DATENSCHUTZ

Big Data – digitale Chance, digitales Risiko

Daten werden ein immer wichtigerer Rohstoff für Unternehmen, und der Umgang mit ihnen birgt neben Chancen auch gravierende Risiken. Wie sieht also eine nachhaltig praktikable Strategie zum sicheren Umgang mit großen Datenmengen aus?

> Warum Sie diesen Artikel lesen sollten: Ohne das digitale Verwerten von Daten läuft heute in vielen Branchen nichts mehr. Erfahren Sie, wie man die Chancen von „Big Data“ nutzt und die Risiken in Schach hält.

Der 15. Dezember 2016 gestaltete sich für Marissa May, die damalige Vorstandsvorsitzende des Online-Konzerns Yahoo!, alles andere als vorweihnachtlich-beschaulich: Das Unternehmen musste einräumen, Opfer eines groß angelegten Datendiebstahls geworden zu sein. Schlimmer noch: Der digitale GAU hatte bereits drei Jahre zuvor stattgefunden. Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten sowie Sicherheitsfragen und -antworten, die zu mehr als einer Milliarde Nutzerkonten gehörten, waren von unbekannten Angreifern ausspioniert und später von osteuropäischen Hackern zum Kauf angeboten worden.

Wenn es um „Big Data“ geht, sind sowohl die Datenmengen als auch die wirtschaftlichen Chancen riesig – laut einer Studie des vom Bundeswirtschaftsministerium geförderten Forschungszentrums Informatik könnte der weltweite Umsatz mit Big-Data-Lösungen bis 2025 auf mehr als 85 Milliarden Euro steigen. Doch auch die Risiken sind beachtlich. Kaum ein Tag vergeht, ohne dass Sicherheitslücken bei Unternehmen oder Behörden aufgespürt werden. Der Missbrauch von Nutzer- oder Kundendaten kann einiges Unheil anrichten. Ein Blick in die Nachrichten – oder in die Kataloge der Anbieter von Lösungen für IT-Security – und man würde am liebsten die Finger von dem ganzen Thema lassen.

Keine gute Idee, meint Jana Moser, auf Datenschutz spezialisierte Rechtsanwältin in Berlin. „Natürlich kann man auch einfach gar nichts machen, aber dann ist man eben bald nicht mehr wettbewerbsfähig. Durch eine solche Verzichts-Strategie schneidet man sich von neuer Technologie ab, wird langsamer und teurer als die Konkurrenz.“ Beim Umgang mit Daten, so die promovierte Juristin, sei demgegenüber ein Vorgehen empfehlenswert, das die Chancen nutzt, die in ihnen stecken, und gleichzeitig die Risiken im Auge behält. Die entscheidende Frage: Wie erhebe, nutze und sichere ich Daten – vor allem die meiner Kunden – möglichst effektiv und effizient, ohne dabei Recht zu verletzen?

Der Rahmen, in dem sich Unternehmen dabei bewegen, wird bislang vor allem von drei Gesetzen beschrieben: dem IT-Sicherheitsgesetz, dem Bundesdatenschutzgesetz und dem Telekommunikationsgesetz. Dazu kommen, eine Ebene darunter, noch eine Vielzahl von weiteren Gesetzen und Verordnungen, in denen Einzelaspekte des Umgangs mit Daten behandelt werden. In Deutschland stets im Fokus: das Recht des Einzelnen auf informelle Selbstbestimmung. Jeder Mensch soll selbst entscheiden können, wem wann welche personenbezogenen Daten zugänglich sein sollen. Dies bringt für Unternehmen Pflichten mit sich, denen sie sich nicht immer bewusst sind. Beispiele dafür sind

die Meldepflicht für Verfahren, mit denen personenbezogene Daten automatisiert verarbeitet werden, oder die Bestellung eines betrieblichen Datenschutzbeauftragten ab einem bestimmten Umfang der Datenverarbeitung.

> „Natürlich kann man in Sachen Daten auch einfach gar nichts machen, aber dann ist man eben bald nicht mehr wettbewerbsfähig."
> Jana Moser, Datenschutz-Expertin

Ab dem nächsten Jahr kommt auch eine europäische Rechtsgrundlage hinzu. Denn ab dem 25. Mai 2018 gilt in allen EU-Mitgliedsstaaten eine neue „Datenschutz-Grundverordnung", die einen EU-weiten Rahmen für die Nutzung und den Schutz von Daten zieht. Mit nur 88 Seiten ist sie für ein gesamteuropäisches Regelwerk geradezu zierlich – aber sie wird stark zur Vereinheitlichung des geschäftlichen Umgangs mit Daten innerhalb der EU beitragen. Und das nicht nur für europäische Unternehmen – auch Unternehmen mit Sitz außerhalb der EU, ob Facebook oder Alibaba, müssen sich bei Angeboten, die sich an EU-Bürger wenden, an die Grundverordnung halten.

Gleichzeitig aber sollten Unternehmer im Hinterkopf behalten, dass Gesetze und Verordnungen in einer sich rapide wandelnden Wirtschaftswelt nur den ungefähren rechtlichen Rahmen liefern können. Vor allem aufgrund des rasanten technischen Fortschritts macht es schlicht wenig Sinn, bestimmte Instrumente oder Verfahren vorzuschreiben oder zu verbieten – zu groß ist die Gefahr, damit Gesetzeslücken zu schaffen. In vielen Fällen werden Standards für den richtigen Umgang mit Daten deshalb nicht vom Staat, sondern von den Unternehmen selbst geschaffen.

Datenschutz-Expertin Moser hält das Vorgehen, transparente Standards und Verfahren zum Umgang mit den Nutzerdaten zu etablieren, gerade dort für sinnvoll, wo es noch gar keine Regulierung gibt, da auf diese Weise „Aufsichtsbehörden ersehen können, was technisch möglich und realistisch umsetzbar ist". Beispiele hierfür seien Selbstverpflichtungen in der Werbeindustrie oder Online-Dashboards, über die Kunden erfahren können, welche Daten von ihnen gesammelt werden. Sie können dann selbst entscheiden, wofür sie die Nutzung erlauben wollen und wofür nicht.

Die Kommunikation mit den Kunden ist dabei für die Unternehmen mindestens ebenso wichtig wie die mit den Datenschützern oder Regulierern. Denn aktuell bestehe bei den Kundendaten laut Jana Moser „das größte Monetarisierungspotenzial": Daten wie Transaktionshistorie, Konsumentenverhalten, soziodemografische Merkmale wie Geschlecht, Ort und Alter können für die eigenen Geschäfte, aber auch für andere Unternehmen zählbare Vorteile bringen.

Bei der Verwertung von Daten kann man vieles falsch machen

Andererseits kann man aber gerade deshalb bei der Verwertung vieles falsch machen: Ein Kopfhörer-Hersteller beispielsweise hat sich kürzlich einen gewaltigen Shitstorm eingehandelt, weil er Nutzerprofile seiner Kunden erstellt hat – wer hört wann welche Musik? – und sich unklar darüber äußerte, ober er diese Profile an andere Unternehmen weiterverkauft hatte. Problematisch dabei war nicht so sehr, dass überhaupt Daten weitergegeben wurden: Jeder, der sich via Spotify oder andere Streaming-Dienste Musik auf die Ohren gibt, weiß ja eigentlich, dass irgendjemand etwas mit diesen Nutzungsdaten anfangen wird. Problematisch war eher, dass man das vom Kopfhörer-Produzenten nicht erwartet hatte.

„Die Akzeptanz ist vom Image des Unternehmens abhängig, vom Vertrauen, das ihm entgegengebracht wird“, weiß die Datenschutz-Expertin Jana Moser. An ein Start-up, das zum Beispiel die Sportaktivitäten seiner Nutzer dokumentiert und daher „vom Start weg“ auf das Erheben von Ortungs- oder Körperfunktionsdaten angewiesen ist, haben die Nutzer andere Erwartungen als an ein Traditionsunternehmen, das sein Geschäft erst digitalisiert und einen Ruf zu verlieren hat. Jana Moser empfiehlt Unternehmen, die sich an die Datennutzung heranmachen, daher eine schrittweise und transparente Vorgehensweise – mit Experimenten, „um Schritt für Schritt mit den Kunden zusammen herauszufinden, was sinnvoll und akzeptiert ist“.

Eine einfache Richtschnur für alle Fälle gebe es dabei aber nicht: „Bezüglich der Akzeptanz der Datennutzung durch die Kunden hängt viel davon ab, um welche Anwendung es gerade geht“, so Moser. „Bei einer App für Kommunikation unter Jugendlichen ist eine umfangreiche Nutzung von Kundendaten oft akzeptiert, manchmal sogar gewünscht.“ Das Gegenteil ist bei anderen Anwendungen der Fall, zum Beispiel beim Abgeben einer elektronischen Steuererklärung.

MERKLISTE

Welche Faktoren ziehen Hacker an?

Unternehmen fürchten den Datenklau, doch stehen nicht alle gleichermaßen im Fokus von Kriminellen. Hier finden Sie Kriterien, die ein Unternehmen für Hacker interessant machen könnten.

- Kennt man Sie? So sind zum Beispiel Firmen, die in den Medien präsent sind, ein attraktiveres Ziel als No-Names.
- Sind Ihre Daten wertvoll? Die Kundenliste eines Zulieferers für die Rüstungsindustrie dürfte spannender sein als die Buchführungsdaten eines Bäckers.
- Ist es technisch anspruchsvoll, in Ihr System einzubrechen? Dabei geht es vor allem um das Renommee, das man innerhalb der Hacker-Community durch einen Angriff erzielen kann.

Und das Risiko, Opfer eines Hackerangriffs zu werden? Ist, so Moser, für die meisten mittelständischen Unternehmen eher gering, weil sie kein attraktives Ziel sind: „Wenn Sie für Hacker nicht interessant sind, sind Sie deswegen zwar nicht sicher – aber die Angriffs-Wahrscheinlichkeit ist kleiner.“

In diesem einen Fall scheint es also von Vorteil zu sein, wenn das eigene Unternehmen nicht so im medialen Rampenlicht steht wie die größere, möglicherweise börsennotierte Konkurrenz. Der Begriff „Hidden Champion“ jedenfalls erhält vor diesem Hintergrund eine weitere positive Konnotation.