/ Data Breaches: 5 Praxistipps

10.04.2015
IT & Outsourcing | Datenschutz

Ob Sicherheitslücken in Kundendatenbanken (vgl. FAZ online vom 10. Februar 2015), gezielte Hacker-Angriffe auf IT-Systeme (vgl. Zeit online vom 18. Dezember 2014), versehentlich falsch adressierte E-Mail-Verteiler (vgl. RP online vom 20. März 2015) oder an falsche Empfänger zugestellte Bankauszüge (vgl. Nordbayerischer Kurier vom 23. Dezember 2014): Wenn man die Meldungen der Tagespresse als Gradmesser heranzieht, scheint seit geraumer Zeit kaum mehr ein Tag zu vergehen, an dem nicht die eine oder andere Datenpanne zu beklagen ist.

Solche Datenpannen, auch „***Data Breaches***" genannt, können schnell zum Verlust einer erheblichen Anzahl **personenbezogener** oder sonstiger hochsensibler **Daten** führen. Für betroffene Unternehmen stellt das nicht nur ein beträchtliches **Haftungsrisiko** dar. Vor allem drohen irreparable **Imageschäden** oder die geschäftsschädigende **Offenbarung wichtiger Geschäftsgeheimnisse**. Umso dringender stellt sich die Frage, wie betroffene Unternehmen mit derartigen Datenpannen am besten umgehen sollten. Die folgenden fünf Praxistipps sollen einen Überblick über die wesentlichsten Schritte einer effektiven und zielführenden Bewältigung von Data Breaches geben:

1. Unverzügliches Ergreifen von Sofortmaßnahmen

Unverzüglich nach Entdeckung eines Data Breaches sollten in einem ersten Schritt **Sofortmaßnahmen mit dem Ziel der bestmöglichen Schadensvermeidung und Schadensbegrenzung** ergriffen werden. Die getroffenen Sofortmaßnahmen sollten mit Blick auf potentielle Haftungsrisiken und die unter Umständen erforderliche Information von Aufsichtsbehörden und Betroffenen (hierzu noch 4.) im Einzelnen **dokumentiert** werden.
Um weiteren Datenverlust zu vermeiden, sollten erkannte **Sicherheitslücken** umgehend geschlossen und die erforderlichen Sicherheitsmaßnahmen getroffen werden. Das kann im Extremfall auch die vorübergehende vollständige oder teilweise Stilllegung betroffener IT-Systeme oder etwa deren Trennung vom Internet erfordern. Bei abhanden gekommenen mobilen IT-Systemen, wie etwa Mobiltelefonen oder Notebooks, bietet sich etwa eine **Fernlöschung** an, falls die Geräte mit hierfür geeigneter Software ausgestattet sind.

Schwieriger wird die Schadensbegrenzung hinsichtlich solcher abhanden gekommener Daten, die bereits unberechtigten Dritten zur Kenntnis gelangt sind oder bei denen eine Kenntnisnahme durch unberechtigte Dritte nicht ausgeschlossen werden kann. Hier sind weitergehende Schritte zu unternehmen, um einen Missbrauch der Daten bestmöglich zu vermeiden. Sind von einer Datenpanne etwa **Zugangsdaten** von Kunden oder Mitarbeitern betroffen, sollte sichergestellt werden, dass betroffene Zugänge bis zu einer erneuten Legitimation durch den Berechtigten, etwa über besondere Sicherheitsabfragen, gesperrt oder zumindest eingeschränkt werden.

2. Informationsermittlung und Beweissicherung

Hand in Hand mit der Umsetzung der Sofortmaßnahmen gehen notwendigerweise Maßnahmen zur **Ermittlung aller relevanter Informationen** über den Data Breach. Die gewonnenen Informationen dienen nicht nur als Grundlage für die zukünftige nachhaltige Verbesserung der IT-Sicherheit (hierzu noch 5.), sondern vor allem für die erforderliche rechtliche Bewertung und haftungsrechtliche Risikoanalyse des Data Breaches (hierzu sogleich 3.) sowie für die unter Umständen erforderliche Information der Aufsichtsbehörden und Betroffenen (hierzu noch 4.).
Ziel dieser Maßnahmen ist eine detaillierte Analyse des Data Breaches, insbesondere dahingehend, auf welche Weise Daten abgeflossen sind und ob und welche Daten Dritten unrechtmäßig bekannt geworden sind oder noch bekannt werden könnten. Die möglichen nachteiligen Folgen der Datenpanne sind dabei unter allen in Betracht kommenden Gesichtspunkten umfassend zu ermitteln.

Zeitgleich sind Maßnahmen zur **Beweissicherung** durchzuführen. Je nach Art und Ausmaß der Datenpanne sollten hierzu

gegebenenfalls spezialisierte Dienstleister für eine **forensische IT-Untersuchung** eingebunden werden.

3. Rechtliche Bewertung des Data Breaches

Auf Grundlage der ermittelten Informationen ist eine rechtliche Bewertung und haftungsrechtliche Risikoanalyse des Data Breaches vorzunehmen, insbesondere auch im Hinblick auf die Erfüllung **gesetzlicher Informationspflichten** und eine potentielle **zivilrechtliche Haftung** gegenüber Betroffenen.
Im Fokus der rechtlichen Bewertung stehen dabei zunächst die für den Fall bestimmter Datenpannen vorgesehenen **gesetzlichen Informationspflichten**: § 42a Bundesdatenschutzgesetz (BDSG), sowie § 15a Telemediengesetz (TMG) und §§ 93 Abs. 3, 109a Telekommunikationsgesetz (TKG) fordern unter bestimmten Voraussetzungen eine unverzügliche Information der zuständigen Aufsichtsbehörde sowie der von der Datenpanne betroffenen Personen. Die gesetzlichen Informationspflichten der § 42a BDSG und § 15a TMG greifen etwa dann ein, wenn **bestimmte Kategorien personenbezogener Daten** unrechtmäßig übermittelt oder auf sonstige Weise **Dritten unrechtmäßig zur Kenntnis gelangt sind**. Die unrechtmäßige Kenntnisnahme durch unbefugte Dritte muss dabei nicht positiv festgestellt sein. Vielmehr entsteht die Informationspflicht schon dann, wenn eine **hohe Wahrscheinlichkeit einer unbefugten Kenntnisnahme durch Dritte** besteht. Die §§ 93 Abs. 3, 109a TKG knüpfen eine Informationspflicht an die **Verletzung des Schutzes personenbezogener Daten** im Anwendungsbereich des TKG, also an eine Verletzung der Datensicherheit, die zur unrechtmäßigen Verwendung personenbezogener Daten führt, die im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste verarbeitet werden (§ 3 Nr. 30a TKG).

Die gesetzlichen Informationspflichten setzen voraus, dass **schwerwiegende Beeinträchtigungen** für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen oder anzunehmen sind. Die verantwortliche Stelle hat bei der rechtlichen Bewertung eine **objektive Gefahrenprognose** vorzunehmen, ob über die mit dem Datenverlust einhergehende Verletzung des Rechts auf informationelle Selbstbestimmung des Betroffenen hinaus eine weitere **schwerwiegende** Beeinträchtigung seiner Rechte oder Interessen zu befürchten ist (z.B. Identitätsdiebstahl). Je gravierender dabei die Folgen für den Betroffenen sein können, desto geringere Anforderungen sind an die Eintrittswahrscheinlichkeit der Beeinträchtigung zu stellen.

4. Information von Behörden und Betroffenen – „Data Breach Notification“

Sofern nach dem Ergebnis der rechtlichen Bewertung gesetzliche Informationspflichten (§ 42a BDSG, § 15a TMG, §§ 93 Abs. 3, 109a TKG) eingreifen, sind die zuständigen Aufsichtsbehörden und in der Regel auch die von dem Data Breach Betroffenen **unverzüglich** zu informieren. Die Benachrichtigung der Betroffenen muss unter anderem eine Darlegung der Art des Data Breaches und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörden muss zusätzlich eine Darlegung möglicher (nachteiliger) Folgen des Data Breaches und der beabsichtigten bzw. bereits ergriffenen Gegenmaßnahmen enthalten.
Eine Information der Betroffenen kann aber auch in solchen Fällen rechtlich erforderlich oder aus anderen Gründen empfehlenswert sein, in denen keine ausdrücklich gesetzlich geregelten Informationspflichten eingreifen:
Schon aus **Imagegründen** kann es für ein Unternehmen ratsam sein, Datenpannen proaktiv anzugehen und betroffene Kunden über das Problem und seine Folgen zu informieren. Die Erfahrung zeigt, dass ein Datenverlust schneller als erwartet in das mediale Rampenlicht geraten kann. Hält ein betroffenes Unternehmen hier Informationen zu lange zurück, besteht die Gefahr, dass das Vertrauen der Kunden erheblichen Schaden nimmt.

Im Übrigen kann die Information der Betroffenen **aus rechtlichen Gründen** auch in Fällen erforderlich sein, in denen keine ausdrücklich gesetzlich geregelte Informationspflicht eingreift. Einerseits können sich Informationspflichten aus allgemeinen **vertraglichen Schutzpflichten** ergeben. Eine Information dürfte in vielen Fällen aber auch zur **Eingrenzung der Haftung** gegenüber den Betroffenen geboten sein.

5. „Post mortem“-Review und „Data Loss Prevention“ –Strategie

Nicht zuletzt sollte der Data Breach im Nachgang einer ausführlichen **„Post Mortem“-Analyse** unterzogen und die aus dem Data

Breach gewonnenen Erkenntnisse, insbesondere auch die negativen wie positiven Erfahrungen aus dem Umgang mit der Datenpanne, zur nachhaltigen Verbesserung der Datensicherheit im Unternehmen der und Erarbeitung einer **„Data Loss Prevention"-Strategie** eingesetzt werden.
Spätestens ein Data Breach sollte der verantwortlichen Stelle Anlass geben, die Datensicherheit im Unternehmen insgesamt zu überprüfen und erforderliche Schritte zur Optimierung von Datenschutz und Datensicherheit in die Wege zu leiten. Dabei ist nicht nur an eine **regelmäßige Überprüfung und Optimierung der eingesetzten IT-Systeme** und **Implementierung anerkannter IT-Sicherheitsstandards** zu denken. Wesentlicher Bestandteil einer nachhaltigen Strategie zur Gewährleistung und stetigen Verbesserung von Datenschutz und Datensicherheit im Unternehmen sind fachlich fundierte **Mitarbeiter-Schulungen** in regelmäßigen Abständen. **Verbindliche Unternehmensrichtlinien und Leitfäden** sollten daneben die Verbindlichkeit und den Stellenwert des verantwortungsvollen Umgangs mit personenbezogenen und sonstigen sensiblen Daten unterstreichen.

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. Daniel Rücker

Practice Group: IT, Outsourcing & Datenschutz

Weitere Artikel: Service-Level-Agreements: 5 Praxistipps

Das könnte Sie auch interessieren: **Outsourcing Day 2015** am 23. April 2015 in München

Contact Person

Dr. Daniel Rücker, LL.M.
Leiter Datenschutz
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628457

Sebastian Dienst
Mitglied der Practice Group Datenschutz
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628457