem Unternehmen sind daher Sorgfalts-

5 Vgl. zu den Rechtsbeziehungen im Kreditkartengeschäft z. B. *Junker*, DStR 1994, 1461.
6 Vgl. § 241 Abs. 2 BGB sowie *Bachmann/Roth*, in: Münchener Kommentar zum BGB, 6. Aufl. 2012, § 241 Rn. 46 ff.
7 Vgl. hierzu nur *Grüneberg*, in: Palandt, BGB, 73. Aufl. 2014, § 328, Rn. 13.
8 Vgl. hierzu nur *Grüneberg*, in: Palandt, BGB, 73. Aufl. 2014, Vorb v § 294, Rn. 105 ff.

pflichten zu beachten, um eine Haftung nach diesen Grundsätzen zu vermeiden.

Wie bei jeder Technologie kann es auch beim Einsatz von Informationstechnologie keine absolute Sicherheit geben. Jedenfalls lässt sich kein Informationstechnologiesystem nach außen so abschotten, dass es gleichzeitig praxistauglich wäre und absolute Sicherheit in Bezug auf Datendiebstähle gewährleistete. Es kann jedoch erwartet werden, dass beim Einsatz von Informationstechnologie die im Verkehr übliche/erforderliche Sorgfalt angewandt wird. Dies bedeutet, dass ein Unternehmen diejenigen Schutzeinrichtungen einführen und umsetzen muss, die im jeweiligen Wirtschaftszweig üblich sind und vernünftiger Weise erwarten werden dürfen. Die Sicherheitsstandards variieren dabei je nach Art der betroffenen Daten. So ist z. B. mit sensiblen Daten sorgfältiger umzugehen als mit weniger sensiblen Daten wie z. B. dem reinen Kaufdatum eines Möbelstücks.

Zur Konkretisierung des Pflichtenprogramms können Industriestandards herangezogen werden, z. B. die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationsgesellschaft oder – speziell für Kreditkartenzahlungen – der „Payment Card Industry Data Security Standard" (PCI DSS) der führenden Kreditkartenorganisationen.

3. Schaden

In der Regel entsteht durch das bloße Abhandenkommen von Daten unmittelbar kein nachweisbarer Schaden. Kundendaten haben zwar einen eigenständigen Wert und werden zu signifikanten Preisen gehandelt. Einen Schaden hat aber insoweit allenfalls das betroffene Unternehmen, dem dieser Gewinn – möglicherweise – entgeht.

Zu einem Schaden kommt es aber z. B. dann, wenn die Daten von einem Unberechtigten verwendet werden, der vorspiegelt, berechtigt zu sein. (Beispiel: unberechtigte Abbuchung von einem fremden Konto.)

Im Übrigen entstehen „Schäden", weil „freiwillig" Maßnahmen ergriffen werden, die dazu dienen, Schäden abzuwenden. So dient z. B. der Austausch von Kreditkarten dazu, einen Missbrauch zu verhindern. Solche Aufwendungen sind ebenfalls grundsätzlich ersatzfähig. Es gilt allerdings, die Grenze zu bestimmen, welche Vorsorgemaßnahmen (noch) ersatzfähige „Schäden" darstellen, die durch das Abhandenkommen der Daten verursacht wurden und welche Aufwendungen nicht mehr zuzurechnen sind, weil es sich um freiwillige Kulanzleistungen handelt oder weil es nicht um bereits entstandene Schäden geht, sondern nur um potenzielle künftige Schäden.

Im deutschen Recht ist der Geschädigte nach § 249 BGB grundsätzlich so zu stellen, wie er stünde, wenn das schadensverursachende Verhalten (d. h. das Abhandenkommen der Daten) nicht eingetreten wäre – also so, als ob die Daten nicht abhandengekommen wären. Da ohne das Abhandenkommen der Daten die Aufwendungen nicht entstanden wären, scheint ein erstattungsfähiger „Schaden" grundsätzlich vorzuliegen. Der Umfang des geschuldeten Schadensersatzes ist aber nicht grenzenlos. Freiwillige Leistungen gehen nicht mehr zwingend auf ein Fehlverhalten zurück, sondern beruhen auf einer eigenständigen Entscheidung des Dritten, die den Zurechnungszusammenhang unterbrechen können. Zudem verstößt der Geschädigte mit übertriebenen freiwilligen Maßnahmen gegen seine Schadensminderungsobliegenheit des § 254 Abs. 2 BGB. Der Geschädigte muss sich Vorteile anrechnen lassen, die er durch den Schadensausgleich erhält. Erstattungsfähig sind damit nur Aufwendungen für Maßnahmen, die eine unmittelbare Gefährdung beseitigen (Kartenaustausch, Hotline, Credit Monitoring etc.). Dies folgt aus dem Gedanken, dass nur solche Maßnahmen effektiv die Schadensentstehung verhindern und in ganz überwiegendem wenn nicht ausschließlichem Interesse des betroffenen Unternehmens erfolgen. Der Dritte kommt damit seiner Schadensminderungsobliegenheit nach.

Die Rechtsprechung hat verschiedene Fallgruppen herausgebildet, in denen sie einen Zurechnungszusammenhang verneint. So kann der Zurechnungszusammenhang entfallen, wenn der Eintritt des Schadens auf einem Willensentschluss des Geschädigten beruht. Allerdings besteht auch in einem solchen Fall eine Ersatzpflicht, wenn der Schaden nach Art und Entstehung nicht außerhalb der Wahrscheinlichkeit liegt und unter dem Schutzzweck der Norm fällt.[9] So unterbrechen Willensentschlüsse des Verletzten den Zurechnungszusammenhang dann nicht, wenn sie nicht frei getroffen, sondern durch das Verhalten des Schädigers herausgefordert oder doch wesentlich mitbestimmt wurden.[10]

4. Vertragliche Notifizierungspflichten gegenüber den Kunden

Jenseits der Schadensersatzverpflichtung stellt sich die Frage, ob das betroffene Unternehmen verpflichtet ist, seine Kunden darüber zu informieren, dass geschützte Daten abhandengekommen sind. Auch dem Kunden obliegt gegenüber seiner Bank die Pflicht der unverzüglichen Mitteilung, wenn entsprechende Kontodaten abhandengekommen sind. Die Verträge zwischen Unternehmen und Endkunden enthalten grundsätzlich keine ausdrücklichen Informationspflichten. Eine Vertragsbeziehung als Sonderrechtsverhältnis kennzeichnet sich jedoch dadurch, dass die Vertragspartner auf ihre jeweiligen Interessen wechselseitig Rücksicht zu nehmen haben. Sie müssen dafür Sorge tragen, die Rechtsgüter der jeweils anderen Partei nicht zu schädigen. Verursacht eine Vertragspartei eine Gefährdung von Rechtsgütern der anderen, muss sie diese auf die Gefährdungslage hinweisen. Nur so kann gewährleistet werden, dass sich die Gefährdung nicht realisiert und effektive Abhilfemaßnahmen geschaffen werden können. Um die Gefährdung zu beseitigen, bedarf es zwingend der Mithilfe des Kunden, sodass dieser unverzüglich zu informieren ist. Grundsätzlich hat die Information an den Kunden/Geschäftspartner direkt zu erfolgen. Man wird indes davon ausgehen können, dass bei einem besonders großen Schadensfall und einer unbestimmten Anzahl von Kunden auch eine allgemeine Notifizierung ausreichend ist (vor allem z. B. dann, wenn Kontaktdaten der Kunden nicht vorliegen).

IV. Regulatorischer Rahmen

Soweit es sich bei den abhanden gekommenen Daten um personenbezogene Daten handelt, enthält das deutsche Recht verschiedene datenschutzrechtliche Notifizierungspflichten. Die relevanteste Vorschrift findet sich in § 42a BDSG, die grundsätzlich für sämtliche personenbezogenen Daten Anwendung findet. Spezialgesetzliche Notifizierungspflichten gibt es darüber hinaus in § 15a TMG (für Bestands- oder Nutzungsdaten im Zusammenhang mit Telemediendiensten) sowie § 109a TKG für personenbezogene Daten im Zusammenhang mit der Erbringung öffentlich zugänglicher Telekommunikationsdienste.

Die Notifizierungspflicht des § 42a BDSG greift immer dann, wenn (i) besondere Arten personenbezogener Daten, (ii) personenbezogene

9 Vgl. hierzu nur *Grüneberg*, in: Palandt, BGB, 73. Aufl. 2014, Vorb v § 294, Rn. 44.
10 Vgl. hierzu nur *Grüneberg*, in: Palandt, BGB, 73. Aufl. 2014, Vorb v § 294, Rn. 41.

Daten, die einem Berufsgeheimnis unterliegen, (iii) personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder (iv) personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Droht in diesem Fall eine „schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen", ist die aus datenschutzrechtlicher Sicht „verantwortliche Stelle" zur unverzüglichen Benachrichtigung der Aufsichtsbehörde sowie der Betroffenen verpflichtet.

1. Unverzügliche Benachrichtigung der Aufsichtsbehörde

Die Benachrichtigung der zuständigen Aufsichtsbehörde muss „unverzüglich" erfolgen. Bei dem Begriff „unverzüglich" handelt es sich um einen unbestimmten Rechtsbegriff, der in § 121 BGB nur wenig genauer als „ohne schuldhaftes Zögern" definiert wird. Die deutschen Datenschutzaufsichtsbehörden gehen jedoch davon aus, dass ein schuldhaftes Zögern nur dann nicht vorliegt, wenn ein Zeitraum von 24 bis 48 Stunden nicht überschritten wird.

Die „unverzügliche" Benachrichtigung der Aufsichtsbehörde muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Darüber hinaus muss die Benachrichtigung eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der verantwortlichen Stelle daraufhin ergriffenen Maßnahmen enthalten.

Spätestens an dieser Stelle wird klar: Will ein von einem Datendiebstahl betroffenes Unternehmen der Notifizierungspflicht nach § 42a BDSG genügen, bedarf eine inhaltlich ordnungsgemäße Benachrichtigung der Aufsichtsbehörde innerhalb eines Zeitraums von 24 bis 48 Stunden einer guten Vorbereitung. Eine Beschäftigung mit den gesetzlichen Anforderungen erst nach Kenntnisnahme von einem Datendiebstahl führt in aller Regel dazu, dass eine „unverzügliche" Benachrichtigung nicht möglich ist.

2. Unverzügliche Benachrichtigung der Betroffenen

Die Benachrichtigung des Betroffenen muss ebenfalls „unverzüglich" erfolgen. Allerdings ist der Anknüpfungspunkt für die „Unverzüglichkeit" ein anderer. Die Benachrichtigung muss nämlich erst dann erfolgen, wenn angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird.

Auch die „unverzügliche" Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Anders als die Benachrichtigung der Aufsichtsbehörde muss die Benachrichtigung der Betroffenen aber keine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der verantwortlichen Stelle daraufhin ergriffenen Maßnahmen enthalten.

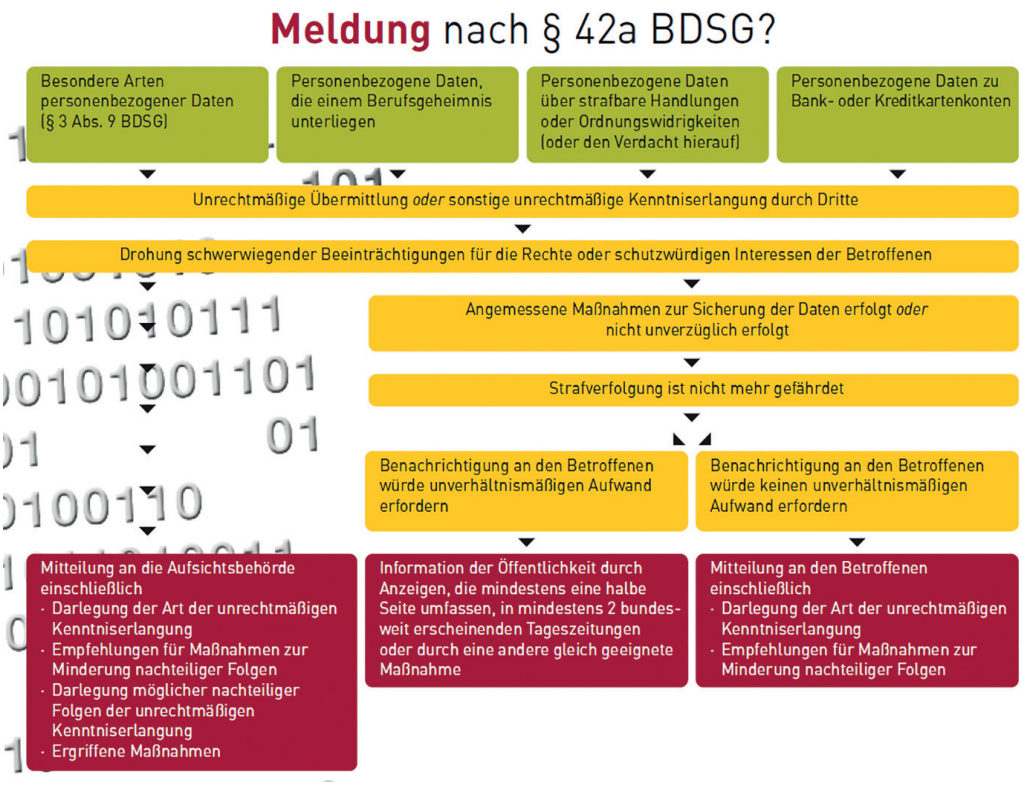
Die Art der Ansprache ist der verantwortlichen Stelle im Wesentlichen frei gestellt. In Betracht kommt sowohl die individuelle Ansprache sowie die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme.

3. Rechtsfolgen von Verstößen

Erfüllt das von einem Datendiebstahl betroffene Unternehmen die ihm obliegende Notifizierungspflicht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig, können sich die durch den eigentlichen Datendiebstahl verursachten Schäden und Nachteile weiter vertiefen. In Betracht kommt auch diesbezüglich wieder eine vertragliche sowie außervertragliche Haftung gegenüber den Geschäftspartnern und Kunden, sofern sich der bei diesen eingetretene Schaden durch die fehlerhafte Benachrichtigung vertieft. Relevanter ist in diesem Zusammenhang aber, dass die fehlerhafte Information selbst eine Ordnungswidrigkeit darstellt, die nach § 43 Abs. 2 Nr. 7 BDSG mit einem Bußgeld von bis zu EUR 300 000 belegt werden kann.

4. Übersicht über die Meldepflicht nach § 42a BDSG

Die einzelnen Prüfungsschritte können wie folgt zusammengefasst werden:



V. Risikomanagement

Die oben angesprochenen Risiken machen es erforderlich, ein Risikomanagement zu betreiben. Ein solches Risikomanagement besteht grundsätzlich aus zwei Teilen: Zum einen sind die Risiken von vorneherein zu minimieren, zum anderen sind die verbleibenden Risiken nach Möglichkeit vom Unternehmen weg zu verlagern.

1. Risikominimierung

Ein Unternehmen muss zunächst einmal ermitteln, mit welchen geschützten Daten das Unternehmen arbeitet und an welchen Stellen. So kann das Unternehmen das Risiko beurteilen, an welchen Stellen mögliche Sicherheitslücken bestehen und wo entsprechende Schutzmaßnahmen zu ergreifen sind.

Eine solche Risikoanalyse sollte alle elektronischen Hilfsmittel einschließen. Neben stationären Geräten und Anwendungen sind dies vor allem mobile Speichermedien, Mobiltelefone, Handheld-Computer, mobile Geräte für den Empfang von E-Mails und Laptops. Zu überprüfen sind hierbei insbesondere ob eine ausreichende und sichere Netzwerkinfrastruktur sowie eine sichere physische Infrastruktur (Zutrittsregelungen, zeitgemäße Verschlüsselungstechnologien, Schlüsselverwaltung) vorhanden und funktionsfähig sind.

Darüber hinaus muss ein Unternehmen Standards einführen, wie mit geschützten Daten umgegangen wird und verhindern, dass geschützte Daten unnötig oft übermittelt werden. Durch standardisierte Prozesse lassen sich nicht nur Fehler vermeiden. Im Haftungsfall kann ein Unternehmen damit unter Umständen zeigen, dass sich ein Datenverlust ohne schuldhafte Pflichtverletzung des Unternehmens ereignete und hierdurch Schadensersatzansprüche vermeiden.

In der Vergangenheit hat sich gezeigt, dass geschützte Daten zu häufig, z. B. auf Laptops mit nach Hause genommen werden und dass sich Angestellte an vereinbarte Beschränkungen nicht halten. So gut die technischen Schutzmaßnahmen im Unternehmen auch sein mögen, so bleibt doch stets die Schwachstelle „Mensch". Häufig setzen Attacken von außen gerade an diesem Punkt an.

Daher sollten Angestellte in Bezug auf den Umgang mit geschützten Informationen sensibilisiert werden. Dies kann z. B. durch die Einführung von IT-Richtlinien erfolgen (so empfiehlt z. B. das Bundesamt für Sicherheit in der Informationstechnik folgende Richtlinien:[11] Richtlinie zur IT-Nutzung, Richtlinie zur Internet- und E-Mail-Nutzung, Richtlinie zum Outsourcing, Sicherheitshinweise für IT-Benutzer, Sicherheitshinweise für Administratoren, Viren-Schutzkonzept, Datensicherungskonzept, Notfallvorsorgekonzept, Archivierungskonzept). Die Einhaltung der im Unternehmen eingeführten Richtlinien sollte auch im Rahmen des Zulässigen kontrolliert werden.

Letztendlich lässt sich ein ordnungsgemäßes Risikomanagement nur einführen und unterhalten, wenn sowohl die technische Seite als auch die organisatorische Seite angemessen berücksichtigt werden.

2. Risikotransfer

Es gibt im Wesentlichen zwei Möglichkeiten, das Risiko vom Unternehmen weg zu verlagern. Zum einen besteht die Möglichkeit, sich für einen entsprechenden Schadensfall zu versichern. Zwar gibt es derzeit noch keine standardisierte Versicherungslösung für einen Datendiebstahl, doch entwickelt sich hier zusehends ein Markt und maßgeschneiderte Versicherungslösungen lassen sich verhandeln. Zum anderen können Unternehmen die verbleibenden Risiken zumindest teilweise auf externe Dienstleister verlagern. Zwar führt der Einsatz externer Dienstleister dazu, dass das Unternehmen für ein Verschulden des externen Dienstleisters haftet, wie für eigenes Verschulden (vgl. § 278 BGB). Wenn ein Datendiebstahl allerdings von einem externen Dienstleister verursacht wurde, steht dem Unternehmen – abhängig von der konkreten Vertragsgestaltung – grundsätzlich der Rückgriff auf den externen Dienstleister offen. Das vom Unternehmen auch ohne Einsatz des externen Dienstleisters zu tragende Risiko eines Datendiebstahls wird daher auf mehrere Schultern verteilt.

VI. Fazit

Nach alledem lässt sich folgendes Fazit ziehen:

(1) Das vermeintliche Opfer eines Datendiebstahls kann medial sowie rechtlich wegen der Ermöglichung der Tat schnell zum „Täter" werden und sich Ansprüchen ausgesetzt sehen. Bislang kam es in Deutschland zwar noch nicht zu einem erheblichen Schadensersatzprozess aufgrund eines Datendiebstahls. Die Erfahrungen aus den USA zeigen jedoch, dass hier ein erhebliches Risiko besteht.

(2) Betroffene Unternehmen sehen sich vertraglichen Haftungsrisiken ausgesetzt. Verstöße gegen regulatorische Anforderungen können die entstehenden Schäden weiter erhöhen.

(3) Durch ein vernünftiges Risikomanagement können Haftungsrisiken minimiert und nach Möglichkeit vom Unternehmen weg verlagert werden.

Dr. Heiko Haller ist Rechtsanwalt und Partner bei Baker & McKenzie am Standort Frankfurt a. M. Er vertritt Unternehmen in komplexen internationalen Schiedsverfahren, insbesondere im Bereich erneuerbarer Energien sowie in der Nuklearindustrie. Innerhalb der European Dispute Resolution Group ist *Heiko Haller* für die Entwicklung und Umsetzung des softwaregestützten Fallmanagements verantwortlich („BakerPro"). Er ist Co-Leiter der Task Force „Cybersecurity".

Dr. Holger Lutz, LL.M., ist Rechtsanwalt bei Baker & Mc Kenzie am Standort Frankfurt a. M. Er berät deutsche und internationale Unternehmen in allen Fragen des Informationstechnologierechts sowie in Fragen des Gewerblichen Rechtsschutzes, des Datenschutzrechts, des Telekommunikationsrechts und des Leasingrechts. Seinen besonderen Beratungsschwerpunkt bilden Rechtsprobleme im Zusammenhang mit Outsourcingverträgen, Hard- und Softwareverträgen, E-Commerce und Datenschutz. Er ist Co-Leiter der Task Force „Cybersecurity".

11 Im Internet abrufbar unter www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html (Abruf: 3.7.2014).