Vom Wert der Daten – was viele verschenken wird teuer weiterverkauft

Zusammenfassung: Kaum ein Unternehmen kennt den Wert seiner Daten, entsprechend gering ist die Bereitschaft, wirksame Maßnahmen gegen Datendiebstahl zu ergreifen. Wenn Mitarbeiter schon ihre eigenen Daten verschenken, wie gehen sie dann erst mit den Unternehmensdaten um? Datendiebstahl kann die Existenz des Unternehmens kosten. Entsprechend sollten alle Unternehmen ihre bestehenden Maßnahmen gegen Datendiebstahl überprüfen und bei Bedarf an die verschärften Gefährdungen anpassen.

Der Praxisfall: Der Geschäftsführer eines mittelständischen Unternehmens erhält einen seltsamen Anruf. Ihm werden Daten von potenziellen Kunden für sein Unternehmen angeboten. Der Anrufer weiß überraschend gut über das Unternehmen Bescheid. So lässt sich der Geschäftsführer auf eine kostenfreie Testbestellung eines Auszugs aus der Liste ein. Die Überraschung: Auf der Liste stehen ausnahmslos tatsächliche Kunden des Unternehmens. Und zwar mit Merkmalen, die so eindeutig vom Unternehmen eingetragen wurden, dass es sich nur um zumindest Auszüge aus dem eigenen CRM handeln kann. Die komplette Liste hätte knapp über 40.000 Euro kosten sollen. Der Geschäftsführer erstattet sofort Anzeige wegen Datendiebstahls. Einige Wochen später erhält er die Mitteilung der Staatsanwaltschaft, dass das Verfahren wegen mangelnder Aussicht auf Aufklärung eingestellt wird. Was bleibt, ist das mehr als ungute Gefühl, dass offenbar irgendjemand eine Kopie seiner CRM-Daten hat und diese für teures Geld an den Mann zu bringen versucht. Bleibt die Frage: Welchen Wert haben eigentlich personenbezogene Daten?

Verschenkte Daten: Im privaten Bereich hat es sich langsam herumgesprochen. Wer Apps nutzt, dazu noch kostenfreie, bezahlt mit seinen Daten. Je nach Anforderung der App-Betreiber stehen in den Allgemeinen Geschäftsbedingungen sowie den Datenschutzbestimmungen mehr oder weniger Datenkategorien, für deren Nutzung durch den App-Betreiber der Anwender seine Zustimmung geben muss, wenn er die App laden und nutzen möchte.

Gestohlene Daten: In unserem Fall muss das etwas anderes gewesen sein. Sollten die zum Kauf angebotenen Daten tatsächlich aus dem eigenen Unternehmen stammen, muss irgendwo ein Datendiebstahl geschehen sein. Wenn der Geschäftsführer Glück hat, lässt sich aufgrund der Logfiles wenigstens ermitteln, wann und von welchem Rechner aus die Daten abgezogen wurden. Wenn der Täter oder Angreifer jedoch clever genug ist, sind die Spuren, die zu seiner Entdeckung führen könnten, sorgfältig verwischt worden.

Warum Diebe Daten stehlen: Über mögliche Gründe kann nur spekuliert werden. Es kann sein, dass der Dieb dem Unternehmen Schaden zufügen wollte. Es kann genauso gut sein, dass der Täter sich bereichern wollte. Es kann sein, dass die Daten ohne das Zutun eines Mitarbeiters gestohlen wurden, vor allem dann, wenn die Sicherheitseinrichtungen nicht gut genug sind oder umgangen wurden. Einer der wichtigsten Gründe dürfte aber darin liegen, dass es in den meisten Fällen zu einfach ist, Daten zu stehlen und dass Datendiebstahl nur in sehr wenigen Fällen aufgeklärt wird, mithin ist das Risiko der Täter erwischt zu werden eher gering.

Über den Neid: Es gibt einen sehr interessanten Versuchsaufbau, der in der Soziologie in den letzten Jahren in den unterschiedlichsten Formen zu immer demselben Ergebnis führt und der tiefe Einblicke in Neid und Missgunst zulässt. Ein Proband erhält 100 Euro geschenkt, unter einer einzigen Bedingung. Er muss jemanden finden, mit dem er das Geld teilt und dieser muss mit der Teilung einverstanden sein. Stellen Sie sich vor, jemand bietet Ihnen 15 Euro ohne Bedingungen an und erzählt Ihnen genau diesen Sachverhalt. Würden Sie die 15 Euro annehmen? Interessant ist das Ergebnis des Versuchs. Mehr als 4 von 5 Probanden gelingt es nicht, jemand anderes dazu zu überreden, das Geld anzunehmen. Fragt man die Zweitbeschenkten hinterher, warum sie der Teilung nicht zugestimmt haben, obwohl doch beide davon profitierten? Und die meisten gaben an, sie seien nicht damit einverstanden gewesen, dass der andere so viel behalten darf und sie nur so wenig bekommen sollten. Dann soll auch der andere nichts bekommen.

Verstand setzt aus: Das Ergebnis lässt sich quer durch alle Versuchsanordnungen immer wieder so messen. Erst ab einer Aufteilung, die in etwa halbe - halbe beträgt, sind die Zweitbeschenkten bereit, dem Erstbeschenkten seinen Anteil zu gönnen und zu ermöglichen. Und das, obwohl auch der Zweitbeschenkte etwas bekommen sollte, was er vorher nicht hatte! Tatsächlich scheint das Gefühl, einem anderen, Geizigen, eins ausgewischt zu haben, ihm also seinen Gewinn verhindert zu haben, wichtiger

zu sein als es der eigene direkte Nutzen ist. Warum das so ist, darüber rätselt die Wissenschaft. Allerdings scheint genau diese Verhaltensweise beim Umgang mit Daten komplett ausgehebelt.

App-Nutzung für teure Daten: Wer eine App nutzen möchte, muss in aller Regel dafür mit seinen Daten bezahlen. Wer wissen möchte, wie teuer derartige Daten gehandelt werden, der muss nur auf die Internetseite eines Datenhändlers gehen und sich dort ein Angebot für eine bestimmte Anzahl von Adressen gegen zu lassen. Je spezifischer die Daten sind, desto teurer sind sie auch. Würde das oben geschilderte Ergebnis der Experimente auch hier zutreffen, müssten sich 85% der Anwender von Messenger-Apps oder anderen Anwendungen dagegen sträuben, ihre Daten dem App-Betreiber kostenfrei zu überlassen. Ohne selbst Neid wecken zu wollen, aber Mark Zuckerberg, der Gründer und Inhaber von Facebook, wurde damit zum jüngsten Milliardär aller Zeiten und ist aktuell der drittreichste Mensch auf Erden. Es ist nur eine Frage der Zeit, bis er die beiden noch vor ihm liegenden übertrumpft. Hier versagt der Neidreflex komplett. Sonst würden von den derzeitigen 2 Mrd. Facebook-Nutzer 1,7 Mrd. die Datenweitergabe abgelehnt haben, weil sie im Vergleich zum Betreiber der App mit der Nutzungserlaubnis viel zu billig abgespeist wurden.

Daten sind oft das wertvollste, was ein Unternehmen hat: In vielen Fällen sind Daten das wertvollste, über das ein Unternehmen verfügt. Das Geld eines Unternehmens wird im Tresor aufbewahrt, die Daten liegen teilweise offen auf den genutzten Geräten. Mehr als die Hälfte der Unternehmen haben so gut wie keine Sicherheitsvorkehrungen ergriffen, um ihre Daten vor unbefugter Mitnahme durch Beschäftigte zu schützen. Die wenigsten sind in der Lage, einen Datentransfer vom Rechner auf einen USB-Stick nachzuvollziehen.

Der Gesetzgeber sieht das anders als etliche Unternehmen: Auf europäischer Ebene wurde die EU-DAGVO erlassen und 2016 in Kraft gesetzt. Wegen der zweijährigen Übergangsfrist gilt sie ab dem 25. Mai 2018 EU-weit ohne weitere Übergangsfristen. Dort gibt es die Anordnung der Data Breach Notification, einer Pflicht zur Information der zuständigen Aufsichtsbehörde für den Datenschutz, wenn personenbezogene Daten aus dem Unternehmen abfließen. Diese Informationspflicht, eben die Data Breach Notification, muss grundsätzlich binnen 72 Stunden erfolgen. Geschieht dies nicht, droht dem Unternehmen eine hohe Geldbuße, die im Extremfall bis zu 4% des weltweiten Jahresumsatzes betragen kann.

Wie genau nehmen es die Mitarbeiter? Wenn schon im privaten Bereich Daten scheinbar keinen Wert haben und einfach so verschenkt werden, stellt sich die spannende Frage, wie die Beschäftigten es dann mit den Unternehmensdaten halten. Wer sich mit dieser Frage näher beschäftigt, wird Erschreckendes zu Tage fördern. Das Gefährdungsbewusstsein ist bei den Beschäftigten nämlich ohne weitere Maßnahmen eher gering ausgeprägt. Die wenigsten Beschäftigten können sich vorstellen, selbst zum Angriffsziel eines Datendiebes zu werden. Entsprechend unbedarft gehen sie mit geschäftlichen Daten um – eben wie mit ihren privaten Daten auch. Dies gilt erst recht, wenn die Mitarbeiter geschäftliche Smartphones erhalten und sie sich private Apps zu Nutzung selbst aufspielen dürfen.

Regelungen zur Compliance unverzichtbar: Unternehmen sind gut beraten, wenn sie dieses Thema sehr ernst nehmen. Neben zusätzlichen Sicherheitsmaßnahmen müssen klare Regeln zum Umgang mit Geräten und Daten her. Diese müssen in Schulungen auch den Beschäftigen vermittelt werden.

Kontrollen erforderlich: Alle Regeln, die vereinbart wurden, müssen auch kontrolliert werden. Schließlich trägt das Unternehmen eine hohe Verantwortung für Kunden- und Beschäftigtendaten. Nur einen Datenschutzbeauftragten zu bestellen, reicht bei weitem nicht aus. Sicherheitsanalysen müssen vorgenommen werden und die daraus abgeleiteten Maßnahmen müssen umgesetzt und kontrolliert werden.

Bewusstsein schärfen: Besonders wichtig ist es jedoch, bei den Beschäftigten das Bewusstsein für Gefährdungen zu wecken und zu schärfen. Gerade weil die Beschäftigten in der Regel nicht mitgekommen, welche Angriffsversuche auf das Unternehmen und seine Daten vorgenommen werden, sollten sie ab und an darüber informiert werden. Sonst könnten sie denken, dass keine Gefahr besteht oder niemand Interesse an den Daten des Unternehmens hat.

Gefahr erkennen und Maßnahmen ergreifen: Das wichtigste ist jedoch, dass Unternehmen erkennen, wie wertvoll ihre Daten tatsächlich sind und welch große Begehrlichkeiten dieser Wert wecken kann. Ist man sich dieser Gefahr erst einmal bewusst geworden, ist der nächste Schritt hin zu wirksamen Maßnahmen nicht mehr ganz so groß. Aber spätestens zum 25. Mai 2018 sollten konkrete Schritte unternommen werden. Ab diesem Datum sind die drohenden Bußgelder so hoch, dass alle Unternehmen aktiv werden müssen.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de.