

Daten und ihr Missbrauch

Dr. Ulrich Bellmann

Das Wissen über die Gefahren der Datenverarbeitung, sowohl in Unternehmen, als auch in staatlichen und anderen privaten Organisationen, hängt in hohem Maße vom Zeitpunkt der Ausbildung ab. Betrachtet man die oberste Führungsebene von großen Unternehmen oder Regierungen europäischer Staaten, so stellt man fest, dass in der Regel die heute über 45-jährigen Menschen noch keine umfangreiche Erfahrungen während ihrer Ausbildung mit komplexen Strukturen der digitalen Welt machen konnten.

Weder Lehrpläne, Studienpläne noch die Erfahrung der Lehrer und Hochschullehrer ließen vor über 20 Jahren erahnen, welche Bedeutung die Computertechnik und alle damit verbundenen Risiken erlangen würden. Um dieses Defizit abzubauen, geht es bei der Beratung von Führungskräften nicht vorrangig darum, diesen nachträglich entsprechende Detailkenntnisse zu vermitteln, sondern es geht um die Herstellung eines umfassenden Verständnisses der technischen, juristischen und gesellschaftlichen Risiken beim Umgang mit Daten. Hierzu gehört auch die Vermittlung einer selbstkritischen Einschätzung der eigenen Fähigkeiten. Zur Lösung von Aufgaben im Bereich der Datentechnik müssen sich alle Verantwortlichen in Unternehmen und der Gesellschaft Hilfe von außen bedienen, wobei die Entscheidungsgrundlagen für Unternehmensregeln oder Gesetze öffentlich diskutiert werden müssen. Nicht das fehlende Wissen der Entscheider ist das Problem, sondern die Tatsache, dass sich die Entscheider nicht eingestehen, dass eine eigene Wissenslücke besteht.

Der Grund für die Diskrepanz zwischen der realen Datenwelt und dem Weltbild der Entscheidungsträger ist die rasante Entwicklung der Datentechnik in den letzten 30 Jahren. Solche Phänomene der verzögerten Wissenswahrnehmung und -akzeptanz gab es in der Geschichte schon häufig. Die Keplerschen Erkenntnisse brauchten über 250 Jahre, um in den Geist der Gesellschaft Einzug zu halten. In einigen, sogar westlichen Kulturkreisen, sind bis heute die Lehren Darwins für gewisse Menschen nicht nachvollziehbar. Während man bei den beiden letzten Phänomenen religions- und übergeordnete machtpolitische Interessen erkennen kann, verhält es sich beim Wissensdefizit im Datenverarbeitungsbereich anders. Daher kann ein einfacher Aufruf, was vorrangig geschehen sollte, Abhilfe schaffen, damit der Stellenwert der Datensicherheit richtig erkannt wird.

Die Rolle des Datenschutzbeauftragten, den es in vielen Unternehmen gibt, sollte überdacht werden. Der Datenschutzbeauftragte kann durch einen CSO (Chief Security Officer) ersetzt werden, der ausschließlich dem Firmenchef oder dem Aufsichtsrat untersteht. Er muss eigenständiges Mitglied der Geschäftsführung sein. Eine maßvoll definierte, aber stringente parallele Hierarchie, die Datensicherheit fordert und überprüft, gibt es heute in kaum einem Unternehmen, sie muss aber sein. Das Vieraugenprinzip bei inneren und äußeren kaufmännischen Prozessen ist nahezu selbstverständlich - bei der Datensicherheit ist es weitgehend unbekannt. Das Prinzip muss aber auch hier eingeführt werden.

Im Deutschen Bundestag erscheint der Datenschutzbeauftragte wie ein „Rufer in der Wüste“, wenn er, für den juristischen Laien bereits vorab erkennbar, zu Recht schwerste Missstände im Umgang mit Personendaten bei der Gesetzgebung anprangert. Hier sollte es ein Ministerium für Datensicherheit inklusive der entsprechenden untergeordneten Organe geben, das unmittelbar an der Gesetzgebung mitwirkt und die Grundrechte der Menschen verteidigt.

Das Grundrecht auf „Informationelle Selbstbestimmung“ ist erst über den Umweg der Rechtsprechung durch das Bundesverfassungsgericht zum Leben erweckt worden, nicht durch ein nominelles und in der Verfassung schriftlich erfasstes und parlamentarisch definiertes Grundrecht.

So ist es heute ein reiner Zufall, dass Mautdaten in Deutschland nicht zur Aufklärung von Straftaten benutzt werden dürfen. Es gibt keine allgemeinverbindlichen Grundsätze bezüglich der Verwertung von Daten, weder im Staat, noch in Unternehmen.

Wenn Regeln fehlen, wird das entstehende Defizit an Strukturen jedoch durch wenig oder nicht nachvollziehbare Prozesse ersetzt. Es bilden sich daher in Unternehmen parallele Interessen, die nicht mehr auf ein gemeinsames Ziel, nämlich den Unternehmensgewinn, abzielen, sondern nur als Selbstzweck dienen. Die EDV-Abteilung oder der gesamte IT-Bereich ist nicht mehr interner Dienstleister, sondern setzt eigene Regeln durch, denen der Bedarfsträger gar nicht zugestimmt hat.

Anstatt klare Regeln des Umgangs mit Daten zum Wohle des Unternehmens zu definieren, ordnen sich Unternehmensführer den Bedürfnissen der Datentechnik gelegentlich regelrecht unter. Als emotionaler Befreiungsschlag ist es zu werten, dass Unternehmer zunehmend dazu übergehen, ihre Datentechnik sogar „outzusourcen“. „Outsourcing“ von EDV verspricht zunächst Kosteneinsparung, Transparenz, Problembewältigung (Verlagerung der Verantwortung), Effizienzsteigerung und Sicherheit. Besonders problematisch wird die Maßnahme, wenn Unternehmen, deren Kernkompetenz sogar im Bereich der Datenverarbeitung liegt, zu solchen Mitteln greifen. Tatsächlich findet im Bereich der Telekommunikation, insbesondere des Mobilfunks, in Europa eine zunehmende Überlassung von Kundendaten an Dritte statt.

Wenn man diese Maßnahme des „Outsourcing“ mit klaren Regeln vollzieht, kann tatsächlich ein Gewinn entstehen. Meist hat die Maßnahme aber ein Übermaß an zusätzlichen Schnittstellen, Schnittstellenverwaltung und Unklarheiten zur Folge, die zu einem dramatischen Verlust der Kontrolle über die ausgetauschten Daten führt. Der Schaden, der dem Unternehmen durch den Diebstahl von Daten entsteht, ist manchmal so groß, dass er durch eine Haftungsregelung mit dem Partner gar nicht ausgeglichen werden kann.

Unternehmen zahlen oft einen hohen Preis, den die öffentlich bekannt gewordenen Datenskandale der letzten Jahre nur erahnen lassen. Abhilfe schafft nur eine gründliche Analyse der Bedürfnisse des Unternehmens. Die einfache Frage nach den Kernkompetenzen des Unternehmens hilft weiter. Darüber hinaus ist die abgestimmte Beschränkung des Zugangs verschiedener Menschen auf bestimmte Daten sinnvoll. In vielen Unternehmen haben zum Teil Hilfskräfte aus dem EDV-Bereich Zugriff auf sämtliche Personaldaten, da es keine Instanzen gibt, die deren Zugriffsrecht beurteilen und überwachen können. Auch die Frage an Mitarbeiter, was sie denn von dem riesigen EDV-Angebot im Unternehmen wirklich brauchen, hilft weiter, mit erstaunlichem Einsparpotential.

Auch das Sprechen einer gemeinsamen Sprache der Mitarbeiter im Unternehmen, bezüglich Datensicherheit, schafft Vertrauen und Bewusstsein für Schwachstellen. So hat sich in der Vergangenheit bei Nachuntersuchungen von „Datenlecks“ herausgestellt, dass Teile der Belegschaft die Schwachstellen genau kannten, aber keine Prozesse im Unternehmen angestoßen werden konnten, die systematisch eine Schließung der Lücken hätten bewirken können.

Fazit: Wissensbündelung, interne Kommunikation und Schaffung von Problembewusstsein bei allen Beteiligten setzen Anreize zur Schließung von Datenlöchern. Nach einer Verlautbarung des Bundeskriminalamtes vom Juni 2010, sind europäische Unternehmen massiven Angriffen durch Industriespionage, vor allem aus Asien und Amerika, ausgesetzt.

„Cloud-Computing“ als neuer Slogan verspricht hier Abhilfe. Die Daten sind sicher, da sie über die ganze Welt verteilt sind. Die große Datenwolke, auch wenn sie uns das Blaue vom Himmel verspricht, ist alleine sicher keine Lösung.

Sicherheit hat ihren Preis; keine zu haben, kommt aber mit Sicherheit noch teurer zu stehen.

29. Juni 2010, Dr. Ulrich Bellmann