von **Sebastian Segmiller**

Online-Shops: Was tun nach Hackerangriff? – Nachsorge und Vorsorge mit Blick auf den BMI-Entwurf eines IT-Sicherheitsgesetzes

Hackerangriffe auf die IT-Infrastruktur von Unternehmen werden immer häufiger. Dabei sind längst nicht mehr nur große Firmen betroffen. Auch kleinere und mittlere Unternehmen sehen sich zunehmend Attacken ausgesetzt. Besonders lukrativ sind dabei Onlineshops, lassen sich hier doch in aller Regel Kundendaten, insbesondere Bankverbindungen, ausspähen, die dann für potentielle Angriffe auf die Konten der Kunden genutzt werden können.

Wie geht man als betroffener Unternehmer bei solchen Angriffen vor? Was ist zu tun und wie kann bzw. muss man solche Attacken künftig verhindern?

Nachfolgender Beitrag soll Aspekte der Nachsorge (I.) und der Vorsorge (II.) gegen Hackerattacken beleuchten. Dabei soll auch ein Blick auf den BMI-Entwurf eines IT-Sicherheitsgesetzes geworfen werden.

I. Nachsorge

Wir wollen zunächst von einem Szenario ausgehen, bei dem ein Hackangriff bereits erfolgt ist.

1. Schadensermittlung

Am Anfang steht die Sichtung der Lage. Es ist zu klären, welche Systeme betroffen waren und welche Daten ausgelesen wurden.

Die Bestimmung der ausgespähten Daten ist für das weitere Vorgehen essentiell, daher sollte hier größtmögliche Sorgfalt an den Tag gelegt werden.

Natürlich ist es in vielen Fällen nicht möglich, genau zu identifizieren, ob und welche Daten im Einzelnen gestohlen wurden. Dann ist eine Aufstellung der möglicherweise betroffenen Daten zu fertigen. Anschließend muss eine Wahrscheinlichkeitseinschätzung vorgenommen werden. Es muss beurteilt werden, wie wahrscheinlich es ist, dass die jeweiligen Daten von unbefugten erlangt wurden. Dazu später mehr.

Sind die betroffenen Daten ermittelt, hängt es von deren Einordnung ab, ob Informationspflichten bestehen.

2. Bestehen einer Informationspflicht

Für bestimmte Daten und ab einer gewissen Gefahrenprognose mit Blick auf Rechtsgüter und Interessen der Nutzer ist eine Informations-/Meldepflicht gegenüber der zuständigen Aufsichtsbehörde und den betroffenen Nutzern vorgesehen.

Zentrale Norm hierfür ist § 42a BDSG.

> “
>
> § 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten
> Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte
>
> 1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
> 2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
> 3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
> 4. personenbezogene Daten zu Bank- oder Kreditkartenkonten
>
> unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. 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, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.
>
> ”

Für den Bereich der Telemedien wird § 42a BDSG durch § 15a TMG ergänzt, der auf § 42a BDSG verweist:

> § 15a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten
>
> Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

a) Art der betroffenen Daten

§ 42a BDSG stellt (u.a.) für private Unternehmen (§ 2 Abs. 4 BDSG) eine Informationspflicht über Hackerangriffe auf, wenn bestimmte Daten betroffen sind.

Für Onlineshop-Betreiber sind insbesondere die personenbezogenen Daten zu Bank- oder Kreditkartenkonten, § 42a Satz 1 Nr. 4 BDSG relevant.

Auch besondere Arten personenbezogener Daten i.S.d. § 42a Satz 1 Nr. 1 i.V.m. § 3 Abs. 9 BDSG können für bestimmte Shops, etwa im Gesundheitsbereich, relevant werden. Das sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Über § 15a TMG, der auf § 42a BDSG verweist, werden auch Bestands- und Nutzungsdaten miteinbezogen.

Nachfolgende Übersicht zeigt die relevanten Daten und ihre Definition:

Art der Daten	Definition
Personenbezogene Daten zu Bank- oder Kreditkartenkonten, § 42a Satz 1 Nr. 4 BDSG	(nach dem FAQ des Berliner Beauftragten für Datenschutz und Informationsfreiheit, Stand 21. Dezember 2010, Teil A 3. d); im Folgenden: FAQ Berlin, zu finden neben anderen Informationen zu diesem Thema unter http://www.lda.bayern.de/lda/datenschutzaufsicht/Unternehmen_Information/lda_informationen_unternehmen.htm) - Sämtliche Daten, die mit solchen Konten in Zusammenhang stehen - bereits Tatsache, dass Kontobeziehung besteht, umfasst - Karten- und Kontonummern, auch wenn kein Namensbezug - Transaktionsdaten, Prägespurdaten, Überweisungsvordrucke, Kreditkartenbelege, Kontoauszüge
Besondere Arten personenbezogener Daten, § 42a Satz 1 Nr. 4 i.V.m. § 3 Abs. 9 BDSG	rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben z.B. auch Personalakten oder Lohnsteuerabrechnungen, wenn entsprechende Daten enthalten (FAQ Berlin, Teil A 3. a))
Bestandsdaten, §§ 15a, 14 TMG i.V.m. § 42a BDSG	Solche Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Dazu zählen insbesondere (Zscherpe in Taeger/Gabel (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013, § 14 TMG Rn. 16): - Personalien des Nutzers (Name, Anschrift, Telefonnummer, E-Mailadresse, ...) - Log-In Daten u.ä. (Benutzername, Passwort, ggf. auch IP-Adresse, sofern als personenbezogen betrachtet) - Informationen über Abrechnungsmodus - Zahlungsmodalitäten (Zeiträume, Zahlungsart, ...) - Weitere Vereinbarungen über Nutzungsmodalitäten o.ä.
Nutzungsdaten, §§ 15a, 15 TMG i.V.m. § 42a BDSG	Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Dazu zählen Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Abzustellen ist hier auf den konkreten Nutzungsvorgang und nicht wie bei den Bestandsdaten auf die Grundlage der (abstrakten) Nutzung. Allerdings überschneiden sich die Begriffe teilweise, insbesondere etwa bei Identifikationsdaten, die sowohl als Grundlage der Nutzung, als auch bei jeder einzelnen Nutzung erhoben werden. Nutzungsdaten sind z.B. die Zeiterfassungen bei der Nutzung von Streamingportalen mit zeitbasierter Abrechnung und die Information darüber, welche Inhalte der Nutzer angesehen hat. Auch (andere) Abrechnungsdaten sind erfasst (vgl. Zscherpe in Taeger/Gabel (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013, § 15 TMG Rn. 12 ff.).

Von Bedeutung ist in diesem Zusammenhang die Unterscheidung von Bestandsdaten/Nutzungsdaten und Inhaltsdaten:

Bestandsdaten/Nutzungsdaten sind nur Daten, die Begründung, Inhalt und Änderung der Nutzung des Dienstes bzw. die konkrete Nutzung (unmittelbar) betreffen. D.h. bei einem Onlineshop nur solche Daten, die die Nutzung des Shops als solchen betreffen, z.B. Log-In Daten.

Daten, die für über den Dienst geschlossene Verträge, wie z.B. den im Shop geschlossenen Kaufvertrag und die sich daran anschließende Warenlieferung und Bezahlung, relevant sind, sind (i.d.R.) keine Bestandsdaten/Nutzungsdaten, sondern Inhaltsdaten. Sie unterfallen damit (i.d.R.) nicht dem TMG, sondern dem BDSG (vgl. Zscherpe in Taeger/Gabel (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013,§ 14 TMG Rn. 19 ff.)

Die Personalien eines dauerhaft für den Onlineshop registrierten Benutzers sind somit Bestandsdaten, soweit sie unmittelbar die Nutzung des Shops betreffen (wenn z.B. bestimmte Angebote nur für eingeloggte Nutzer sichtbar sind oder bestimmte Funktionen des Shops nur im eingeloggten Zustand genutzt werden können). Andere Personalien oder Personalien eines Nutzers, der nur als Gast bestellt und damit die Daten nicht zur Nutzung des Dienstes (= Shop) sondern zur Durchführung seines Kaufvertrages (Bestellung) angibt, sind hingegen Inhaltsdaten und unterfallen nur dem BDSG.

Auch solche Daten können aber dem TMG unterfallen, wenn die Bestellung selbst einen Telemediendienst darstellt (so Zscherpe aaO, der als Beispiel die Bestellung von Inhalten für E-Books nennt).

Das hat für die Frage der Informationspflicht Bedeutung:

Liegen keine Bestands- sondern Inhaltsdaten vor, ist § 42a BDSG direkt anwendbar und eine Meldepflicht ergibt sich nur für die dort genannten Daten.

So müsste z.B. ein Ausspähen von Personalien gemeldet werden, wenn diese zur Nutzung des Shops, also des Dienstes, gespeichert wurden und damit Bestandsdaten oder Nutzungsdaten darstellen. Nicht gemeldet werden müsste eine solches Ausspähen hingegen, wenn diese Personalien, etwa bei Gastbestellungen, nicht zur Nutzung des Shops (das ist ja auch anonym möglich) sondern nur zur Abwicklung des Kaufvertrags erhoben wurden, sofern sie nicht unter die in § 42a BDSG genannten Daten fallen (wird also nur Name und Adresse des Gastnutzers ausgespäht, bestünde keine Meldepflicht; hätte ein Gastnutzer hingegen zusätzlich z.B. seine Gewerkschaftszugehörigkeit angegeben, etwa um einen exklusiven Rabatt für Gewerkschaftsmitglieder zu erhalten, bestünde wegen § 42a Satz 1 Nr. 1 i.V.m. § 3 Abs. 9 BDSG Meldepflicht, sofern die weiteren Voraussetzungen vorliegen, s.u.).

Da jedoch der wohl häufigste und relevanteste Fall das Ausspähen von Bank- oder Kreditkartenkontodaten sein dürfte und diese in jedem Fall von § 42a BDSG erfasst werden, wird auch bei Inhaltsdaten meist eine Informationspflicht bestehen.

b) unrechtmäßige Kenntniserlangung

§ 42a BDSG (i.V.m. § 15a TMG) setzt eine unrechtmäßige Übermittlung oder unrechtmäßige Kenntniserlangung durch Dritte auf sonstige Weise voraus.

Das ist gegeben, wenn die Betroffenen nicht zugestimmt haben und kein gesetzlicher Erlaubnistatbestand vorliegt (FAQ Berlin, Teil A. 4.).

Bei Hackerangriffen ist dies immer erfüllt. Sie fallen dabei unter die Alternative der unrechtmäßigen Kenntniserlangung durch Dritte auf sonstige Weise.

Die unrechtmäßige Kenntniserlangung muss nicht mit Sicherheit feststehen. Es genügt, wenn diese offensichtlich ist oder aufgrund tatsächlicher Anhaltspunkte eine gewisse Wahrscheinlichkeit dafür besteht (vgl. FAQ Berlin, aaO)

Diese Beurteilung obliegt dem Diensteanbieter. Er trägt auch das Risiko einer Fehleinschätzung (wenn keine Information erfolgt, sich dann aber herausstellt, dass ein Angriff und Datendiebstahl stattgefunden hat), d.h. er haftet bei ihm vorwerfbarer Nichtinformation (siehe dazu auch unten). Es sollte stets bedacht werden, dass eine verspätete oder nicht erfolgte Mitteilung an die betroffenen Nutzer zu beträchtlichen Schäden bei diesen führen kann. Werden z.B. Kontoinformationen entwendet, kann durch rechtzeitige Information den Nutzern ermöglicht werden, die Konten zu sperren. Je schneller dies geschieht, umso größer ist die Chance, Schäden zu verhindern. Daher sollte auch dann über eine Information der Nutzer nachgedacht werden, wenn (nach sorgfältiger Beurteilung) keine gesetzliche Pflicht dazu besteht.

Erweist sich die Beurteilung als schwierig, sollte der Beurteilungsvorgang sorgfältig und nachvollziehbar dokumentiert werden.

c) Schwerwiegende Beeinträchtigungen für Rechte/Interessen der Nutzer

Sowohl § 42a BDSG als auch § 15a TMG sehen eine Informationspflicht nur im Falle schwerwiegender Beeinträchtigungen für Rechte/Interessen des/der Nutzer vor.

Der Diensteanbieter hat hier eine Prognoseentscheidung auf Grundlage der Art der betroffenen Rechte und schutzwürdigen Interessen und der Wahrscheinlichkeit eines Schadenseintritts zu treffen. Je schutzwürdiger die Rechte und Interessen sind, d.h. je stärker mögliche Beeinträchtigungen ausfallen, desto geringer sind die Anforderungen an die Wahrscheinlichkeit.

Es muss bedacht werden, wer (soweit bekannt) welche Daten erlangt hat und wozu diese verwendet werden können. Etwaige (zivilrechtliche) Ausgleichsansprüche der betroffenen Nutzer bleiben außer Betracht. Die Nutzer sollen in die Lage versetzt werden, rechtzeitig effektive Gegenmaßnahmen zu ergreifen. Das Risiko eines Irrtums/einer Fehleinschätzung trägt der Diensteanbieter (wie bereits oben bei der Frage, ob ein Angriff erfolgt ist/Daten entwendet wurden). Eine Dokumentation des Entscheidungsprozesses inklusive nachvollziehbarer Begründung unter Einbeziehung des Datenschutzbeauftragten, sofern vorhanden, ist dringend anzuraten (FAQ Berlin, Teil A 5.).

Sind die in § 42a BDSG benannten Daten betroffen, wird häufig eine schwerwiegende Beeinträchtigung

der Rechte/Interessen der Nutzer drohen, da es sich dabei per se um sehr sensible Daten handelt (Moos in Taeger/Gabel (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013, § 15a TMG Rn. 6). Gerade bei Kontodaten kann innerhalb kürzester Zeit ein weiterer Angriff auf die jeweiligen Konten erfolgen. Dadurch können enorme finanzielle Schäden entstehen.

Bei Bestands- bzw. Nutzungsdaten i.S.d. §§ 15a, 14, 15 TMG dürfte dies nicht immer der Fall sein. Gerade bei bloßen Identifikationsdaten wie Name und Anschrift wird regelmäßig keine schwerwiegende Beeinträchtigung drohen (Moos aaO).

Ferner stellt § 15a TMG explizit auf die Rechte/Interesse des betroffenen Nutzers ab, § 42a BDSG hingegen auf diejenigen der Betroffenen (Plural!). Bei Bestands- bzw. Nutzungsdaten wird daher eine schwerwiegende Beeinträchtigung nicht schon aus der großen Anzahl Betroffener abzuleiten sein (Moos in Taeger/Gabel (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013,§ 15a TMG Rn. 7).

3. Information der Aufsichtsbehörde und der betroffenen Nutzer

Besteht eine Informationspflicht, ist diese wie folgt zu erfüllen:

a) Zeitpunkt

Die Information muss nach § 42a Satz 1, 2 BDSG „unverzüglich“, d.h. ohne schuldhaftes Zögern (§ 121 Abs. 1 Satz 1 BGB) erfolgen.

Gegenüber der Aufsichtsbehörde ist der Zeitpunkt maßgeblich, zu dem vom Angriff Kenntnis erlangt wurde. Dem Unternehmen wird ein Prüfzeitraum zugebilligt, dessen Länge einzelfallabhängig ist. I.d.R. werden dies nicht mehr als zwei Wochen sein (FAQ Berlin, Teil B. 1.).

Gegenüber den Betroffenen ist unverzüglich zu informieren, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Wird die Information (insbesondere der Betroffenen) verzögert, sollten die Gründe dokumentiert werden (FAQ Berlin aaO).

Maßnahmen zur Sicherung sind nur solange ein Grund für die Zurückhaltung der Information der Betroffenen, wie eine solche den Erfolg der Maßnahmen gefährden würde. Solche Maßnahmen sind z.B. bei Sicherheitslücken der Software Rücksprachen und Beseitigungsaufforderungen an den Hersteller („responsible disclosure“). Hinsichtlich einer Gefährdung der Strafverfolgung sollte der Einschätzung des zuständigen Staatsanwalts gefolgt werden (FAQ Berlin aaO).

b) Inhalt

Die Aufsichtsbehörde ist über folgende Punkte zu unterrichten (§ 42a Satz 4 BDSG und FAQ Berlin Teil B 2.):

- Wann kamen die Daten abhanden bzw. wann wurde dies entdeckt?
- Welche Daten sind betroffen?
- Wie wurden diese unberechtigt erlangt?
- Welche nachteiligen Folgen sind möglich?
- Welche Maßnahmen wurden ergriffen?
- Wurden die Betroffenen benachrichtigt? Wenn nein, warum nicht? Wenn ja, was wurde empfohlen?

Die einzelnen Punkte sind jeweils ausführlich zu erläutern. Sämtliche relevanten Informationen sollten mitgeteilt werden. Im Falle einer bloßen Wahrscheinlichkeit für einen Angriff ist diese ausführlich darzulegen.

Die Betroffenen sind über die Art der unrechtmäßigen Kenntniserlangung zu informieren und ihnen sind Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen zu geben, § 42a Satz. 3 BDSG. Die Betroffenen müssen erkennen können, welche Daten konkret betroffen sind und wie sie Schutzmaßnahmen treffen können. Es sind konkrete Handlungsempfehlungen zu geben, die auf den Wissensstand der Betroffenen Rücksicht nehmen. Auch Unterstützung in Form von Hotlines ist möglich (FAQ Berlin Teil B 3.).

c) Form

Die Aufsichtsbehörde sollte schriftlich benachrichtigt werden, um später ggf. die Benachrichtigung nachweisen zu können (wenngleich eine Form nicht explizit vorgeschrieben ist).

Eine Liste der Aufsichtsbehörden der Länder findet sich hier.

Die Betroffenen sind grundsätzlich individuell zu benachrichtigen, wie aus § 42a Satz 5 folgt. Letzterer sieht nur für den Fall, dass eine individuelle Benachrichtigung unverhältnismäßig aufwendig ist, eine öffentliche Benachrichtigung vor. Dazu soll eine mindestens halbseitige Anzeige in zwei bundesweit erscheinenden Tageszeitungen erfolgen, alternativ eine andere gleich geeignete Maßnahme.

Für den Bereich der Telemedien dürfte in entsprechender Anwendung des § 42a BDSG, wie von § 15a TMG vorgesehen, eine Veröffentlichung im Internet genügen (Moos in Taeger/Gabel (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013, § 15a TMG Rn. 8).

Es ist jedoch schon aus Gründen der Vermeidung negativer Publicity eine individuelle Benachrichtigung dringend anzuraten.

Diese kann per E-Mail an die betroffenen Nutzer erfolgen. Die Mailversendung sollte aus Nachweisgründen dokumentiert werden. Im Falle der Benachrichtigung per Postversand sollte zum Nachweis des Zugangs ein Einwurf- oder Übergabeeinschreiben gewählt werden (Übergabeeinschreiben haben jedoch den Nachteil, dass bei Nichtantreffen und anschließender Nichtabholung kein Zugang

eintritt und auch eine Zugangsfiktion infolge Zugangsvereitelung nicht immer greift. Beim Einwurfeinschreiben sollten die Postbelege gut aufbewahrt werden, da nur über diese im Wege des Anscheinsbeweises der Zugang nachgewiesen werden kann).

Eine Information im Newsletter genügt allenfalls dann, wenn sichergestellt ist, dass jeder der betroffenen Nutzer den Newsletter erhält. Da gerade bei Online-Shops viele Nutzer auf ein Abonnement des Newsletter verzichten, wird eine Newsletterbenachrichtigung häufig nicht ausreichen. Zudem kann die Information in einem Newsletter auch sehr schnell „untergehen", wenn zusätzlich über andere Dinge berichtet wird. Das kann der Annahme einer individuellen Benachrichtigung entgegenstehen. Zumindest sollte daher ein Sondernewsletter gewählt werden. Da bei einem solchen aber immer auch nicht betroffene Nutzer adressiert werden, scheint eine Einzelbenachrichtigung via E-Mail (im Sinne eines Rundschreibens an alle Betroffenen) vorzugswürdig.

4. Konsequenzen bei Verstößen

Wer seiner Mitteilungspflicht nach § 42a BDSG nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt, handelt ordnungswidrig und kann mit einer Geldbuße bis zu 300.000 Euro belegt werden, § 43 Abs. 2 Nr. 7, Abs. 3 BDSG. Auch eine Straftat nach § 44 Abs. 2 BDSG ist denkbar.

Eine entsprechender Ordnungswidrigkeitentatbestand (bzw. Straftatbestand) fehlt jedoch im TMG, sodass Verstöße gegen § 15a TMG keine Ordnungswidrigkeiten (oder Straftaten) darstellen (hinsichtlich der Ordnungswidrigkeit ist dies wohl ein Redaktionsversehen des Gesetzgebers, eine Analogie zu § 43 BDSG ist aber wegen § 3 OWiG nicht möglich, Moos in Taeger/Gabel (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013,§ 15a TMG Rn. 9).

Ferner kommen Schadensersatzansprüche der Betroffenen in Betracht.

Besteht zu diesen eine vertragliche Beziehung, wäre an §§ 280 I, 241 II BGB zu denken. Das jeweilige Vertragsverhältnis dürfte im Rahmen seiner Schutzpflichten zum sicheren Umgang mit und zum Schutz sensibler Daten ebenso verpflichten wie zu einer Möglichst raschen und umfassenden Information über das Abhandenkommen solcher Daten. Vor oder nach Beendigung vertraglicher Beziehungen käme eine Haftung auf derselben Grundlage i.V.m. den Grundsätzen der culpa in contrahendo, § 311 Abs. 2 BGB, bzw. der culpa post contractum finitum in Betracht.

Außerhalb vertraglicher Beziehung ist an § 823 Abs. 2 i.V.m. § 42a BDSG bzw. 15a TMG zu denken. Auch eine Verkehrspflichtverletzung im Rahmen des § 823 Abs. 1 in Form der unterlassenen Information käme in Betracht, sofern Rechtsgüter des § 823 Abs. 1 betroffen sind.

Ferner wären Abmahnungen/Unterlassungsansprüche durch Konkurrenten denkbar (§ 8 Abs. 1 und 3 Nr. 1, §§ 3, 4 Nr. 11 UWG i.V.m. § 42a BDSG bzw. §15a TMG), sofern man § 42a BDSG bzw. § 15a TMG marktverhaltensregelnden Charakter i.S.d. § 4 Nr. 11 UWG zuschreibt (was denkbar wäre, da sowohl das BDSG als auch die datenschutzrechtlichen Normen des TMG eine Datenerhebung zu geschäftlichen Zwecken ermöglichen und § 42a BDSG bzw. § 15a TMG einem verantwortungslosen/sorglosen Umgang im Falle von Störungen im Zusammenhang mit diesen Erhebungen Grenzen setzen, um die Persönlichkeitsrechte des Nutzers zu schützen, die gerade durch seine Marktteilnahme, also sein Marktverhalten, berührt werden; vgl. OLG Köln, Urteil vom 14. August 2009, Az. 6 U 70/09, wo § 28 BDSG

in gewissem Umfang marktverhaltensregelnder Charakter zugebilligt wird).

5. Strafanzeige

Schließlich kann und sollte Strafanzeige gestellt werden (die Strafbarkeit von Hackerangriffen folgt aus § 202a StGB). Sollten die Angreifer – wie meistens – nicht bekannt sein, kann Anzeige gegen unbekannt erstattet werden.

II. Vorsorge

Damit es gar nicht erst zu derartigen Konsequenzen kommt, empfiehlt es sich, Hackerangriffen frühzeitig vorzubeugen.

1. Vorsorgemöglichkeiten

Die Möglichkeiten der Vorsorge sind vielfältig und in hohem Maße einzelfallabhängig.
Hier können daher nur einige allgemeine Punkte, die wahrscheinlich vielen bereits bekannt sind, angesprochen werden.

Software und Hardware sind auf dem neuesten Stand zu halten. Das bedeutet, stets aktuelle Updates zu installieren, Patches/Bugfixes anzuwenden, Empfehlungen des Herstellers/Entwicklers zu beachten und technische Entwicklungen zu beobachten. Eine starke Verschlüsselung, die dem aktuellen Stand der Technik entsprich, kann helfen, im Fall von Angriffen den Schaden zu begrenzen.

Zugänge, etwa zu administrativen Backends von Content-Management-Systemen, sind ausreichend zu sichern. Passwörter sind so zu wählen, dass sie nicht ohne weiteres durch einfache Software ermittelt werden können (d.h. in der Regel mindestens sechs Zeichen oder mehr, darunter Groß- und Kleinbuchstaben sowie Sonderzeichen).

Personal ist ausreichend zu schulen. Nachlässigkeiten, z.B. nicht sauber beendete Programme oder Dienste, können Einfallstore für Hacker bilden. Gegebenenfalls sind Softwareinstallationsrechte auf einen engen Personenkreis zu beschränken. Attacken werden nicht selten über zuvor versehentlich installierte Programme (Trojaner etc.) geführt. Hilfreich kann auch ein interner IT-Leitfaden sein, in dem Hinweise zum sicheren Umgang mit der IT-Infrastruktur gegeben werden (keine unbekannten Mailanhänge öffnen, etc.)

Für Fälle, in denen einen Informationspflicht nach §§ 42a BDSG, 15a TMG greift, sollte ein Verfahren schriftlich definiert sein, das einzuhalten ist. Zuständigkeiten sollten klar geregelt und die Dokumentation sichergestellt sein.

Im Sinne einer größtmöglichen Schadensbegrenzung im Ernstfall sollte auch überprüft werden, ob alle derzeit gespeicherten Daten wirklich benötigt werden. Auch wenn Einwilligungen der Nutzer vorliegen, sollten nicht relevante Daten nicht unnötig auf den Servern aufbewahrt werden.

2. Vorsorgepflicht

Unabhängig von etwaigen vertraglichen oder deliktischen Schutz- bzw. Verkehrssicherungspflichten könnte sich in naher Zukunft für Betreiber von Internetseiten eine Pflicht zur Sicherung ihrer Systeme gegen unberechtigte Zugriffe aus dem TMG ergeben.

Der vergangenen Montag, 18.08.2014, veröffentlichte „Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)“ des Bundesinnenministeriums (BMI) sieht eine Ergänzung des § 13 TMG vor. Dort soll folgender Absatz 7 eingefügt werden:

> *„(7) Diensteanbieter im Sinne von § 7 Absatz 1 und § 10 Absatz 1 haben, so-weit dies technisch möglich und zumutbar ist, für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien durch die erforderlichen technischen und organisatorischen Vorkehrungen sicherzustellen, dass ein Zugriff auf die Telekommunikations- und Datenverarbeitungssysteme nur für Berechtigte möglich ist. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Bei personalisierten Telemediendiensten ist den Nutzern die Anwendung eines sicheren und dem Schutzbedarf angemessenen Authentifizierungsverfahrens anzubieten.“*

Um angemessene Erkennungs-, Eingrenzungs- und Beseitigungsmaßnahmen in Bezug auf Störungen zu ermöglichen, soll in § 15 TMG ferner folgender Abs. 9 eingefügt werden, der dazu eine über die bisherige Regelung hinausgehende Erhebung und Verwendung von Nutzungsdaten zulässt:

> *„(9) Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 gilt entsprechend.“*

Damit soll insbesondere das beiläufige Herunterladen von Schadsoftware auf einer präparierten Webseite (Drive-by-downloads) eingedämmt werden. Solche Downloads stellen der Entwurfsbegründung zufolge einen der Hauptverbreitungswege von Schadsoftware dar.

Genannt wird zudem auch eine Verbreitung von Schadsoftware durch fremde, kompromittierte Werbebanner auf der eigenen Seite.

Als mögliche Maßnahmen werden die regelmäßige Softwareaktualisierung, das Einspielen von Sicherheitspatches und die vertragliche Verpflichtung der Werbenden, entsprechende Schutzmaßnahmen zu treffen, genannt.

Die Regelung trifft ausweislich der Entwurfsbegründung alle kommerziellen Telemedienanbieter, vom Kleingewerbetreibenden bis zum Großunternehmer.

Über das Merkmal der Erforderlichkeit könnten einzelfallabhänge Lösungen gefunden werden. Erforderlich seien Maßnahmen dann, wenn der nötige Aufwand in einem angemessenen Verhältnis zum zu erreichenden Schutzzweck stehe.

Hinzu kommt zudem die Verpflichtung, bei personalisierten Telemediendiensten (also v.a. Internetangebote, die eine Identifizierung, etwa durch Ausweisvorlage o.ä., erfordern) ein sicheres und dem Schutzbedarf angemessenes Authentifizierungsverfahren anzubieten. Verfahren, die den aktuellen Richtlinien des BSI entsprechen, sollen dabei laut Entwurfsbegründung genügen.

Ob diese Verpflichtungen letztlich in dieser Form bestehen bleiben und wie genau sie sich - sollte dies der Fall sein – in der Praxis auswirken, bleibt abzuwarten.
Eine Bußgeldbewehrung bei Verstößen ist bislang nicht vorgesehen.

III. Fazit

Wer als Internetdienstleister Opfer eines Hackerangriffs wurde, sollte folgende Punkte beachten, entsprechend handeln und (!) dies sorgfältig und nachvollziehbar dokumentieren:

1. Schaden ermitteln ? welche Daten wurden betroffen?

2. Informationspflicht (§§ 42a BDSG, 15a TMG) bedenken

a) Wurden Bestands- oder Nutzungsdaten nach §§ 15a, 14, 15 TMG oder Daten nach § 42a Satz 1 Nr. 1-4 BDSG betroffen?

b) Steht eine unberechtigte Kenntniserlangung fest oder ist wahrscheinlich?

c) Drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des/der betroffenen Nutzer(s)?

3. Information erteilen

a) der Aufsichtsbehörde: schriftlich und unverzüglich, i.d.R. nicht später als zwei Wochen nach Kenntnis

- Wann kamen die Daten abhanden bzw. wann wurde dies entdeckt?
- Welche Daten sind betroffen?
- Wie wurden diese unberechtigt erlangt?
- Welche nachteiligen Folgen sind möglich?
- Welche Maßnahmen wurden ergriffen?
- Wurden die Betroffenen benachrichtigt? Wenn nein, warum nicht? Wenn ja, was wurde empfohlen?

b) den Betroffenen: unverzüglich, sofern nicht Sicherungsmaßnahmen oder Strafverfolgung gefährdet, über Art des Angriffs und der Daten unter Empfehlung von Maßnahmen zur Minderung etwaiger nachteiliger Folgen

- Information individuell an jeden Betroffenen per E-Mail oder Einschreiben (Newsletter reicht eher nicht)

- Nur, wenn individuelle Information nicht möglich/unverhältnismäßig aufwendig, öffentliche Information möglich durch halbseitige Anzeige in zwei bundesweit erscheinenden Tageszeitungen oder gleichwertige Maßnahme bzw. wohl auch im Internet, sofern nur Pflicht über § 15a TMG i.V.m. § 42a BDSG

Um Angriffen wirksam vorzubeugen, sollten Software und Hardware immer auf dem neuesten Stand gehalten, Zugänge ausreichend gesichert und Personal entsprechend geschult werden. Solche Maßnahmen zur Prävention unbefugter Zugriffe auf sensible Daten sind nicht zuletzt mit Blick auf den aktuellen Entwurf eines IT-Sicherheitsgesetzes des Bundesinnenministeriums anzuraten.

Inwieweit die Prävention tatsächlich zu einer explizit gesetzlich geregelten Pflicht wird, bleibt abzuwarten.

Autor:
Sebastian Segmiller
(jur. Mitarbeiter der IT-Recht Kanzlei)