von Rechtsanwalt **Dr. Daniel S. Huber**

Pflichten von Online-Händlern bei Verdacht auf Diebstahl von Kundendaten

Webshops sind einer permanenten Gefahr ausgesetzt, Opfer eines Hacking-Angriffs zu werden. Im Mittelpunkt solcher Server-Angriffe steht häufig der Diebstahl von Kundendaten. Hat ein Online-Händler den begründeten Verdacht, dass Hacker oder sonstige Personen persönliche Daten von Kunden entwendet haben könnten, so ist er von Gesetzes wegen zu einer schnellen Reaktion gezwungen. Die IT-Recht Kanzlei berichtet, welche Schritte ein Online-Händler unternehmen muss, wenn er davon ausgehen muss, dass ihm personenbezogene Kundendaten gestohlen worden und deshalb Dritten zur Kenntnis gelangt sind.

I. Einführung

Durch Hacking in Computersysteme (z.B. Server), Abhandenkommen oder Diebstahl von Datenträgern oder mobilen elektronischen Geräten wie Laptops oder Tablets und durch vertrauensunwürdige Mitarbeiter können bei Webshop-Portalen gespeicherte Kundendaten wie etwa Adress-, Bank-, Kreditkarten-, aber auch telemedienrechtliche Bestands- und Nutzungsdaten in fremde Hände geraten.

Online-Händler, die den Verdacht eines solchen Datenverlustes in Bezug auf ihren Webshop haben, sollten wissen, wie sie darauf richtig und angemessen zu reagieren haben, insbesondere, wen sie bei einem solchen Verdacht wann und in welcher Weise informieren müssen und welche haftungsrechtlichen Folgen auf sie zukommen können.

II. Gesetzliche Meldepflichten

Bei Abhandenkommen von Kundendaten, etwa durch Hacking-Angriffe, unterliegen Online-Händler öffentlich-rechtlichen und zivilrechtlichen Meldepflichten.

1. Öffentlich-rechtliche Meldepflicht gemäß § 42a BDSG

Nach § 42a des Bundesdatenschutzgesetzes (kurz: BDSG) muss eine sog. nichtöffentliche Stelle, also eine natürliche oder juristische Person, eine Gesellschaft oder eine andere Personenvereinigung des privaten Rechts, wie etwa ein kaufmännischer Betrieb oder eine Gesellschaft mit beschränkter Haftung (GmbH), der zuständigen Aufsichtsbehörde sowie dem bzw. den Betroffenen melden, wenn bestimmte personenbezogene Daten (etwa von Kunden) unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

Voraussetzung für diese gesetzliche Meldepflicht ist allerdings zum einen, dass es sich um eine bestimmte Art von personenbezogenen Daten handelt, zum anderen, dass durch die Kenntniserlangung des Dritten schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

a) Besondere Art von personenbezogenen Daten

Die Meldepflicht nach § 42a BDSG besteht lediglich dann, wenn es um ganz besonders sensible personenbezogene Daten, im Einzelnen um:

- gespeicherte besondere Arten personenbezogener Daten nach § 3 Absatz 9 BDSG (das sind Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben - im E-Business-Bereich dürften diese Daten wohl keine Rolle spielen),
- um personenbezogene Daten, die einem Berufsgeheimnis unterliegen (so etwa denkbar bei Ärzten, Anwälten etc.),
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

geht.

Im Online-Handel dürften vor allem Daten über die Bank- und Kreditkartenkonten der Kunden eine Rolle spielen. Sobald diese betroffen sind, ist der Anwendungsbereich von § 42a BDSG eröffnet.

b) Unrechtmäßige Kenntniserlangung durch Dritte

Die gesetzlichen Meldepflichten bestehen darüber hinaus jedoch nur dann, wenn zudem Dritte außerhalb des Unternehmens von diesen unrechtmäßig Kenntnis erlangt haben.

- Dies ist etwa dann der Fall, wenn Daten zu Bank- oder Kreditkartenkonten von Kunden unverschlüsselt an Dritte nach außen gedrungen sind, etwa weil sich ein Hacker Zugriff zu den Servern verschafft und die entsprechenden Kundendaten exportiert hat. Sind die Daten hingegen nach dem Stand der Technik verschlüsselt gewesen, so dass nicht davon auszugehen ist, dass die Hacker die Datensätze entschlüsseln und auslesen können, so ist der Tatbestand der Kenntniserlangung nicht erfüllt; denn dann hätten Dritte nur Kenntnis von verschlüsselten, also insoweit unbrauchbaren Daten, mit denen sie nichts weiter anfangen könnten. Lediglich wenn die Daten nicht oder nur unzureichend verschlüsselt gewesen sind und daher davon auszugehen ist, dass Dritte diese auslesen und nutzen können, ist der Tatbestand diesbezüglich erfüllt.

- Die gesetzliche Meldepflicht besteht darüber hinaus nur dann, wenn das Unternehmen selbst Kenntnis davon hat, dass die entsprechenden Daten Dritten zur Kenntnis geraten sind. Dies muss zumindest sehr wahrscheinlich sein. Die reine Möglichkeit, also der vage Verdacht oder reine Vermutungen, dass sensible Daten nach außen an Dritte gelangt sein könnten, genügen hierfür nicht, um die gesetzliche Meldepflicht auszulösen. Zur Prüfung eines etwaigen Verdachts muss der betroffene Webshop ggf. die Log-Files auswerten, um so rauszufinden, ob und wenn ja welche Daten Eindringlinge exportieren konnten. Online-Händler, die somit lediglich einen Verdacht haben, dass Dritte sensible Daten geklaut haben könnten, unterliegen nicht der gesetzlichen Meldepflicht, wenn der Verdacht keine besonders tragfähige Grundlage hat.

c) Schwerwiegende Beeinträchtigung für Rechte oder schutzwürdige Interessen des Betroffenen

Als dritte Voraussetzung für die gesetzliche Meldepflicht muss es sich nach § 42a BDSG (objektiv) um eine schwerwiegende Beeinträchtigung für Rechte oder schutzwürdige Interessen des vom Datentransfer Betroffenen handeln.
Damit ist gemeint, dass dem Betroffenen ein erheblicher persönlicher Schaden (beispielsweise in Form eines Imageverlustes) oder wirtschaftliche Einbußen drohen müssen; eine lediglich leichte Beeinträchtigung oder eine Belästigung reichen nicht aus.
Allerdings trägt der Webshop-Anbieter das diesbezügliche Prognoserisiko, d.h. er muss dies einschätzen und bei einer Fehleinschätzung die diesbezüglichen negativen Konsequenzen tragen. Häufig lässt sich jedoch abstrakt nicht oder nur schwer sagen, wie sich der Datenverlust konkret auf die einzelnen

Betroffenen auswirken wird. Daher sollte der Webshop-Anbieter im Zweifel besser kein Risiko gehen und der Aufsichtsbehörde und dem Betroffenen lieber einmal zu viel als zu wenig Bescheid geben, soweit sich der eigene (wirtschaftliche) Aufwand hierfür in Grenzen hält.

d) Unverzügliche Meldung an die Aufsichtsbehörde und die Betroffenen:

Liegen die drei genannten Voraussetzungen vor, so muss der vom Datenverlust betroffene Online-Händler sowohl die zuständige Aufsichtsbehörde als auch den bzw. die Betroffenen unverzüglich hierüber informieren.

Unverzügliche Benachrichtigung

Die Benachrichtigung gegenüber der Aufsichtsbehörde und dem Betroffenen hat unverzüglich zu erfolgen, d.h. gemäß § 121 BGB ohne schuldhaftes Zögern seitens des Online-Händlers; hierfür werden in der Regel grundsätzlich 24 bis 48 Stunden veranschlagt. Dabei muss die Benachrichtigung keiner besonderen Form entsprechen, es genügt also eine E-Mail oder in besonders eiligen Notfällen zunächst auch ein Telefonanaruf oder eine SMS.

Betroffener

Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, aber erst nachdem angemessene Maßnahmen zur Sicherung der Daten ergriffen worden sind und die Strafverfolgung nicht mehr gefährdet wird (§ 42a Satz 2 BDSG). Somit darf der Online-Händler den Betroffenen ggf. nicht sofort informieren, sondern muss abwarten, bis das etwaige Datenleck gefunden und beseitigt worden ist, so dass nicht Trittbrettfahrer, die von dem Leck Wind bekommen, ebenfalls Daten stehlen und damit den Schaden noch vergrößern. Dasselbe gilt für die Strafverfolgung: die Strafverfolgungsbehörden sollten möglichst einen Wissensvorsprung vor den Tätern erhalten, damit sie größere Chancen haben, diese aufzuspüren.

Inhaltlich muss die Benachrichtigung des Betroffenen einen Hinweis über die Art und Weise der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten (§ 42a Satz 3 BDSG). Die Betroffenen sollen somit erfahren, dass und welche ihrer Daten in fremde Hände geraten sind, was genau passiert ist und wie sie sich jetzt am besten verhalten können, etwa Kontostände prüfen, Kreditkartendaten sperren oder Passwörter ändern.
Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere gleich wirksame und somit gleichsam geeignete

Maßnahme (§ 42a Satz 5 BDSG).

Zuständige Aufsichtsbehörde

Inhaltlich muss die Benachrichtigung der zuständigen Aufsichtsbehörden zunächst dieselben Angaben enthalten, die auch gegenüber dem Betroffenen gemacht werden müssen.

Darüber hinaus muss zusätzlich angegeben werden, welche nachteiligen Folgen sich durch die Kenntniserlangung der Daten durch Dritte ergeben können und welche Maßnahme der Webshop-Anbieter dagegen ergriffen hat bzw. noch weiter ergreifen wird.

Welche Aufsichtsbehörde bezüglich der Benachrichtigung zuständig ist, hängt davon ab, in welchem deutschen Bundesland der entsprechende Webshop seinen Sitz hat.

Eine Liste der zuständigen Stellen findet sich auf **dieser Webseite**.

Sanktionen

Wer vorsätzlich oder fahrlässig gegen § 42a BDSG verstößt, handelt gemäß § 43 Absatz 2 Nr. 7 BDSG ordnungswidrig, wenn er die entsprechende Mitteilung an die zuständige Aufsichtsbehörde und/oder an den oder die Betroffenen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. Dadurch sind Bußgelder von bis zu EUR 300.000,- möglich, wobei in einfachen Fällen sich die Bußgelder sicherlich im niedrigen Bereich bewegen dürften.

2. Öffentlich-rechtliche Meldepflicht nach § 15a TMG

§ 15a des Telemediengesetzes (kurz: TMG) enthält für Diensteanbieter im Internet wie Webshop-Betreiber hinsichtlich der Bestands- und Nutzungsdaten der Nutzer des Webshops eine Verweisung auf § 42a BDSG.

Dies bedeutet, dass die gesetzliche Meldepflicht aus § 42a BDSG für Online-Händler nicht nur dann besteht, wenn etwa Daten zu Bank- oder Kreditkartenkonten an Dritte gelangen, sondern auch, wenn es um die Bestands- und Nutzungsdaten der Kunden geht, also beispielsweise um die im Internet getätigten Einkäufe, das Surfverhalten sowie die Adressdaten des Kunden.

Mangels entsprechender gesetzlicher Verweisung stellt ein Verstoß gegen § 15a TMG jedoch keine Ordnungswidrigkeit dar, so dass Webshop-Betreiber (wohl zumindest gegenwärtig) nicht fürchten müssen, Ordnungswidrigkeiten zu begehen und Geldbußen entrichten zu müssen, wenn sie den zuständigen

Aufsichtsbehörden und den Betroffenen nicht melden, dass Bestands- oder Nutzungsdaten im Sinne des TMG an Dritte gelangt sind.

Rechtsexperten sind diesbzüglich der Auffassung, dass der Gesetzgeber aufgrund eines redaktionellen Versehens vergessen hatte, die entsprechende Ordnungswidrigkeit zu regeln.

3. Zivilrechtliche Meldepflichten

Neben den öffentlich-rechtlichen Meldepflichten nach § 42a BDSG und § 15a TMG unterliegt ein Webshop-Betreiber auch zivilrechtlichen Meldepflichten, aufgrund des Vertragsverhältnisses zwischen dem Händler und dem Kunden nach § 241 Abs. 2 BGB. Auch aufgrund dieser vom Gesetzgeber bewusst sehr allgemein formulierten Vorschrift muss der Online-Händler den Kunden darüber informieren, dass dessen personenbezogene Daten in fremde Hände gelangt sind, so dass sich der betroffene Kunde vor (weiterem) Schaden hinreichend schützen kann.

Dabei gibt es im Gegensatz zur Situation bei den öffentlich-rechtlichen Meldepflichten keine Beschränkung auf die Art der personenbezogenen Daten, d.h. bei jeder Art von Datenleck muss der Online-Händler seine Kunden entsprechend (ggf. per E-Mail, SMS etc.) informieren.

Die besonderen, für die öffentlich-rechtlichen Meldepflichten nach § 42a BDSG dargestellten Voraussetzungen bestehen gerade nicht bei den zivilrechtlichen Meldepflichten. Dies bedeutet, dass es sein kann, dass ein Webshop-Betreiber zivilrechtlich zur Benachrichtigung seiner Kunden verpflichtet ist, während er aus öffentlich-rechtlicher Sicht keine Meldung an den Kunden oder die zuständige Aufsichtsbehörde tätigen muss.

Verstößt ein Online-Händler gegen seine zivilrechtlichen Meldepflichten, so haftet er bei Vorsatz oder Fahrlässigkeit auf Schadensersatz gemäß §§ 280 Absatz. 1, 241 Absatz 2 BGB.

III. Zivilrechtliche Haftung auf Schadensersatz

1. Haftung aus §§ 280 Absatz 1, 241 Absatz 2 BGB

Verstößt ein Online-Händler vorsätzlich oder fahrlässig i.S.d. § 276 BGB gegen Pflichten aus dem Vertragsverhältnis mit dem Kunden, so hat er dem Kunden den daraus entstandenen Schaden nach Maßgabe der §§ 249 ff. BGB zu ersetzen.

a) Verstoß gegen Datensicherungspflichten

Online-Händler sind nach § 241 Absatz 2 BGB gesetzlich dazu verpflichtet, die Rechtsgüter und Interessen ihrer Kunden zu schützen. Dazu zählt auch die Sicherung (und Verschlüsselung) der Kundendaten vor dem Zugriff Dritter nach dem jeweiligen Stand der Technik, unabhängig davon, ob es sich um Bestands-, Nutzungs- oder Bank- und Kreditkartendaten der Kunden handelt.
Verstößt ein Händler hiergegen vorsätzlich oder fahrlässig i.S.d § 276 BGB, so muss er dem Kunden den daraus entstandenen Schaden ersetzen. Dieser kann beispielsweise darin liegen, dass die Dritten, die die Daten gestohlen haben, unter der Identität des
Kunden Käufe tätigen, so dass Kosten entstehen, oder die Bankkonten des Kunden leerräumen.

b) Verstoß gegen Informationspflichten

Weiter sind Online-Händler nach § 241 Absatz 2 BGB auch dazu verpflichtet, den Kunden über Gefahren und Gefährdungen aufzuklären. Dazu zählt auch die unverzügliche Aufklärung über den Diebstahl von Daten durch Dritte. Hat somit ein Händler zwar die Daten sorgfältig nach dem Stand der Technik gesichert, so dass er für den Hackerangriff auf den Server mit dem damit verbundenen Datenklau nichts kann, so muss er dennoch für die Schäden beim Kunden haften, die diesem deshalb entstanden sind, weil der Händler ihn gar nicht, nicht richtig oder nicht rechtzeitig und umfassend über den Vorfall informiert hat.

In diesen Fällen muss der geschädigte Kunde darlegen und ggf. beweisen, dass und in welcher Höhe ihm ein solcher Schaden entstanden ist.

2. Haftung aus Delikt

Verstoßen Online-Händler gegen die öffentlich-rechtlichen Meldepflichten aus § 42a BDSG bzw. § 15a TMG, so haften sie auf Ersatz des daraus entstandenen Schadens ebenfalls nach § 7 BDSG und nach § 823 Absatz 2 BGB in Verbindung mit § 42a BDSG bzw. § 15a TMG.

IV. Fazit

Zusammenfassend ergibt sich folgendes Bild:

- Online-Händler unterliegen öffentlich-rechtlichen Meldepflichten gemäß § 42a BDSG und § 15a TMG, wenn sie erfahren, dass Dritte von personenbezogenen Daten ihrer Kunden wie Bank- und Kreditkartendaten sowie telemedienbezogene Bestands- und Nutzungsdaten Kenntnis erlangt haben und diesen dadurch schwerwiegende Beeinträchtigungen drohen. Dabei trägt der Händler das Prognoserisiko bezüglich der Einschätzung der Folgenschwere des Datenzugriffs. Haben Händler lediglich den Verdacht, dass Dritte solche besonders sensiblen Kundendaten erlangt haben, so bestehen die gesetzlichen Meldepflichten nicht; denn die bloße Möglichkeit oder Vermutung der Kenntniserlangung der Daten durch Dritte genügt nicht, diese muss vielmehr sehr wahrscheinlich sein, damit die gesetzliche Meldepflicht ausgelöst wird.
- Online-Händler kommen ihrer Meldepflicht aus § 42a BDSG und § 15a TMG dadurch nach, dass sie die durch den unrechtmäßigen Datenzugriff Betroffenen sowie die zuständige Aufsichtsbehörde unverzüglich, d.h. ohne schuldhaftes Zögern in Kenntnis setzen und darüber informieren, was genau passiert ist, wie schwer die Folgen sind und wie der Betroffene den Schaden möglichst gering halten kann. Während der Händler die Aufsichtsbehörde in jedem Fall möglichst sofort benachrichtigen muss, kann er im Einzelfall dazu verpflichtet sein, gegenüber dem Kunden damit solange zuzuwarten, bis das Datenleck gefunden und behoben sowie die Strafverfolgungsbehörden entsprechend informiert und tätig geworden sind, so dass weder ein noch größerer Schaden (etwa durch Trittbrettfahrer) entsteht, noch die Strafverfolgung durch indirekte Warnung der Täter vereitelt wird.
- Gegenüber den vom Datenklau Betroffenen sind Online-Händler nicht nur öffentlich-rechtlich, sondern auch zivilrechtlich zur Benachrichtigung gemäß § 241 Absatz 2 BGB verpflichtet.
- Bei vorsätzlichen oder fahrlässigen Verstößen gegen die öffentlich-rechtliche Meldepflicht aus § 42a BDSG drohen Geldbußen bis zu EUR 300.000,- sowie Schadensersatzansprüche der Betroffenen nach § 7 BDSG und § 823 Absatz 2 BGB in Verbindung mit § 42a BDSG. Bei vorsätzlichen oder fahrlässigen Verstößen gegen die zivilrechtliche Melde- und Aufklärungspflicht aus § 241 Absatz 2 BGB bestehen ebenfalls Schadensersatzansprüche (gemäß §§ 280 Absatz 1, 241 Absatz 2 BGB).

Autor:
RA Dr. Daniel S. Huber
Rechtsanwalt