IT-SECURITY

Überwachung: Gläserne Mitarbeiter?

Eine wirksame Überwachung muss nicht zwangsläufig die Persönlichkeitsrechte der Mitarbeiter verletzen. So kann der Konflikt entschärft werden.

Überwachung kann bei Mitarbeitern schnell Unbehagen auslösen. Spontan kommen einem Begriffe wie Spionieren, Aushorchen oder Misstrauen in den Sinn. Bei der Überwachung geht es dem Arbeitgeber jedoch um andere Dinge: Abläufe sichern, Qualitätsmanagement, Betriebssicherheit, Prävention und Aufklärung von Straftaten.

Die Rechtslage

Die Möglichkeiten des Arbeitgebers sind jedoch begrenzt. Aus rechtlicher Sicht hat der Arbeitgeber die Pflicht, die Persönlichkeit des Arbeitnehmers zu achten und zu schützen (Art. 328 OR). So darf er Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind (Art. 328b OR). Zudem muss der Arbeitgeber die datenschutzrechtlichen Grundsätze beachten: Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckgebundenheit und Richtigkeit der Daten. Rechtmässigkeit bedeutet, die Daten dürfen nicht in Verletzung gesetzlicher Bestimmungen erhoben und bearbeitet werden. Treu und Glauben ist gegeben, wenn die Datenbearbeitung für den Angestellten erkennbar ist. Er muss aus den Umständen darauf schliessen können oder vorgängig aufgeklärt worden sein. Verhältnismässigkeit besagt, dass so viele Daten wie nötig, jedoch so wenig wie möglich bearbeitet werden dürfen.

Zweckgebunden ist die Datenbearbeitung, wenn sie nur zu dem Zweck erfolgt, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgeschrieben ist. Richtigkeit der Daten bedeutet, dass die Informationen inhaltlich korrekt sein müssen. Hält sich der Arbeitgeber nicht an diese Grundsätze und gibt es dafür keinen Rechtfertigungsgrund (z.B. Einwilligung), begeht er eine Persönlichkeitsverletzung.

So klar und einfach die Gesetze lauten, so komplex sieht die Realität aus. Die heutigen technischen Überwachungsmöglichkeiten sind so vielschichtig wie noch nie. Längst muss nicht mehr bloss in die Kamera gelächelt werden. Gerade am Arbeitsplatz bieten sich unzählige Möglichkeiten, die Angestellten zu überwachen: Internet- und E-Mail-Protokolle, Telefonverbindungsdaten, Standort des Mobiltelefons, Zeiterfassungssystem, Drucker- und Faxdaten, Zugriffsprotokollierungen auf Datenbanken usw. Überall hinterlassen Mitarbeiter elektronische Spuren. Und der Appetit kommt beim Essen: Ist die Möglichkeit einmal da, lockt die Versuchung, Informationen zu sammeln, zu sichten, auszuwerten oder zu missbrauchen.

Transparenz & Information

Es gilt die Balance zwischen Arbeitgeberinteressen und dem Persönlichkeitsschutz des Arbeitnehmers zu finden. Dabei kann nicht oft genug betont werden, dass eine angemessene Information und regelmässige Schulung aller Mitarbeitenden im Umgang mit Geschäfts- und Personendaten sowie den IT-Arbeitsmitteln von essentieller Bedeutung sind. Klare Regelungen über die Unternehmensziele, das Er-/Unerlaubte, die Ausgestaltung der Überwachung und Kontrolle, die Zuständigkeiten und die Konsequenzen. Die Angestellten dürfen auch jederzeit Auskunft über die Bearbeitung ihrer Daten verlangen und der Arbeitgeber muss die Angestellten über die Beschaffung besonders schützenswerter Personendaten informieren.

«Überwachung – ja, aber nur mit klaren Spielregeln!»

Die Verabschiedung, Kommunikation und Anpassungen der Regeln sind Aufgabe des Managements. Aus technischer Sicht sollte der Arbeitgeber auf präventive Massnahmen setzen wie Passwort- und Zugriffsschutz, Antivirenprogramme, Sperrung unerwünschter Internetangebote, Backup, Firewall usw.

Ist der Mitarbeiter informiert, können die vereinbarten Regeln auch durchgesetzt werden. Wenn gegen diese Regeln oder gesetzlichen Vorschriften verstossen wird, darf der Arbeitgeber die vorher festgelegten Konsequenzen ziehen (disziplinarische Strafen bis zur Entlassung).

Eine klare Informationspolitik und Schulung der Mitarbeiter braucht Zeit und Geduld. Doch langfristig lohnt sich die Investition. Statt Misstrauen und Unsicherheit wird gegenseitiges Verständnis, Akzeptanz und im besten Fall sogar Mithilfe beim Aufdecken von Sicherheitslücken gefördert. ■

DIE AUTORIN

Liliane Mollet ist Beraterin für IT-Security und IT-Recht bei der conpro Consulting AG in Bern
www.conpro.ch

Mehr zur IT-Security:
www.computerworld.ch