Eine Reihe von Skandalen brachte uns im letzten Jahr das Thema Datenmissbrauch schlagartig ins Bewusstsein. Laut jüngster Studie der Arbeiterkammer Oberösterreich fühlt sich mehr als ein Viertel aller Arbeitnehmer überwacht. Erleben wir nach der Finanzkrise jetzt eine Daten(schutz)krise? Und was könnte die Rolle der CIOs dabei sein? Wenn einer Bescheid weiß, ist es der Datenschutzspezialist **RAINER KNYRIM.**

„EIN CIO MUSS ERKENNEN, *wo es Handlungsbedarf gibt"*

VON TINA PAIRITS

Herr Dr. Knyrim, sind wir schon in der Datenkrise? Gibt es auch in Sachen Datenschutz, genauso wie beim Thema Investment, immer mehr Unternehmen, die sich nicht an Gesetze halten?

Grundsätzlich muss man feststellen, dass es in den meisten Fällen keine böse Absicht der Unternehmen ist, wenn es zum Verstoß gegen das Datenschutzgesetz kommt. Sie machen sich einfach keine Gedanken darüber. Das liegt auch daran, dass die technologische Entwicklung sehr rasch voranschreitet – immer mehr elektronische Systeme bestimmen unseren Alltag – da ist die Nutzung dieser Systeme ganz selbstverständlich. Es ist sehr schwierig, damit rechtlich Schritt zu halten.
Durch die größere Dichte an Skandalen fühlen sich die Leute unbehaglich und reagieren sensibler auf das Thema Datenschutz, die Mitarbeiter und vor allem auch die Betriebsräte. >

Eine Buchempfehlung dazu finden Sie auf Seite 91.

Drohen die CIOs immer mehr zur Unternehmenspolizei zu werden?

Es stimmt, dass die CIOs beim Thema Datenschutz Gefahr laufen, immer stärker in die Rolle als Gegenspieler des Betriebsrates zu geraten. Die Betriebsräte haben sich mit diesem Bereich schon intensiver befasst und im Moment einen Wissensvorsprung. Es gibt genügend Möglichkeiten, wie man sogar große Konzerne „über die Datenschutz-Karte leicht aufmachen kann."
Ein Beispiel: In einem Konzern mit 5.000 Mitarbeitern wollte die Geschäftsführung die Signaturen von allen Mitarbeitern einscannen. Der Betriebsrat hat nach dem Grund gefragt und die Antwort war: „Wenn ein Mitarbeiter Prokurist wird, haben wir seine Unterschrift dann schon." Daraufhin hat der Betriebsrat nachgerechnet, wie hoch der Anteil der Prokuristen unter den Mitarbeitern denn ist. Das Ergebnis waren 4%. Und dafür sollten alle Mitarbeiter ihre Signatur einscannen lassen? Ganz offensichtlich hat sich kein Mensch in der Geschäftsleitung vorher eine datenschutzrechtlich zulässige Begründung überlegt. Das ist sehr repräsentativ und zeigt, dass die meisten Unternehmen ziemlich blauäugig und unwissend an die Sache herangehen. Bei dem konkreten Beispiel hat der Betriebsrat noch nie eine so einfache Besprechung gehabt – seitdem ist das Thema vom Tisch.
Weil viele Firmen auf eine solche Weise angreifbar sind, wird das Thema Datenschutz firmenintern auch zunehmend zu einem politischen Instrument. Es gibt gerade bei den Themen E-Mail und Internet Konfliktpotenzial zwischen Geschäftsführung und Betriebsrat – der CIO gerät dann häufig auch ins Spannungsfeld. Ob er sich in die Rolle eines Unternehmenspolizisten drängen lässt, liegt jedoch bei ihm. Wenn der Geschäftsführer zu ihm sagt: „Schauen Sie sich die Mails an", muss der CIO nicht mitspielen.

Drohen den CIOs in solchen Fällen rechtliche Konsequenzen?

Es hat Fälle gegeben, etwa bei internen Revisionen, wo Einsicht in E-Mails genommen wurde, und alle Beteiligten dann im Nachhinein wegen illegaler Datenbeschaffung angezeigt wurden. In solch einem Fall hat also auch der IT-Verantwortliche, der die Daten beschafft, unter Umständen strafrechtliche Konsequenzen zu befürchten. Das ist aber eine Ausnahme. In erster Linie betrifft die Haftung die Geschäftsführung, direkte rechtliche Konsequenzen drohen den CIOs nur in „schweren" Fällen. Es ist vor allem ein internes Problem – gerät die Geschäftsführung unter Druck, gibt sie den häufig an den CIO weiter. Wenn etwa der Chef der Deutschen Bahn wegen Verfehlungen gegen das Datenschutzgesetz seinen Hut nehmen muss, hat vermutlich auch der CIO keine leichte Zeit gehabt.

Gerade die Themen, die CIOs betreffen, wie E-Mail und Internet, sind rechtlich nicht immer ganz klar.

Das Thema private E-Mail- und Internetnutzung ist sogar eine extreme Grauzone – es fehlen die rechtlichen Grundlagen. Gerade deshalb muss ich aber als Unternehmen aktiv werden und Policies aufsetzen und als CIO in eigenem Interesse darauf drängen. Am besten ist es, möglichst klare Richtlinien zu schaffen – etwa, außer im Notfall, private Mails nur mit Webmail, aber nicht über den Firmen-Account zuzulassen. Und sich private Mails auch nicht an den Firmen-Account senden zu lassen.
Nur wenige Unternehmen haben solche Policies und nur die allerwenigsten gute und konsequent durchdachte. Wie weit man hier proaktiv und im Einzelfall aber tatsächlich gehen kann, das ist von der Gesetzgebung her sehr unklar. Es macht auf jeden Fall Sinn und ist gesetzlich auch verpflichtend, eine Betriebsvereinbarung aufzusetzen, dass Mails im Bedarfsfall kontrolliert werden können.

Wenn schon für Juristen Grauzonen bestehen, welche Chance haben dann die CIOs, sich zurecht zu finden?

Natürlich ist ein CIO kein Jurist, aber er muss mögliche Probleme und Handlungsbedarf identifizieren können und an die Rechtsabteilung weitermelden. Das ist ja auch durchaus etwas, womit sich ein CIO positionieren kann, indem er als Projektleiter Aufgaben an die Unternehmens-Juristen oder die HR-Abteilung delegiert. Da besteht noch sehr viel Entwicklungspotenzial. Beispielsweise könnte man sich durchaus vorstellen, dass zukünftig im Rahmen eines Notfallplanes für Fälle von Datenmissbrauch – hier gibt es seit 1. Jänner 2010 eine neue Informationspflicht – der CIO der Richtige ist, der nach außen hin dazu etwas sagt und nicht unbedingt die PR-Abteilung. Wer wäre denn sonst kompetenter dafür als der Chief Information Officer?

DR. RAINER KNYRIM

.... absolvierte nach seinem Studium in Graz, Wien und Paris ein Verwaltungspraktikum bei der Europäischen Kommission in der GD Wettbewerb. Nach seiner Tätigkeit für die IT-Abteilung von Faegre Benson Hobson Audley Rechtsanwälte in London sowie als Juniorpartner bei Schönherr Rechtsanwälte, wurde er 2003 Partner bei Preslmayr Rechtsanwälte in Wien. Er ist Experte für die Themen Datenschutz und IT-Recht. Rainer Knyrim ist Mitglied der Task Force Privacy der International Chamber of Commerce, Paris, Beirat der Zeitschrift „jusIT" und des österreichischen IT-Rechtstages. Er ist Autor eines der heimischen Standardwerke in Sachen Datenschutz, des „Praxishandbuchs Datenschutzrecht" sowie Mitherausgeber des größten österreichischen Datenschutz-Kommentars Dohr/Pollirer/Weiss/Knyrim.

Ist das Thema Überwachung, beispielsweise durch Videokameras, eine Herausforderung, die auf CIOs zukommt?

Die plakativen Themen wie Videoüberwachung oder Fingerprints sehe ich nicht als so „heiß". Spitzelei ist in Österreich trotz allem kein großes Thema. Wenn etwa Diebstähle im Lager passieren, dann ist Unternehmen eher davon abzuraten, selber mit Videoüberwachung zu beginnen, sondern damit zur Polizei zu gehen. Oft sind das auch stumpfe Waffen – ich kenne Fälle, wo man Überwachungskameras installiert hat, und dann sieht man auf den Videos die Täter mit Strumpfmasken oder nur von hinten. Das Thema ist nach dem Diebstahl der Saliera einfach etwas in Mode gekommen.
Fakt ist: Für eine Überwachung per Videokamera sind eine Betriebsvereinbarung und eine Genehmigung der Datenschutzkommission notwendig. Traurig ist, dass die Dunkelziffer eine sehr hohe ist. Den jährlich 250.000 verkauften Videokameras, die man auch für solche Zwecke einsetzen kann, stehen vielleicht 1.000 Anträge zur Videoüberwachung bei der Datenschutzkommission gegenüber. Der Genehmigungsaufwand ist nicht so hoch, dass man sich als CIO die Blöße geben sollte, keine Genehmigung einzuholen und dann von der Belegschaft, dem Betriebsrat oder den Medien als Gesetzesbrecher hingestellt zu werden.
Wenn man solch einen Antrag stellt, muss man die eingesetzten Mittel gegenüber der Datenschutzkommission allerdings argumentieren. Ich kenne ein Beispiel, wo ein Unternehmen die Zeiterfassung mit Fingerprints einführen wollte und dies extrem technisch begründet hat – das ging bis zur Widerstandsfähigkeit der Geräte. Der Betriebsrat klagte dagegen bis zum Obersten Gerichtshof hinauf. Dieser ist zu dem Schluss gekommen, dass dabei die Interessen der Mitarbeiter nicht ausreichend berücksichtigt wurden.

Wo sehen Sie dann die künftig heißen Themen?

Die sind im Alltag eines Unternehmens, in den gängigen Arbeitssituationen zu finden, in denen elektronische Tools zum Einsatz kommen und keiner mehr darüber nachdenkt.
Es gibt zum Beispiel immer wieder den Fall, dass Mitarbeiterdaten innerhalb eines Konzerns in die Zentrale, etwa in die USA, transferiert werden und dass es dann heißt „Die werden dort doch nur gespeichert." Das sind jedoch Daten, die unter Umständen für Performance- und Gehaltsvergleiche, Vorschläge für Mitarbeiterabbau oder im Fall von Fusionen sogar für Prescreenings herangezogen werden können.
Elektronische Mitarbeitergespräche in Konzernen sind ein ähnlicher Fall. Es ist legitim, dass ein Konzern einen Überblick über seine Talente haben und internationale Karrieren forcieren möchte. Dann gibt es aber immer wieder den klassischen Fall, wo ein Mitarbeiter in Österreich in der elektronischen Befragung angibt, dass er nicht ins Ausland wechseln möchte, weil er hier seine Familie und schulpflichtige Kinder hat. Nach dem zweiten Mal erhält er aus der Firmenzentrale in den USA den Vorwurf, dass er sich nicht weiterentwickeln will. Das ist eine Nutzung der Daten zum klaren Nachteil des betreffenden Mitarbeiters.
Ein Thema, das im Arbeitsalltag immer mehr integriert wird, sind Presence Tools. Natürlich ist es hilfreich, wenn ich sehe, ob der Kollege gerade in einem Meeting ist. Wenn ich damit aber auswerten kann, wie viel ein Mitarbeiter arbeitet oder wie viele Pausen er macht, dann wird es sehr problematisch. Auch dafür wäre eine Betriebsvereinbarung notwendig.
Themen, die auch immer stärker aufkommen, sind Standortüberwachung mit GPS oder RFID oder auch spezifische Dinge wie Fahrzeugdatenauswertung. Die Fuhrparks kaufen verstärkt eine neue Generation von LKWs, bei denen bis zu 60 Zustandsdaten permanent ausgewertet werden können – Geschwindigkeit, Betriebstemperatur, Spritverbrauch, in welchem Gang gefahren und ob zu stark beschleunigt wird. Wenn ich diese Daten, die noch dazu oft auf Servern in den USA liegen, mit dem Dienstplan der Fahrer kombiniere, habe ich gleich ein ganzes Paket von Datenschutzproblemen. □

Die private Nutzung von E-Mail und Internet ist eine extreme Grauzone. Gerade deshalb muss ich als Unternehmen klare Policies schaffen und als CIO darauf drängen.

Rainer Knyrim,
Datenschutzspezialist
bei Preslmayr
Rechtsanwälte OG