

Mitarbeiterkontrolle

Big Brother Inc.

Faule Mitarbeiter aussortieren, Industriespionage aufdecken, Klagen vermeiden: Warum Unternehmen ihre Angestellten immer stärker überwachen. Was technisch möglich und rechtlich erlaubt ist.

Queen of the Sky – unter diesen Namen ist Ellen Simonetti im Internet bekannt. Seit Anfang 2004 breitet die Stewardess der US-Fluggesellschaft Delta Air Lines ihre Gedanken, Gefühle und Erlebnisse in ihrem Weblog aus. Für die Flugbegleiterin war das Schreiben Therapie, um über den Krebstod ihrer Mutter hinwegzukommen. Für ihren Arbeitgeber ist es ein Kündigungsgrund – weil Simonetti auf einigen Fotos in ihrem Web-Tagebuch in Uniform zu sehen ist. „Ich will meinen Job zurück“, sagt die Stewardess, die ihren Arbeitgeber wegen Diskriminierung verklagt hat. Noch immer ist Simonetti über den Rauswurf verstört. Vor allem, weil Delta anscheinend systematisch ihren Blog ausgewertet hat.

Mehr als 80 Prozent aller US-Unternehmen, so schätzt das New Yorker Beratungsunternehmen American Management Association, setzen mittlerweile elektronische Kontrollinstrumente ein – mehr als doppelt so viel wie Mitte der Neunzigerjahre. Juristische Grenzen gibt es kaum. Das Überwachen von Internet und E-Mail, das Auswerten von Telefongesprächen und Anrufbeantwortern, das Prüfen der Kreditwürdigkeit und das Anbringen von Überwachungskameras – mit der Ausnahme von Toiletten und Umkleieräumen – all das ist in den USA erlaubt. Nach amerikanischer Philosophie stellt der Arbeitgeber den Arbeitsplatz und hat damit alle Freiheiten über die Arbeitsmittel. Selbst wenn Mitarbeiter ihre E-Mails löschen ist das noch keine Gewähr, dass nicht der Arbeitgeber über eine Kopie verfügt. In fast allen großen Unternehmen werden als Routine E-Mails zentral gesichert, um sie nach einem Ausfall wiederherstellen zu können.

Das musste auch Frank Quattrone, zu Dotcom-Zeiten der erfolgreichste und prominenteste Banker im Silicon Valley, erfahren. Zum Verhängnis wurde dem früheren Investmentbanker von Credit Suisse First Boston eine E-Mail, in der er Mitarbeiter im Dezember 2000 zum Vernichten von Unterlagen aufgefordert hatte. Eine elektronische Notiz mit Folgen: In Kürze muss der Multimillionär für 18 Monate ins Gefängnis.

Mittlerweile wird Mitarbeitern schneller der Prozess gemacht – auf allen Hierarchieebenen. Daniel Finney etwa, Redakteur des „St. Louis Post-Dispatch“, verlor seinen Job, nachdem er sich in seinem Blog unter dem Pseudonym Roland H. Thompson mehrfach kritisch über die Tageszeitung geäußert hatte. Finneys Identität festzustellen war leicht. Denn noch nie hatten Unternehmen so viele Instrumente zur Hand, um ihre Mitarbeiter auf Schritt und Tritt zu kontrollieren – selbst nach Feierabend. Videokameras in Besprechungsräumen sind längst Standard. Und dank des Internets, der fortschreitenden Digitalisierung der Kommunikation sowie der Kreativität von Programmierern sind der Überwachung kaum noch Grenzen gesetzt.

Im Dauereinsatz: Spezialsoftware, die den Besuch von Internetseiten protokolliert und den E-Mail-Verkehr überwacht; Programme, die Tastenanschläge festhalten oder nach Schlüsselwörtern in Telefongesprächen, elektronischen Dokumenten oder E-Mail-Nachrichten fahnden; Internetsuchmaschinen, die den Inhalt von Web-Seiten vorhalten, auch wenn das Original bereits gelöscht wurde. „Privatsphäre am Arbeitsplatz“, sagt Lewis Maltby der Chef des National Workrights Institute, „gibt es in den USA schon lange nicht mehr.“

Auch in Deutschland kontrollieren die Unternehmen mittlerweile jeden dritten PC-Arbeitsplatz. Das ergab eine Umfrage der Unternehmensberatung Mummert Consulting. Gleichzeitig ist in knapp 70 Prozent der Unternehmen die private Online-Nutzung am Arbeitsplatz nicht geregelt. „Die Rechtslage“, sagt Roland Gastell von der Anwaltssozietät Lovells, „ist oft unklar“.

Was viele Unternehmen aber nicht davon abhält, die Surfgewohnheiten ihrer Angestellten mittels spezieller Programme zu überwachen. Koordiniert werden die Überwachungsmaßnahmen von hausinternen Sicherheits- oder den Personalabteilungen. „Elektronische Späher eignen sich ideal dazu, die Arbeitsproduktivität zu messen“, sagt Arbeitsrechtler Jan Tibor Lelley von der Kanzlei Buse Heberer Fromm.

So bietet die Mobiltelefongesellschaft Nextel ihren US-Kunden einen Service an, mit dem Unternehmen ihre Mitarbeiter via Handy überwachen können. Per Satellit und Mobilfunknetz wird auf einer via Internet zugänglichen Karte der genaue Aufenthaltsort übermittelt. Auf ihr lassen sich Zonen oder Punkte einstellen, die während der Arbeitszeit nicht aufgesucht werden dürfen. Wer sich in der Bar tummelt oder mal schnell ins Einkaufszentrum zum Shoppen verschwindet, wird ebenso gemeldet wie das Rasen mit dem Firmenfahrzeug auf dem Weg zum Kunden.

Entwickelt hat das System das junge Unternehmen Xora aus dem Silicon Valley. „Wir kriegen jeden Monat 200 Neukunden“, sagt Xora-Chef Sanjay Shirole. Mehr als 2500 Unternehmen nutzen das System bereits, darunter viele Baufirmen und Speditionen. Für den kalifornischen Fußbodenhersteller Butler-Johnson hat sich der Einsatz der elektronischen Fesseln gelohnt: Die Zahl der Überstunden seiner Lieferfahrer hat sich um die Hälfte verringert. Xora berechnet monatlich zwölf Dollar pro Mitarbeiter. Hinzu kommen die Kosten für Mobiltelefon und Vertrag. „Trotzdem sparen unsere Kunden im Schnitt 1500 Dollar pro Mitarbeiter und Jahr“, behauptet Shirole.

Über ein gutes Geschäft freut sich auch Doug Fowler, Chef von Spectorsoft aus Florida. Das Unternehmen hat sich auf Software zum Überwachen von Web-Seiten, E-Mails und Chats spezialisiert. Konkurrent Websense hat ein Programm entwickelt, das komplette Unternehmensnetze überwacht. Bestimmte Web-Seiten lassen sich nicht nur blockieren, sondern deren Nutzung auch zeitlich einschränken. Beispielsweise Einkaufsseiten wie Amazon oder Overstock.

Métier aus Washington D. C. wiederum bietet eine Software namens Worklenz an, die unter anderem vom Rüstungskonzern Lockheed Martin sowie der US-Sparte von BMW genutzt wird. Worklenz bucht sich in E-Mail-Programme, Kalender, Aufgabenlisten sowie Projektmanagementsoftware von Mitarbeitern ein und wertet die dabei gewonnenen Informationen aus. Beispielsweise, wie lang der Mitarbeiter benötigt, um eine bestimmte Aufgabe zu erfüllen und wie viele Schritte er dafür braucht. Anhand der Angaben kann das Programm prognostizieren, ob Projekte im Termin liegen oder mit Sicherheit verzögert werden.

Die Schnüffelei boomt nicht nur, um ineffiziente oder faule Mitarbeiter herauszufiltern. Sie geschieht auch aus Selbstschutz, etwa um sich vor Klagen wegen Diskriminierung zu schützen, wenn Kollegen anzügliche Bilder im hausinternen Netzwerk verschicken oder munter auf Porno-Web-Seiten surfen. Auch für deutsche Unternehmen wird diese Kontrolle angesichts schärferer Gesetze immer wichtiger.

Ein weiteres Motiv für den Einsatz der elektronischen Spürhunde: Mit dem scharfen internationalen Wettbewerb nehmen die Fälle von Industriespionage zu – vor allem weil Internet und Minifestplatten die Weitergabe von Dokumenten erleichtern. Als bei einem großen Mittelständler in Süddeutschland plötzlich 30 Leute geschlossen zu einem anderen Unternehmen wechselten, wurde der Chef stutzig. Sein Verdacht: gezielte Absprachen und Weitergabe von Betriebsgeheimnissen an die Konkurrenz. Er beauftragte zwei IT-Experten, die Festplatten nach Stichworten zu durchsuchen. Mit Erfolg: Nach drei Wochen hatten die Computerfreaks auch von den Exmitarbeitern akribisch gelöschte Dateien wiederhergestellt. Und den Betrug dokumentiert.

Ob Mittelständler, Großbank oder Wirtschaftsprüfer, ob in Deutschland oder den USA: Wegen der Betrugsskandale der vergangenen Jahre müssen vor allem Banken und Versicherungskonzerne sicherstellen, dass ihre E-Mails nicht nur regelmäßig archiviert, sondern auch vor Manipulation und Löschen geschützt werden. Sobald das Management von illegalen Praktiken erfährt – beispielsweise durch eine ausgewertete E-Mail –, muss es tätig werden, um sich nicht selbst strafbar zu machen.

Eine Hamburger Privatbank etwa speichert auf ihrem zentralen Server jeden Schritt, den die Mitarbeiter online machen, notiert die Verbindungsdaten und macht im Verdachtsfall Screenshots der besuchten Internetseiten, also Momentaufnahmen, die dann mit Datumstempel versehen vor Gericht verwertbar sind. Der Chef surft den ganzen Tag mit – dieser totalen Kontrolle hat jeder Mitarbeiter allerdings vorher ausdrücklich zugestimmt.

Einen Schritt weiter ging eine Sparkasse in Baden-Württemberg. Sie verdächtigte einen Mitarbeiter, einem Abteilungsleiter einen anonymen Drohbrief geschickt zu haben. Um den Täter zu überführen, lud der Vorstand zur geselligen Besprechungsrunde bei Kuchen und Wein – und schickte hinterher Gabeln und Gläser, die der Verdächtige benutzt hatte, ins Labor zur DNA-Probe. Ergebnis: Speichelproben von Weinglas und Briefumschlag waren identisch, der Mann wurde kurzerhand entlassen. Zwar konnte der so Überführte vor Gericht erfolgreich gegen das Vorgehen der Bank klagen. Aber bei Verdacht auf schwerere Straftaten, so Arbeitsrechtler **Michael Kliemt**, könne eine DNA-Analyse künftig auch beim Überprüfen von Mitarbeitern geduldet werden. „Warum sollte ein Weg, der hilft, Mordfälle aufzuklären“, so **Kliemt**, „künftig nicht auch gegen kriminelle Mitarbeiter zum Einsatz kommen?“

STEFFI AUGTER, MATTHIAS HOHENSEE

08.02.2005


Aus der WirtschaftsWoche 07/05
Kennen Sie schon das Miniabo?

Alle Rechte vorbehalten.

Die Web-Seiten von wiwo.de, ihre Struktur und sämtliche darin enthaltenen Funktionalitäten, Informationen, Daten, Texte, Bild- und Tonmaterialien sowie alle zur Funktionalität dieser Web-Seiten eingesetzten Komponenten unterliegen dem gesetzlich geschützten Urheberrecht der ECONOMY.ONE GmbH. Der Nutzer darf die Inhalte nur im Rahmen der angebotenen Funktionalitäten der Web-Seiten für seinen persönlichen Gebrauch nutzen und erwirbt im übrigen keinerlei Rechte an den Inhalten und Programmen.

Die Reproduktion oder Modifikation ganz oder teilweise ist ohne schriftliche Genehmigung der ECONOMY.ONE GmbH untersagt. Unter dieses Verbot fällt insbesondere die gewerbliche Vervielfältigung per Kopie, die Aufnahme in elektronische Datenbanken und die Vervielfältigung auf CD-Rom.

© ECONOMY.ONE GmbH, 2000-2005

 Fenster schließen!