

Bruch der Datensicherheit: ein Albtraum

Der Anruf eines Mandanten weckt den Anwalt aus tiefem Schlaf: Ein ungesichertes Smartphone oder Tablet eines Mitarbeiters mit wichtigen Kundendaten ist verschwunden – vermutlich gestohlen. Keiner im Unternehmen ist erreichbar. Was tun? Eine schwierige Situation: Soll das Unternehmen die Alarmglocken läuten? Wer muss innerhalb und außerhalb des Unternehmens benachrichtigt werden? Was ist, wenn das Gerät unversehens wieder auftaucht? Zumindest der Imageschaden für das Unternehmen kann enorm sein, wenn das Unternehmen umsonst Alarm geschlagen hat. Wenn das Unternehmen und der Rechtsberater die falsche Weiche stellen, drohen Schadensersatzforderungen der Betroffenen oder Geldbußen. Durchschnittlich kostet ein Unternehmen ein sog. Data Breach-Störfall US-\$ 3,8 Mio., wie das *Ponemon Institute* auf der Basis von elf Ländern kürzlich errechnet hat – 23% mehr als noch im Vorjahr.

§ 42a BDSG regelt auf allgemeiner Ebene die Informationspflichten der nicht-öffentlichen Stellen beim Bruch der Datensicherheit, allerdings nur für konkrete Daten: besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG), personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten. Das deutsche TK-Recht hält weiterhin im § 109a TKG eine Reihe von Regelungen für öffentliche TK-Anbieter bereit. Diese Vorschriften rühren eher an die Spitze des Eisbergs, der weit über den deutschen Rechtsbereich hinausreicht. Die Niederlande haben am 26.5.2015 ein neues Gesetz zur Meldepflicht verabschiedet. Das deutsche IT-Sicherheitsgesetz weckt Erwartungen, deckt aber auch nur einen Teilbereich ab.

Das Risiko, etwas in diesem hochsensiblen – möglicherweise auch strafrechtlich relevanten – Sektor falsch zu machen, wächst fast logarithmisch mit Big Data und dem Internet of Things. In einer Welt voll von RFID-Chips, Kameras und Sensoren wird auch das Problem des Bruchs der Datensicherheit immer größer und schwieriger zu lösen. Die Datenmenge wächst und der Datenfluss ist nur noch schwierig zu verfolgen. Die Bedrohung durch „Ugly Gorillas“ und andere von fremden Regierungen oder Dritten gesponserte Hacker hat der weitgereiste Sozialwissenschaftler *Phillip N. Howard* (Yale University) in seinem neuen Buch „Pax Technica“ sehr anschaulich beschrieben. Eine Forderung in dem Buch ist, dass die Unternehmen in einer Art

Verteidigungspakt freiwillig eng zusammenarbeiten. Aber wer deckt schon gerne interne Regeln und Zugriffsrisiken gegenüber seinen Wettbewerbern auf?

Kommt es zu einem Störfall, wissen die meisten Unternehmensmanager oder Behördenleiter häufig nicht, was überhaupt passiert ist und welche und wessen Daten betroffen sind. Hinzu kommt, dass viele Endgeräte schon von Haus aus nicht datensicher sind: „Die heutige Sicherheit in vielen Geräten ist außergewöhnlich schwach. Die Frage ist nicht, ob sich Malware verbreitet, sondern welche Maßnahmen die Hersteller und Unternehmen ergreifen, um das System adäquat herunterzufahren. Eine hundertprozentige Sicherheit ist nicht erreichbar, ebenso nicht die Verhinderung aller kriminellen Akte; der Einsatz ist enorm und die Bedrohung reicht weit über mit dem Internet verbundene Waschmaschinen oder Lichtschalter hinaus“ (S. *Greengard*,

Internet of Things, S. 160). Beim Internet of Things geht es nicht nur um die Lokalisierung von Objekten, sondern um die Beobachtung, die Vermessung der Bewegung der Welt und unserer Handlungen. Die generierten Daten erlauben tiefe Einblicke in die menschlichen Beziehungen, den Umgang miteinander und sogar die Physik unseres Planeten (a.a.O., S. 169).

Diese große Menge von generierten Daten und ihre möglichen Verknüpfungen durch das Internet of Things werfen viele neue Fragen auf:

- Ist der Bruch der Datensicherheit von der Haftpflichtversicherung abgedeckt?
- Welcher IT-Partner steht kurzfristig zur Verfügung, um die Folgen des Störfalls zu analysieren?
- Welche Beweissicherungsmaßnahmen müssen durchgeführt werden?
- Wo befinden sich die vom Störfall Betroffenen?
- Wie kann der Datenfluss nach außen kurzfristig unterbunden werden?
- Wer nutzt die betroffenen Daten?

Der Gesetzgeber in den USA hechelt der Entwicklung hinterher: Seit dem Jahr 2002 bis heute weisen die Gesetze der meisten US-Bundesstaaten Regelungen zur Mitteilungspflicht bei einem Bruch der Datensicherheit auf. Ein Bundesgesetz gibt es in den USA trotz verschiedener Initiativen im *US-Kongress* immer noch nicht. Die *Federal Trade Commission (FTC)* und in bislang geringerem Umfang der *U.K. Information Commissioner* bestrafen



Dr. Axel Spies
ist Rechtsanwalt bei
Morgan, Lewis & Bockius LLP,
Washington DC/Frankfurt/M.,
und Mitherausgeber der ZD.

Unternehmen, die ihre Daten ungenügend gesichert haben – die Tendenz der Fälle ist steigend. Die *Cybersecurity-Abteilung des US-Justizministerium (DoJ)* hat am 29.4.15 eigene Leitlinien zum Bruch der Datensicherheit veröffentlicht (Best Practices for Victim Response and Reporting of Cyber Incidents), die leicht im Internet zu finden sind. Deren Vorschläge betreffen insbesondere den Notfallplan der Unternehmen, bevor es zu einem solchen Ereignis kommt. Vor allem sollten die Unternehmen vorab intern klären, wer die Verantwortung für die verschiedenen Schritte eines Plans hat, wie diese Personen zu erreichbar sind und wie der Umgang mit einem Bruch der Datensicherheit festgestellt und notfalls nach außen kommuniziert wird. In Frage kommen die Aufsichtsbehörden, Polizei und möglicherweise schon zu einem frühen Stadium betroffene Dritte. Alle Beteiligten sollten die Verfahren einüben. Das *DOJ* schlägt auch die ständige Beobachtung des Netzes auf Eindringlinge hin vor. Besonderen Wert legt das *DOJ* auf die erste Einschätzung des Bruchs der Datensicherheit (Was und wer ist betroffen? Woher kommt die Bedrohung? Wer ist eingeloggt?). Gerade in dieser weichenstellenden Phase können zahlreiche Fehler gemacht werden. Das *DOJ* empfiehlt überdies, alle in und außerhalb des Unternehmens getroffenen Maßnahmen genau zu protokollieren und eine forensische Sicherung (Forensic Image) zu erstellen. Um den Erfordernissen Rechnung zu tragen, werden die meisten Unternehmen nicht um eine detaillierte, auf das Unternehmen angepasste „Data Breach Policy“ (interne Richtlinien zum Bruch der Datensicherheit) herumkommen.

Das *Bundeswirtschaftsministerium (BMWi)* hat die Initiative „IT-Sicherheit in der Wirtschaft“ gestartet, um das IT-Sicherheitsniveau bei kleinen und mittelständischen Unternehmen zu verbessern. Ein Kernbereich ist der *IT-Sicherheitsnavigator* – ein von der Initiative „IT-Sicherheit in der Wirtschaft“ entwickeltes Informationsangebot, das sich insbesondere an kleine und mittelständische Unternehmen richtet. Er bündelt und kategorisiert kostenlose Informations- und Beratungsangebote regionaler und bundesweit tätiger IT-Sicherheitsinitiativen und gibt einen schnellen Überblick über regionale Beratungsstellen, Basis-Sicherheitschecks zum Selbsttesten, einen Veranstaltungskalender sowie Broschüren und Leitfäden. Hinzu kommen die Initiativen des *BSI*, wie die „Sicherheitsempfehlungen für Cloud-Computing-Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit)“.

Der *Berliner Datenschutzbeauftragte* hat eigene FAQs zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG veröffentlicht. Er stellt u.a. klar, dass ein Auftragsdatenverarbeiter selbst nicht Adressat des genannten § 42a BDSG ist: „Gem. § 11 Absatz 4 BDSG gelten für den Auftragnehmer nur bestimmte Vorschriften des BDSG. § 42a BDSG wird in § 11 Absatz 4 BDSG nicht erwähnt und zählt daher nicht zu den für den Auftragnehmer anwendbaren Vorschriften. Für einen Verlust von Daten, die beim Auftragnehmer im Auftrag gespeichert waren, ist der Auftraggeber verantwortlich.“ Der

Auftraggeber muss demnach dafür Sorge tragen, dass der Auftragnehmer zur unverzüglichen Meldung gegenüber dem Auftraggeber verpflichtet ist, wenn es beim Auftragnehmer einen Bruch der Datensicherheit gibt. Diese Meldung kann problematisch sein, wenn der Auftragnehmer z.B. im Ausland sitzt und eventuell selbst noch nicht viele Kenntnisse über die Datenpanne hat. Wie bei dem Kinderspiel „Stille Post“ kann es dann passieren, dass die Beteiligten die vorhandenen Informationen verändert, verwässert oder schlimmstenfalls gar nicht weitergeben. Die von den Behörden geforderte „Kontrolle des Meldeprozesses“ ist keine einfache Aufgabe. Besonders relevant wird die Informationspflicht, wenn medizinische Daten betroffen sind (Dateien von Ärzten, Krankenhäusern, Versicherungen etc.), einschließlich der Kontaktdaten von Patienten, § 42a Satz 1 Nr. 1 BDSG. Schwierig wird die Analyse, wenn Datenträger an Orten verlorengehen, wo sie Dritten zugänglich sind und die Daten verschlüsselt sind. Dann stellt sich die Frage, wie sicher dieser Schlüssel sein muss, damit das Unternehmen davon ausgehen kann, dass kein Dritter die Daten unberechtigt auswerten kann. Der *Berliner Datenschutzbeauftragte* führt hierzu aus: „Eine Zugangssperre, etwa in Form des Windows-Login, reicht nicht aus. Diese kann technisch leicht umgangen werden.“ Nicht nur an Bedrohungen von außen ist zu denken. Hält sich z.B. ein Mitarbeiter nicht an seine arbeitsvertraglich festgelegten Befugnisse und schickt er Daten unbefugt an private eigene E-Mail-Adressen, dann handelt er nach Auffassung der Datenschutzbehörden als Privatperson. Er steht dann außerhalb der verantwortlichen Stelle und wird mithin zum „Dritten“, § 3 Abs. 8 Satz 2 BDSG.

Die zahlreichen, für ein Unternehmen nicht einfach zu filternden Initiativen und Ratschläge entlassen die Unternehmen nicht aus der Verpflichtung, die für sie geeigneten und notwendigen Maßnahmen auszuwählen und umzusetzen – dies allein ist schon eine anspruchsvolle Aufgabe. Ein hoher Sicherheitsstandard erfordert einigen Aufwand an Investitionen, den die Verantwortlichen gegenüber dem Vorstand, der Geschäftsführung usw. rechtfertigen müssen. Der deutsche Begriff „Datenpanne“ verniedlicht das Problem. Die „Datenpanne“ kann an die Existenz des Unternehmens rühren und zahlreiche Haftungsfolgen auslösen. Faktoren wie eine absichtliche Schädigung durch eigene Mitarbeiter (z.B. aus Unzufriedenheit oder Rache) und Konkurrenten, menschliches Versagen, Gutgläubigkeit oder auch nur Unachtsamkeit kann auch die beste Data Breach-Policy kaum einfangen. Data Breach-Policies sind keine „Schlafmittel“ oder bloße Beruhigungspillen für das Management, insbesondere wenn sie intern nicht umgesetzt, eingeübt und nötigenfalls überarbeitet und nicht an die sich ändernden Bedürfnisse angepasst werden. Wer sich in falscher Sicherheit wiegt, hat vermutlich schon verloren („If you snooze you lose“). Insofern dürften diese Themen mit ihren vielfältigen Szenarios für Störfälle vielen IT-Sicherheitsexperten und ihren Beratern einige unruhige Nächte bereiten.