DBSC Infoletter Datenschutz-Praxis ► 2013-09

Datenschutzkonforme Gestaltung und Nutzung von Cloud Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten.

Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zutragen.

Zu verlangen sind also mindestens

• offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

• transparente, detaillierte und eindeutige vertragliche Regelungen der Cloudgestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität, • die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und CloudAnwender und

• aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe (http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf) der Arbeitskreise "Technik" und "Medien" zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

Quelle: Bericht der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Angriff auf Server von Vodafone Deutschland: Stammdaten von zwei Millionen Kunden erbeutet

12.9.2013: Vodafone Deutschland ist Ziel eines kriminellen Datenangriffs auf einen seiner Server geworden. Dieser Angriff war nur mit hoher krimineller Energie sowie Insiderwissen möglich und fand tief versteckt in der IT-Infrastruktur des Unternehmens statt. Dabei erlangte der Täter Zugang zu Stammdaten von 2 Millionen Personen. Er entwendete Angaben zu Name, Adresse, Geburtsdatum, Geschlecht, Bankleitzahl und Kontonummer. Sicher ist, dass der Täter keinen Zugang zu Kreditkarten-Daten, Passwörtern, PIN-Nummern, Mobiltelefonnummern oder Verbindungsdaten hatte. Vodafone bedauert den Vorfall sehr und bittet alle Betroffenen um Entschuldigung. Diese werden derzeit per Brief informiert.

Der Angriff wurde von Vodafone entdeckt, gestoppt und unverzüglich zur Anzeige gebracht. Seitdem arbeitet das Unternehmen eng mit den deutschen Aufsichts- und Justizbehörden zusammen. Sämtliche Zugänge, die der Täter genutzt hatte, wurden sicher verschlossen. Dieser Fall betrifft ausschließlich Vodafone Deutschland, andere Länder sind nicht berührt. Die Behörden hatten Vodafone zunächst gebeten, keine Informationen an die Öffentlichkeit zu geben, um die Ermittlungen nicht zu gefährden. Inzwischen haben sie einen

Tatverdächtigen identifiziert und bei ihm eine Hausdurchsuchung vorgenommen. In Abstimmung mit den Behörden informiert Vodafone Deutschland jetzt alle betroffenen Personen umfassend und unterstützt sie dabei, mögliche Beeinträchtigungen zu vermeiden.

Von Vodafone eingeschaltete unabhängige Sicherheitsexperten bestätigen: Es ist für den Täter kaum möglich, mit den gestohlenen Daten direkt auf die Bankkonten der Betroffenen zuzugreifen. Allerdings könnte mit zusätzlichen Phishing-Attacken, zum Beispiel durch gefälschte E-Mails, versucht werden, weitere Daten wie Passwörter und Kreditkarteninformationen abzufragen. Vodafone rät seinen Kunden daher zu besonderer Vorsicht bei möglichen Telefon- oder E-Mail-Anfragen, in denen sie zur Herausgabe von persönlichen Informationen wie Passwörtern oder Kreditkartendaten aufgefordert werden. Vodafone stellt solche Anfragen grundsätzlich nicht. Ferner sollten Kunden ihre Kontoauszüge regelmäßig überprüfen und bei Unregelmäßigkeiten umgehend ihre Bank kontaktieren.

Quelle: http://www.vodafone.de/privat/hilfe-support/kundeninformation.html?icmp=Privatkunden

Refurbishing - Laptop weiterverkauft, samt der Daten des Vorbesitzers

Ein Elektronikmarkt verkaufte einen, wegen eines Defekts umgetauschten Laptop mit privaten Daten als Neuware. Der neue Besitzer fand darauf Steuerunterlagen, Firmenpapiere und private Fotos eines anderen Kunden. Die Sache ging vor Gericht.

Es waren vertrauliche Daten: Steuerunterlagen, Firmenpapiere, private Fotos. Um so größer war der Schrecken des Kunden, ein Münchner Geschäftsmann, als wildfremde Leute anriefen, um ihm mitzuteilen, dass sie all diese Dokumente auf einem als neu gekauften Laptop gefunden hatten. Tatsächlich hatte der Geschäftsmann seinen tragbaren Computer, den er bei einem großen Elektronikmarkt gekauft hatte, schon sehr schnell wegen eines Totalausfalls gegen ein neues Gerät eintauschen müssen. Für knapp 800 Euro hatte der Münchner den Laptop vor vier Jahren in einem Pasinger Elektronikmarkt gekauft. Noch am selben Tag hatte er alle wichtigen Daten von einem mobilen Speicher auf die Computerfestplatte überspielt. Dann ließ sich der PC aber nicht mehr hochfahren. Als der Mann den Schaden umgehend reklamierte und im Rahmen der Gewährleistung anstandslos ein Ersatzgerät bekam, habe er auf die Datenübertragung hingewiesen: Dies versicherte er in der Verhandlung und erklärte, dass der Verkäufer ihm die sofortige Löschung zugesichert habe.

Fast drei Jahre später kam dann der Anruf der neuen Besitzer, die im selben Elektronikmarkt genau diesen PC erworben hatten - angeblich als originalverpacktes neues Gerät. Dass sich die vertraulichen Daten des Vorbesitzers darauf befanden, bemerkten sie aber erst viel später, nachdem das Gerät erneut ausgefallen war. Ein computerkundiger Nachbar hatte ihnen geholfen, den Rechner wieder flott zu machen und war dabei auf mysteriöse Dateien gestoßen, deren Inhalt erkennbar sehr persönlich war.

Im folgenden Rechtsstreit zwischen dem betroffenen Kunden und dem Elektronikmarkt war die mit der Sache befasste Richterin der Auffassung, dass es im Allgemeinen Sache des Eigentümers sei, für die Löschung vertraulicher Daten zu sorgen. Allerdings habe das Gerät in diesem Fall überraschend nicht mehr funktioniert und eine mechanische Zerstörung der Festplatte wäre wohl überzogen gewesen, meinte die Richterin. Andererseits habe der Verkäufer bei einer Rückgabe noch am Kauftag nicht unbedingt damit rechnen müssen, dass schon so viele wichtige Daten aufgespielt seien.

Die Parteien waren um Einigung bemüht. Der Ausgang des Verfahrens ist nicht bekannt.

Quelle: Süddeutsche Zeitung vom 13.08.2013 - http://www.sz.de/1.1745963

Fazit: Wichtige vertrauliche oder persönliche Informationen sollten niemals unverschlüsselt auf Laptops transportiert werden - sie können leicht in die Hände unbefugter Dritter geraten. Nicht nur für den Fall eines Defekts eines Laptops oder PC's sollten Sicherheitskopien angefertigt werden. Bei vorhandenen Backups fällt es leicht, die Festplatte von persönlichen Daten zu reinigen oder sogar vollständig zu formatieren. Darüber hinaus finden sich im Internet zahlreiche Werkzeuge für die sichere Löschung von Daten.

Nützliche Links für Informationen zur IT-Sicherheit und Werkzeugen:

- BSI für Bürger: http://www.bsi-fuer-buerger.de
- Computerwoche: Ratgeber Festplatten-Verschlüsselung: Wie Notebooks sicherer werden, unter http://www.computerwoche.de/a/wie-notebooks-sicherer-werden,2484630
- Heidi Computers Eraser, Download z.B. unter http://www.chip.de/downloads/Eraser_12994923.html
- (Kostenlose) IT-Sicherheits-Werkzeuge, z.B. unter http://www.heise.de/security/tools/