So werden Sie vom Chef überwacht!

GEWINN verrät, was Ihr Vorgesetzter alles über Sie wissen kann.

GEWINN zeigt auf, was der Arbeitgeber darf und was nicht.

Wir sitzen in einer Rechtsanwaltskanzlei am Chef-Schreibtisch und lesen von dem dortigen PC aus private E-Mails eines Mitarbeiters, dessen Computer mehrere Zimmer weiter weg steht, mit. Auch sein privater Webmail-Account über gmx.at bleibt nicht frei von unserer Einsicht, da wir in seinen Arbeitsplatz und damit in seine offenen Bildschirmfenster hineinsehen. Der Mitarbeiter steht dabei neben uns und erblasst leicht, als er sieht, welche Möglichkeiten sein Chef hat.

Das unbemerkte Einloggen in den Arbeitsplatz samt Mitlesen, was der Mitarbeiter so tut, funktioniert übrigens auch, wenn man gar nicht im Büro ist. Etwa bei einem guten Frühstück vom Café Landtmann aus – wie uns ein IT-Leiter dank seines Laptops sowie des Funknetzwerks des Cafés zeigt.

Szenenwechsel. Wir gehen mit dem Chef der Wiener Tochtergesellschaft einer amerikanischen Firma in die Kantine. Die Türen auf dem Weg dorthin öffnet er mit seiner Magnetkarte, über die auch seine Essensabrechnung in der Kantine läuft. Wir fragen ihn, ob wir ein Bier bestellen können. Sein „Natürlich" kommt etwas gequält rüber, da dies nun in seiner Lohnverrechnung aufscheint.

Wieder im Büro angelangt werfen wir einen Blick auf den Monitor und orten Thomas Bogensperger übers Web, der gerade auf einer Salzburger Landstraße fährt, was uns ein roter Punkt auf einer Straßenkarte anzeigt. Wir rufen ihn an. Tatsächlich, er ist dort – und gar nicht überrascht, dass wir wissen, wo er ist, hat er uns doch das Passwort für

seine Handyortung gegeben. Bogensperger ist Chef von Virtic Austria, ein Unternehmen, das (mobile) Zeiterfassung und GPS-Tracking bzw. auch Handyortung betreibt. „Dürfen wir das rechtlich eigentlich?", fragen wir ihn. „Wenn es darüber eine Betriebsvereinbarung gibt oder in Firmen, wo es keinen Betriebsrat gibt, der Mitarbeiter, also in dem Fall ich, das Einverständnis dazu gibt, ja."

Ein Industriebetrieb mit mehreren hundert Beschäftigten in Niederösterreich. Wir blicken dem IT-Leiter über die Schulter auf seinen Monitor, während er uns die verschiedensten Kamerapositionen, die im Betrieb aufgestellt sind, zeigt. Dabei erzählt er von Mitarbeitern, die über Nacht „Bandbreite durch mp3- oder Video-Download" gesaugt haben, von Beweisführungen dank Überwachungskameras, die klar gemacht haben, dass doch nicht die Mitarbeiter schuld daran sind, warum eine Maschine ausgefallen ist, was der Maschinenlieferant stets zum „Abputzen" behauptet hat. Dank der Kamera konnte das bewiesen werden.

Er berichtet aber auch, dass es zwar eine Betriebsvereinbarung zwischen Eigentümer und Betriebsrat über die Überwachungstools und deren Anwendung gibt, er sie aber gar nicht kennt und so mehr oder weniger tut, was er ethisch und rechtlich für vertretbar hält.

Wieder in Wien, in einem anderen Betrieb. Wir blicken auf einen Monitor und sehen einem Mitarbeiter zu, der uns anstarrt. Genauer gesagt, blickt er in seinen Monitor und arbeitet auf seinem Computerarbeitsplatz – und hat keine Ahnung, dass wir ihn über die im Monitor seines Notebooks eingebaute Webcam live beobachten.

Ein IT-Leiter, gleichzeitig Sicherheitsbeauftragter in seiner Firma, zeigt uns ein Foto auf seinem PDA, das im Lager geschossen wurde. Es zeigt eine Person, die dort nichts zu suchen hat. Wir werden aufgeklärt: „Der Bewegungsmelder meldet der Kamera, dass sich im Raum was tut, die Webcam schießt ein Foto oder macht ein Video, das sie an mich weitermailt."

So werden Sie vom Chef überwacht!

Nur einige Erlebnisse im Zuge der Recherche, die uns zu denken geben. Allerdings: Denken Sie jetzt nicht gleich an vermeintlich böse Unternehmen und misstrauische Chefs, die kein Vertrauen in ihre Mitarbeiter haben. Und

Foto: Reuters/Paul Sakuma

Ließ den gesamten Vorstand von Hewlett-Packard überwachen – die Ex-Verwaltungsrats-Vorsitzende Patricia Dunn (hier vor Gericht)

auch nicht in die andere Richtung, dass Mitarbeiter prinzipiell zu wenig arbeiten für ihr zu hohes Gehalt, vielleicht noch wie die Raben stehlen und die Firma überhaupt nur ausnützen – darum geht es in dieser Titelgeschichte nicht!

Vielmehr geht es auf den folgenden Seiten darum, Licht in einen Bereich zu bringen, der von rechtlicher Seite oft auch als Grauzone bezeichnet wird. Ein Bereich, in dem sich viele – Arbeitgeber und Arbeitnehmer gleichermaßen – unsicher fühlen, weil sie nicht genau wissen, was denn nun rechtens ist und was nicht. Und nachdem sich kaum jemand wirklich technisch auskennt: Was geht überhaupt? Kann man die Inhalte von E-Mails wirklich mitlesen? Können Passwörter, etwa beim Online-Banking von der Firma aus, tatsächlich ausgespäht werden? Und wer kann/darf das? Alles Fragen, die wir sowohl den Chefs als auch den Mitarbeitern auf den folgenden Seiten beantworten, denn alles, was im Text vorkommt, gibt es auch in der Praxis!

Wie häufig wird überwacht?

In den USA scheinbar ständig. Der Succus aus mehreren diesbezüglichen Studien scheint zu sein, dass mindestens jedes zweite mittelständische Unternehmen drüben seine Mitarbeiter überwacht. Allerdings ist dort die Rechtslage auch eine andere als bei uns. Was die Amis wissen, denn der informelle Druck, den sie auf Europa (auf die EU, aber auch auf die Lieferanten, Kunden und Tochtergesellschaften) ausüben, ist scheinbar groß. Was daraus ersichtlich ist, dass sie auch in europäischen Firmen „Verpfeif-Hotlines" (siehe „Kommt die Amerikanisierung der Betriebsvereinbarungen?") sowie Betriebsvereinbarungen durchsetzen wollen, in denen sogar geregelt sein soll, dass jedes Wort, das im Wagen von Außendienstmitarbeitern fällt, aufgezeichnet wird – was hierzulande ein glatter Rechtsbruch wäre.

Im Zuge der Recherche trat noch ein interessantes Phänomen auf: Es gab noch nie so viele von uns kontaktierte Personen, die zu diesem Thema einiges zu sagen hatten, die das aber nicht in ihren Büros und Firmen tun wollten. Kaum ein IT-Leiter wollte sich fotografieren lassen, kaum ein Firmenchef wollte sein Zitat abgedruckt wiederfinden. Grundtenor: „Wir halten uns streng an die Regeln, machen nichts Ungesetzliches und ich sag es Ihnen auch gerne, aber off records. Das Thema ist halt heikel."

Ein weiterer Grundtenor: Die Sensibilität für das Thema steigt auf beiden Seiten, das berichten alle Vertreter (AK, Gewerkschaft, Manager, IT-Firmen etc.), mit denen wir gesprochen haben. Technisch ist praktisch alles möglich. Detaillierteste Arbeitszeiterfassung, Ortung des Außendienstmitarbeiters per Handy bis auf wenige Meter genau, Erfassung der Leistung (wie auch immer definiert) des Mitarbeiters, wodurch ein Karriereprofil (wer wird befördert, wer nicht) erstellt werden kann. Sogar ein Bewegungsprofil innerhalb der eigenen Firma (wer steht am häufigsten auf, wer geht öfter zum Kaffeeautomaten, wer druckt und kopiert am meisten etc.) kann angelegt werden.

„Kann", nicht „wird"! Denn Daten zu sammeln ist das eine, es rechtmäßig zu dürfen, sie auszuwerten und – die schlimmste Vision der Datenschützer – sie miteinander zu verknüpfen das andere. Denn auch wenn man sagt „Ich habe nichts zu verbergen", zeigt die Praxis der „kalten amerikanischen Kündigung", dass irgendetwas immer gefunden werden kann (und sei es, dass man mit dem Firmen-Pkw mehrmals zu schnell gefahren ist), was dann gegen einen – rechtmäßig oder nicht – verwendet wird.

Überwachung oder Effizienzsteigerung?

Die Frage, die sich daher immer häufiger aufdrängt, lautet: Gibt es in Zukunft noch eine eindeutige Trennung zwischen den Begriffen „Effizienzsteigerung" (jede Firma lebt

Illustration: Erik Bauer

Der Systemadministrator sitzt an der Quelle der Überwachungsmacht. Zum einen hat er wenig Zeit, zum anderen laufen alle Begehrlichkeiten – vom Chef, vom Betriebsrat, vom Mitarbeiter und vom Lieferanten – bei ihm zusammen. Ob alle Anfragen rechtens sind, kümmert diese oft nicht. Um nicht mit einem Fuß im Kriminal zu stehen, sollte er sich rechtlich auf dem Laufenden halten. Und was, wenn er die Firma einmal verlässt? Dann gilt der Administrator-Witz: „Entweder wir investieren Wochen und ändern alle Passwörter und Zugänge – oder wir erschießen ihn einfach."

notwendigerweise davon) und „Überwachung"?

Wie diese Grenzen mittlerweile verschwimmen, zeigt sich zum einen am Führerstand der Taurus-Lok der ÖBB. Der Lokführer muss alle 30 Sekunden ein Pedal treten, sonst meldet sich das System bei ihm, um zu überprüfen, ob er eingeschlafen ist oder nicht. Falls er das nicht tut, wird der Zug automatisch angehalten. Klassische Überwachung, aber niemand wird was dagegen haben. Oder denken Sie an die Möglichkeit der optimalen Routenplanung bei Außendienstmitarbeitern, wenn man weiß, wo sich diese befinden. Überwachung = Effizienzsteigerung.

Wie diese Frage beantwortet wird, davon wird es abhängen, wie homogen das Klima und das notwendige Vertrauen zwischen Arbeitgeber und Arbeitnehmer in Zukunft sein wird. Denn rein rechtlich sieht die Situation so aus, dass – wenn nicht ein klarer Gesetzesbruch vorgenommen wird – es auf die Betriebsvereinbarung mit dem Betriebsrat (den haben aber nur 14 Prozent der heimischen Firmen) oder ansonsten auf die notwendige Vereinbarung, die von der Firma mit jedem einzelnen Arbeitnehmer abgeschlossen werden muss, ankommt, was man darf und was nicht. Natürlich gibt es Mitarbeiter, die sich nicht scheuen, „Nein, das geht zu weit und ist nicht rechtens" zu sagen, aber wie praxisnah ist dies bei der heutigen Angst um den Arbeitsplatz?

Zudem kann Überwachung auch positiv sein. Kein Betriebsrat wird sich dagegen wehren, wenn Mobbing im Unternehmen stattfindet und – was immer wieder passiert – böse Kollegen die Gelegenheit des unbenutzten Arbeitsplatzes der gemobbten Person nutzen, um beleidigende Rundmails in fremdem Namen abzuschicken. Durch die Überwachung hat der Mitarbeiter die Chance, dies zu entkräften. Zudem haben es auch viele Betriebsräte satt, sich für Kollegen ins Zeug zu legen, die trotz Abmahnung immer noch Pornos oder anderes auf das Betriebsmittel Notebook laden, um es gleich darauf auf einen privat angeschlossenen USB-Stick oder auf CD zu überspielen. Das Firmensystem protokolliert das im Hintergrund mit, und es kam schon in mehreren Fällen zu fristlosen Entlassungen, gegen die auch vom Betriebsrat kein Einspruch erfolgte.

Kann kontrolliert werden, welche Seiten ich im Internet ansurfe?

Ja, durch Einsatz von Proxyservern oder spezielle Programme zum „Monitoren" der Internet-Seiten kann detailliert festgestellt werden, welche Seiten hier angesurft werden. Im Firmenumfeld werden hier meist aufwendige professionelle Lösungen verwendet, aber auch im Privatbereich gibt es, oft sogar kostenlose, Programme, die unter anderem zur Kontrolle der Surfgewohnheiten der Kinder verwendet werden können (z. B. Bluecoat K9 Webfilter – siehe www.bluecoat.de).

Die Videoüberwachung ...

... ist wohl eine der klassischen Methoden. Kameras haben sich bewährt. Auf öffentlichen Plätzen, in der U-Bahn und sogar im Foyer des Hotel Sacher sorgen sie für unsere Sicherheit, dienen der Terrorprävention und verhüten Diebstähle. Genauso überwachen sie ganze Unternehmen. Voraussetzung ist, dass sie ausschließlich auf allgemeine Bereiche wie Rezeptionen, Gänge

Foto: Reuters/Anthony P. Bolante

Auch der Ex-Boeing-Chef Harry Stonecipher musste aufgrund von nicht erlaubten privaten E-Mails den Abflug machen

oder Bürotüren gerichtet sind. Intimzonen wie die Toiletten, Damenumkleidekabinen (auch wenn viel gestohlen wird, indem Frau mehrere Schichten Kleidung übereinander anzieht und rausspaziert) sind tabu.

Hans G. Zeger, Obmann ARGE Daten: „In der Regel unzulässig und somit nicht mitbestimmungsfähig, d. h. auch wenn es darüber eine Betriebsvereinbarung zwischen Firma und Betriebsrat geben sollte, werden Video- und Gesprächsaufzeichnungen sein. Hier geht der OGH regelmäßig davon aus, dass der Eingriff zu invasiv ist und somit kein Berühren der Menschenwürde, sondern ein Verletzen vorliegt."

Typische Ausnahmefälle wären etwa Arbeitsplätze, bei denen regelmäßig telefonisch, also mündlich, rechtsverbindliche Verträge vereinbart werden (z. B. Sprachaufzeichnung bei Bestellungen im Call-Center), weiters Videoüberwachungen an besonders gefährdeten Stellen (Bankkassier), bei denen nicht die Überwachung des Mitarbeiters, sondern „der Schutz des Objekts", wie es rechtlich heißt, im Vordergrund steht.

Wobei einige IT-Chefs, die immer häufiger auch für die Videoüberwachung zuständig sind, aus der Praxis erzählen, dass die Zustimmung zur Überwachung bei Männern leichter als bei Frauen zu bekommen ist.

Wie geht das in der Praxis vor sich? Blumenhändler Bernd Doll beispielsweise hat in seinem Geschäft und auch im Eingangsbereich Kameras installiert: „Das war, weil unsere Lieferanten außerhalb unserer Öffnungszeiten liefern und einen Schlüssel haben. Und da hat es mal einen Fall gegeben, den ich zum Anlass für die Überwachung genommen habe. Denn das Misstrauen gegen die Lieferanten oder die Mitarbeiter frisst einen ja innerlich auf und ist nicht förderlich für das Geschäftsklima. So werden die Daten drei Monate aufgezeichnet, wenn was passiert, kann man nachsehen und die Sache hat sich." Anders als in jenem Fall in Oberösterreich, der vor einem Monat durch die Medien geisterte, wo die Kameras auch in der Toilette (Doll dazu: „So was ist katastrophal und gehört gerichtlich verfolgt!") angebracht waren, verzichtete Doll auf die Überwachung sonstiger sensibler Bereiche. „Wichtig sind alle Ein- und Ausgänge und die Kassa." Gefragt hat er die Mitarbeiter zwar nicht, ob er die Kameras installieren darf, „es hat sich aber auch kein Mitarbeiter deswegen beschwert".

Kurt Retzer von der Arbeiterkammer weiß, dass die Videoüberwachung stets ein strittiger Punkt ist: „Das geht sogar so weit ins Detail, dass bei Verfahren die Richter dann jeden einzelnen Zentimeter des Schwenkbereichs der Kameras beurteilen und vorgeben." Doll: „Es hat sich bewährt, das haben auch die Mitarbeiter gesehen. So konnte etwa die Behauptung einer Kundin, sie habe beim Wechselgeld um 100 Euro zu wenig rausbekommen, durch die Aufzeichnung sofort widerlegt werden, was ja auch im Sinne der Mitarbeiterin war."

Auch Rechtsanwalt Roland Gerlach weiß um die abschreckende Wirkung von Kameras und hat einen treffenden Vergleich: „Radar-Warnungen sind auch sinnvoll, die Leute halten

Gerichtsurteile im Download

Foto: Michael Hetzmannseder

Dr. Wolfgang Zankl hat extra für GEWINN-Leser Gerichtsurteile zusammengestellt. Sie können diese unter GEWINN online downloaden

In Österreich findet man nur wenig Rechtsliteratur zu Urteilen, die den Umgang mit E-Mail- und anderen Kontrollen regelt. Daher wird fast immer auf das Deutsche Recht und die dort getroffenen Urteile verwiesen, die laut Expertenmeinungen auch auf Österreich umzulegen sind.
Ao. Univ.-Prof. Dr. Wolfgang Zankl, Leiter des e-center, des Europäischen Zentrums für e-commerce und Internet-Recht, hat extra für GEWINN-Leser eine Übersicht über die Urteile zu Themen wie „Private E-Mail- und Internet-Nutzung am Arbeitsplatz" oder „Datenmissbrauch und fristlose Kündigung" zusammengestellt.
Die fein säuberlich zusammengestellten, für jedermann verständlichen Urteile sowie die jüngste OGH-Entscheidung zum erwähnten Thema Biometrie können Sie einfach und bequem downloaden, und zwar unter www.gewinn.com, Menüpunkt Aktionen.

Bei uns wird jetzt vorgeschrieben, dass alle Passwörter mindestens acht Zeichen haben müssen. Sind diese Passwörter wenigstens sicher genug?
Sofern die Passwörter bestimmten Regeln entsprechen (z. B. nicht leicht erratbar) kann man diese als halbwegs sicher einstufen. Noch sicherer sind allerdings Methoden wie etwa Einmalpasswörter oder eine sogenannte Zwei-Faktor-Autorisierung. Es gibt allerdings physische Keylogger (schlichtweg gesagt ein „intelligentes" Kabel, das zwischen Tastaturstecker und Computer eingesteckt wird), welche unabhängig vom verwendeten Betriebssystem jeden Tastenanschlag aufzeichnen können (siehe www.keyghost.com).

sich viel mehr an die Geschwindigkeitsbegrenzung." Diebstähle sind dadurch nun ausgeschlossen? Doll: „Das nicht, eine Mitarbeiterin hat sich anscheinend so an die Kameras gewöhnt, dass sie sie vergessen hat, als sie ihre Finger in der Kassa hatte . . ."

Auch hier ist die Technik im Übrigen vorangeschritten. Moderne Sicherheitsbeauftragte in den Firmen installieren Bewegungsmelder zu den Kameras dazu, die nur dann filmen, wenn sich auch etwas im Blickfeld bewegt – und gegebenenfalls auch live aufs Handy des Verantwortlichen berichten, entweder als Foto oder als Live-Video. Nicht zuletzt ist auch der starke Preisverfall für das Equipment oder die Dienstleistung mit ein Grund, warum die Unternehmen immer öfter dazu greifen.

Zutrittskontrollen und Zeiterfassung

Elektronische Zutrittskontrollen erfolgen mittels Magnetkarte, Chipkarte, Zahlencode oder biometrische Kennzeichen. Sie erfüllen zwei Zwecke: Erstens lässt sich genau feststellen, wer sich gerade in welchem Bereich aufhält. Besonders in Konzernen mit hoher Sicherheitsstufe gelangt man nur nach Kontrolle von einem Raum in den anderen. Auf einem zentralen Server ist gespeichert, für welche Räume man zutrittsberechtigt ist. Im Wiener Millennium-Tower etwa hält der Lift nur in jenen Stockwerken, die man betreten darf. Diese Berechtigung ist – wie vieles andere – auf der persönlichen Mitarbeiter-ID-Card vermerkt.

Zweitens ist mithilfe der Zutrittserfassung auch der Zeitpunkt Ihres Arbeitsbeginns nachvollziehbar. Das führt uns zum Thema Arbeitszeiterfassung. Eva Angerler, bei der Gewerkschaft der Privatangestellten zuständig für Arbeit und Technik: „Dieses Thema kommt besonders im Bereich der mobilen Arbeit immer stärker. Die Erfassungssysteme werden immer detaillierter, immer projektbezogener."

Hier hat der OGH vor kurzem anlässlich eines Falls in einem Krankenhaus, wo ein Fingerscansystem zwecks Zeiterfassung ohne Zustimmung des Betriebsrats (der daraufhin klagte und eine einstweilige Verfügung auf Verbot des biometrischen Einsatzes erwirkte) installiert wurde, entschieden, dass dies nicht rechtmäßig ist und der Betriebsrat in Form einer Betriebsvereinbarung zustimmen muss. Aus Sicht des OGH berühren übliche Zeiterfassungssysteme (Stechuhren, Magnetkarten) die Menschenwürde des einzelnen Arbeitnehmers nicht, sofern dadurch nicht ein exaktes Bewegungsprofil des Arbeitnehmers erstellt werden kann. Salopp formuliert hat sich der OGH nicht gegen den Einsatz eines biometrischen Systems ausgesprochen, sondern vielmehr gefunden, dass man mit diesem System zur trivialen Kom-

Kameras dürfen nur in Abstimmung mit dem Betriebsrat oder jedem einzelnen Mitarbeiter im Unternehmen installiert werden

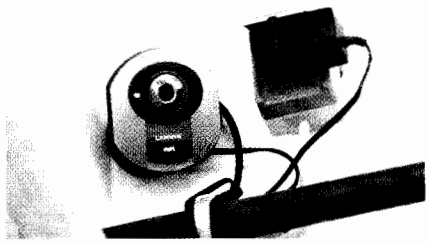


Foto: Pepo Schuster

men-und-gehen-Erfassung übers Ziel hinausgeschossen war, da man immer das einfachste Mittel anwenden sollte (Stichwort Menschenwürde). Das genaue Urteil können Sie über GEWINN online, siehe „Gerichtsurteile im Download", abrufen.

Weiters macht es auch einen großen Unterschied, ob die Arbeitszeit zu laufen beginnt, wenn man das Gebäude betritt, im Zimmer eintrifft oder sich in den PC einloggt. Also zum Beispiel – wie es derzeit in mehreren großen heimischen Firmen diskutiert wird – wenn man um acht Uhr ins Unternehmen kommt, sich aber erst um 8.30 Uhr über den PC einloggt und dort acht Uhr reinschreibt. Die Diskussion läuft dahingehend, dass es doch einfacher sowie verrechnungs- und aufwandtechnisch besser wäre, wenn der Mitarbeiter gar nichts mehr eintippen muss, sondern sich einfach nur einloggt und die Zeit wird mitprotokolliert. In diesem Fall würde er/sie eine halbe Stunde Zeit verlieren, da er/sie sich nicht sofort im System angemeldet hat.

Man kann gespannt sein, wie die Diskussion ausgeht, denn es gibt auch Firmen, in denen Extremfälle anzutreffen sind wie jener, dass sich der Computer selbsttätig wieder ausloggt, wenn man eine gewisse Zeit lang keine Taste gedrückt hat – und diese Pau-

Wir haben nun Produkte im Einsatz, die uns für jede Anmeldung ein neues Passwort generieren. Können diese Passwörter mitgelesen werden?
Hier handelt es sich um Produkte, die sogenannte Einmalpasswörter generieren. Diese sind innerhalb einer bestimmten Zeitspanne (meist 60 Sekunden) nur ein einziges Mal verwendbar. In Kombination mit einem sonst niemand bekannten PIN-Code sind diese Passwörter derzeit eine der sichersten Methoden, sich anzumelden.

Eine Frage von Moral und Vertrauen

Kurt Stroh, Geschäftsführer von IT-Help: „Die Frage ist immer: Was ist sinnvoll und wirtschaftlich?"

Foto: Pepo Schuster

GEWINN: *Herr Stroh, Sie kommen ursprünglich aus der Technik und waren langjähriger EDV-Leiter von Moulinex Österreich und dem Ed. Hölzel Verlag in Wien. Nun sind Sie spezialisiert auf die IT-Projektleitung für Büroinstallationen. Zuletzt haben Sie die Firmennetzwerke zweier großer Anwaltskanzleien konzipiert und umgesetzt. Anwälte haben besonders hohe Ansprüche in puncto Dokumentensicherheit. Welche Ziele verfolgen Unternehmen, die ihre Mitarbeiter elektronisch überwachen?*

Stroh: Die Frage ist immer: Was ist sinnvoll und wirtschaftlich? Zuerst einmal geht es schlicht um Kostenoptimierung. Wenn Mitarbeiter das Firmenequipment für private Zwecke nutzen, kostet das Geld. Surfen im Internet, Speicherplatz für Urlaubsfotos, Zusatzprogramme für Bildbearbeitung oder Musikdownload – das alles belastet die Systeme, bindet Speicherplatz und kostet Geld. Dazu kommt die Arbeitszeit, die nicht produktiv fürs Unternehmen genutzt wird. Das zweite Ziel ist die Sicherheit. Jeder fürchtet sich davor, dass Ex-Mitarbeiter die Kundenkartei mitgehen lassen. Wenn der Geschäftsführer vorhat, einen Mitarbeiter zu kündigen, sollte er eigentlich seinen IT-Chef zeitgleich mit dem Betriebsrat informieren. Nur so lässt sich verhindern, dass der Mitarbeiter das geistige Eigentum des Unternehmens mitnimmt.

GEWINN: *Wie weit darf Sicherheit gehen?*

Stroh: Hier kommen Moral und Recht ins Spiel. Es ist beispielsweise absolut erlaubt, alles mitzuloggen, was auf den Geräten des Unternehmens passiert. Der legitime Hintergrund ist, potenzielle Gefahren abzuwenden – Stichworte Virenverseuchung, Manipulation der Geräte entgegen den Firmenrichtlinien oder strafbare Handlungen wie etwa Kinderpornos downloaden. Das Protokollieren ist immer erlaubt, nicht aber das Lesen der Dokumente. Hier gilt das Briefgeheimnis, außer es besteht der Verdacht einer strafbaren Handlung. Manche Firmen umgehen das, indem sie private Nutzung grundsätzlich verbieten oder alle auf ihrem Equipment erstellten Dokumente als Firmeneigentum deklarieren. Das steht dann aber im Dienstvertrag oder im Code of Conduct, den die Mitarbeiter unterschreiben.

GEWINN: *Der IT-Manager ist also absoluter Vertrauensträger der Geschäftsleitung?*

Stroh: EDV ist immer Vertrauenssache. Der Geschäftsführer kann alle Schlösser tauschen lassen – aber er kann nicht das Administrator-Passwort ändern. Das ist der Generalschlüssel für die gesamte Firma. Technisch ist heute alles möglich.

GEWINN: *Die IT hat damit viel weiter gefasste Aufgaben, als PC-Anwender gemeinhin glauben . . .*

Stroh: Die IT trägt viel mehr Verantwortung als nur dafür, dass alle PCs immer brav laufen. Sie hat eine Sonderstellung im Unternehmen und unterliegt weder dem Umsatzdruck der Operation noch der wirtschaftlichen oder politischen Großwetterlage. Ob der Geschäftsführer ausgetauscht wird, der Eigentümer wechselt oder ein anderer politischer Wind weht – die EDV bleibt immer dieselbe!

se wird einem von der Arbeitszeit abgezogen.

Ganz unbemerkt für den Mitarbeiter können auch Bewegungskontrollen auf der persönlichen ID-Karte installiert werden. Wenn man also das Büro verlässt und Kaffee holen geht, registriert der Sensor das auch ohne das Wissen des Mitarbeiters – und das System zieht die Pause von der Arbeitszeit ab. Ebenso kann leicht nachvollzogen werden, welche Räume man im Laufe eines Tages wie oft aufgesucht hat. Dazu Rechtsanwältin Alexandra Knell: „Unzulässig, da Pausen zulässig sind, denken Sie nur an den Gang zum WC."

Dennoch können die Systeme dies technisch ganz genau eruieren, ob sie allerdings aktiviert werden, steht auf einem anderen Blatt. Angerler: „Bei mobilen Sozialarbeitern etwa, die für ihre Patienten auch des Öfteren einkaufen gehen, wird die Fahrt mit dem Auto zum Einkaufen und retour vom Auftraggeber oft nicht mehr bezahlt, da dies nicht im Arbeitsprofil des Sozialarbeiters drinsteht, dieser es aber aus Herzensgüte gerne mit erledigt." Wie kann der Auftraggeber überhaupt wissen, dass man einkaufen war? „Durch GPS-Tracking im Auto, das mittlerweile immer häufiger wird." (Dazu später mehr.)

Auch für Tätigkeiten im Freien (Baustellen) gibt es übrigens elektronische Lösungen: Mithilfe von wetterfesten ID-Buttons, die auf jeden Schlüsselbund passen, checken die Arbeiter ein und aus. Das zeitaufwendige Erfassen und Protokollieren ihrer Arbeits- und Pausenzeiten entfällt. Der Empfänger dazu ist an einem zentralen Platz auf der Baustelle angeschlossen und funktioniert weltweit über das Mobilfunknetz. Er ist nicht größer als eine Zigarettenpackung.

Was machen Sie am Bildschirm?

Sie glauben tatsächlich, dass nur jene Dateien, die Sie aktiv auf dem Firmenlaufwerk gespeichert haben, nachvollziehbar sind? Sie täuschen sich. Alle paar Minuten, in manchen Firmen sogar mehrmals innerhalb einer Minute, erfolgt eine automatische Systemsicherung, die in erste Linie dem Wiederherstellen der Dokumente im Fall eines Systemabsturzs dient. Die wenigsten Mitarbeiter wissen jedoch, dass damit auch ganz einfach kontrolliert werden kann, was sie gerade am Bildschirm tun.

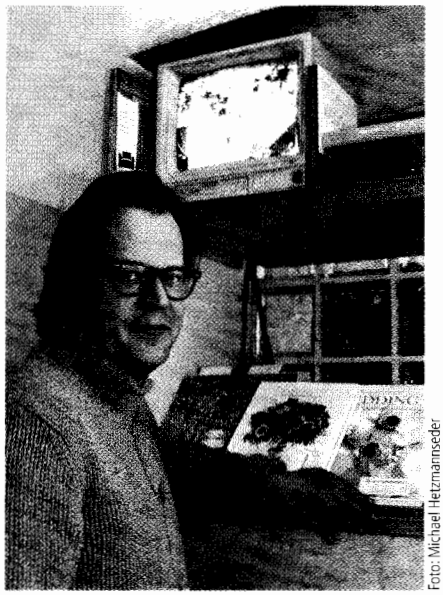


Foto: Michael Hetzmannseder

Wiener Blumenhändler Bernd Doll: „Die Videoüberwachung war notwendig, denn das Misstrauen gegenüber den Mitarbeitern der Lieferanten, die bei uns reinkönnen, wenn wir nicht da sind, frisst einen sonst innerlich auf."

Grundsätzlich kann der gesamte Bildschirminhalt vom Systemadministrator zu jeder Zeit gelesen, gescannt und gespiegelt werden. Natürlich lässt sich auch haargenau feststellen, wenn Sie externe Laufwerke (USB-Sticks, externe Festplatten) anschließen. Diese zu sperren oder zumindest mitzuloggen ist dank spezieller Software eine Fingerübung für jeden ITler – was auch zulässig ist.

Was am häufigsten mitgeloggt wird:

- Die Zeiten, in denen man online ist;
- der Mailverkehr;
- die MS-Office-Dokumente, die man erstellt;
- das Internet-Surfverhalten und
- die Aktivitäten in den Betriebswirtschaftssystemen, mit denen die Firma arbeitet.

Das macht durchaus Sinn: Bei einer SAP-Buchhaltungsanwendung etwa kann jederzeit nachvollzogen werden, ob Buchhalter Meier oder Müller eine bestimmte (Fehl-)Buchung durchgeführt hat.

Wunderbar zum aktiven Beobachten der Mitarbeiter-PCs eignet sich das Programm PC-Duo, früher Remcon (siehe dazu auch die Internet-Links): Die rettenden Engel aus der EDV steigen in ihrer Helpdesk-Funktion in den Computer eines Hilfe suchenden Users ein und lösen online dessen Anwenderprobleme („1st Level Support"). Dagegen hat niemand etwas, im Gegenteil, in diesen Fällen lernt man die Möglichkeiten des Systemadministrators schätzen.

Allerdings können sich die Gurus auch völlig unbemerkt dazuschalten und checken, was der Kollege gerade tut. Als aufmerksamer User erkennen Sie das, falls überhaupt, nur an einem kurzen Flackern des Bildschirms.

Knell: „Die Kontrolle, was der Mitarbeiter am Arbeitsplatz macht, also dass der Bildschirminhalt gelesen, gescannt und gespiegelt wird, ist sehr häufig. Die Zustimmung des Betriebsrats ist aber erforderlich. Die ist auch notwendig, wenn das Helpdesk beim Mitarbeiter-PC miteinsteigt." Aber natürlich gilt generell: Wenn „Gefahr im Verzug" ist, also man den Verdacht hat, dass ein Mitarbeiter etwas tut, was er nicht darf, kann man sofort eingreifen und mitprotokollieren (das steht aber sowieso in jeder Betriebsvereinbarung drin).

Ein anderes (legales) Gustostückerl sind Spionageprogramme, die nicht den Bildschirminhalt, sondern Ihre Tastenkombinationen mitschreiben. Damit sind auch unsichtbare Passwörter, die man für geheim hält, jederzeit zu knacken. Laut Knell kommen diejenigen immer häufiger in Firmen zum Einsatz, die alles „mitloggen", was am Bildschirm gemacht wird, auch Passwörter, Tastenkombinationen etc. Diese Programme sind sogar sehr günstig.

Wir haben auf unseren Notebooks eine Software installiert, die das Auffinden eines gestohlenen Notebooks erleichtern soll.

Es gibt Dienstleister, die auf einem Notebook ein Stück Software installieren, welches für den Normalbenutzer unsichtbar ist. Dieses Programm kontaktiert den Hersteller bei Vorhandensein eines Internet-Anschlusses und teilt diesem die aktuelle Netzwerkadresse mit. Aufgrund derer kann der Standort oft bis auf Stadt- oder Stadtteilgröße bestimmt werden. Wenn die Adresse von einer bestimmten Firma registriert ist, ist auch diese Information vorhanden. Eine Garantie, dass ein gestohlenes Notebook dadurch gefunden werden kann, kann aber keiner dieser Dienste abgeben.

Foto: Pepo Schuster

Ein typischer Spaß, wenn einem Systemadministrator (selten) fad ist: Er beobachtet per Notebook-Webcam, was Mitarbeiter so treiben

Keylogger sind schon um 25 bis 70 Euro erhältlich. Knell: „Die Zustimmung des Betriebsrats oder der Mitarbeiter ist auch hier erforderlich."

Die heikle Frage der E-Mails

Darf jemand aus der Firma E-Mails des Mitarbeiters lesen? Eine Frage, die jeden betrifft und zu der es verschiedene Zugänge gibt. Der eine ist die Vereinbarung, dass das Schreiben von privaten E-Mails verboten ist. Das wird rechtlich nicht halten, denn der Gesetzgeber billigt Arbeitnehmern zu, private E-Mails im normalen (nicht näher definierten) Ausmaß (z. B. „Komme später nach Hause") schreiben zu dürfen.

Der andere ist, per Vereinbarung den gesamten Mailverkehr als Firmenverkehr zu definieren – alles darf gelesen werden, da es ja die Firma betrifft. Der Mitarbeiter muss davon nicht einmal informiert werden, wenn die Geschäftsführung und der Betriebsrat sich darauf festlegen. Knell: „Das ist sehr problematisch in Hinblick auf das Datenschutzrecht." Aber auch hier wird eine fristlose Kündigung wegen privaten Mails im normalen Ausmaß vor Gericht nicht halten.

Gehen Sie davon aus, dass alle eingehenden Mails zu Ihrem eigenen Besten grundsätzlich auf Viren gescannt werden. Manchmal wird allerdings aus Security-Gründen auch der gesamte Inhalt automatisch durchleuchtet. Österreich-Töchter von US-Konzernen erzählen von einschlägigen Erlebnissen mit E-Mails, die sogenannte Bannworte beinhalten. Das sind in Amerika als böse eingestufte Begriffe, die auf eine schwarze Liste gesetzt und vom Server nicht durchgelassen werden. So kann es passieren, dass ein Freund Sie ganz unschuldig ins Casino einladen will – das Wort „Casino" ihn allerdings auf die Blacklist katapultiert und seine Mails für alle Zeiten sperrt.

Es soll doch tatsächlich noch Outlook-Anwender geben, die glauben, eine Mail ist entfernt, wenn sie in den Ordner „Gelöschte Objekte" verschoben wurde. Doch selbst wenn man diesen regelmäßig ausleert, kann der gesamte Mail-Verkehr noch immer am (Exchange-)Server als Sicherungskopie abgespeichert sein. Ob das tatsächlich so ist, hängt davon ab, wie der Server standardmäßig eingestellt wurde. Manchmal ist man sogar froh über ein Back-up: Immer wieder sind besonders Manager aus den höheren Rängen sehr dankbar, wenn irrtümlich gelöschte wichtige Mails wiederhergestellt werden können. In internationalen Firmen werden E-Mails bzw. der gesamte E-Mail-Verkehr jahrelang extra abgespeichert und aufbewahrt.

Outlook kennt zahllose Möglichkeiten zu Ihrem Schutz und zu dem Ih-

Kann man meine Passwörter, die ich auf verschiedenen Web-Seiten verwende, herausfinden?
Wenn die Web-Seiten (wie etwa Web-Mail, Online-Gaming etc.) unverschlüsselt aufgerufen werden, so besteht theoretisch die Möglichkeit, dass Administratoren von Netzwerken, Proxyservern oder Firewalls den Netzwerkverkehr überwachen und dadurch zu Anmeldeinformationen wie Benutzernamen und Passwort gelangen. Dazu werden aber oft administrative Zugänge benötigt. Daher wird immer empfohlen, bei verschiedenen Anwendungen oder Web-Seiten nie die gleichen Passwörter zu verwenden.

Checkliste für Betriebsvereinbarungen zur Internet-Nutzung

Foto: Michael Hetzmannseder

Dr. Alexandra Knell ist auch Vortragende für Security-Manager-Rechtsberatung: „Wenn ich über rechtliche Konsequenzen für sie spreche, höre ich oft, das soll mir mal jemand beweisen."

Was wird geregelt?
- Nutzung von Firmen-PC
- Internet-Nutzung allgemein
- E-Mail-Nutzung (Firmenaccount oder private Accounts, z. B. Hotmail oder Yahoo!)
- Laden von Programmen auf Firmen-PC

Gebote und Verbote
- Zeitlicher und inhaltlicher Umfang der Nutzung von Firmen-PC
- Umfang und Inhalt der Internet-Nutzung und der E-Mail-Nutzung
- Welche Programme geladen werden dürfen?

Kontrollmaßnahmen
- Darf der Arbeitgeber Kontrollmaßnahmen durchführen?
- Welche Kontrollmaßnahmen sind zulässig? (Log-Files, Überprüfung der geöffneten Websites etc.)
- Wie ist die Kontrolle durchzuführen? (Wann? Durch wen?)
- Was passiert mit den Ergebnissen der Kontrolle? Wer darf die Ergebnisse einsehen? Wie lange werden sie aufgehoben/gespeichert?

Gültigkeit der Betriebsvereinbarung
Wie lange ist die Betriebsvereinbarung gültig?
Wie endet sie (Befristung, Kündigung)?

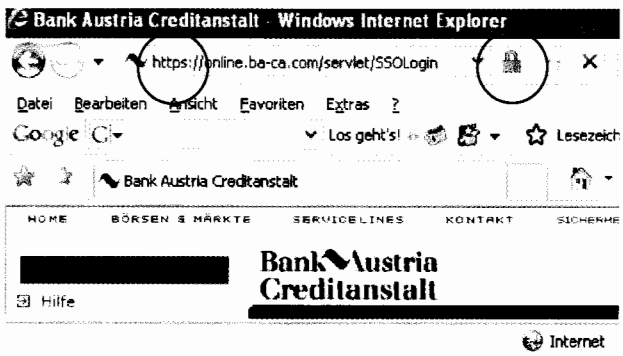
ERSTELLT VON RECHTSANWÄLTIN DR. ALEXANDRA KNELL

res Arbeitgebers. Sie reichen vom simplen Übernehmen des Postein- und -ausgangs bis zum Katalogisieren und Umleiten der Mails einzelner Sender oder Empfänger durch den Systemadministrator. Bei verdächtigen (Verdacht auf Zugriff von Daten, zu denen er/sie keine Berechtigung hatte) Mitarbeitern oder jenen, die sich in Kündigungsfrist befinden (siehe Interview mit Kurt Stroh), können ausgehende Mails komplett abgefangen werden, ohne dass der Mitarbeiter eine „Nicht zugestellt"-Nachricht erhält. Auch Attachments werden durch Größenbeschränkungen limitiert oder ganz unterdrückt – der Gekündigte kann dann weder Kundenlisten aus der Firma schmuggeln noch seinen Lebenslauf an Bewerbungsschreiben anhängen. Übrigens: Auch das Ausdrucken der Kundenliste auf Papier wird mitprotokolliert …

Laptops und Mobiltelefone

Laptops verlassen bestimmungsgemäß das Firmennetzwerk und müssen vor jedem neuerlichen Zuschalten auf Viren gescannt werden. Dabei wird allerdings auch alles mitprotokolliert, was der Laptop-Besitzer in der Zwischenzeit am Gerät getan hat. Wer sich also für besonders schlau hält, wenn er sich Sexseiten im Web auf seiner privaten mobilen Datenkarte anschaut, hat sich getäuscht: Das gesamte Surfverhalten wird immer mitgeloggt und beim Wiedereintritt ins Firmennetz auf den Zentralserver übertragen …

Kann man meine verwendeten TAN-Nummern beim Internet-Banking ablesen? Und vom Firmen-PC aus?
Im Normalfall nicht, es gibt aber technische Möglichkeiten, wenn der Angreifer an einer strategisch günstigen Stelle sitzt, dass eine sogenannte „Man in the Middle"-Attacke durchgeführt wird. Dabei täuscht der Angreifer dem Anwender die Bank vor und kann dadurch rein theoretisch in den Besitz der übermittelten TAN kommen. Dies ist aber technisch sehr aufwendig und in normalen Firmennetzwerken kaum durchführbar.
Vom Firmen-PC aus: Generell gilt Internet-Banking als sichere Art der Datenübertragung, solange es sich um eine HTTPS-Verbindung handelt. Das erkennen Sie am Bildschirm links oben in der Adresszeile Ihres Browsers (https:// statt http://) und rechts unten am Icon in Form eines kleinen Schlosses.



Achten Sie auf verschlüsselte Übertragung beim Online-Banking. Also mit zugemachtem Schloss und „https" statt „http"

Die Bank kümmert sich darum, dass niemand die Daten zwischen Ihrem Computer und dem Bankserver sieht. Sie weiß allerdings nicht, was mit Ihrem Rechner passiert. Wenn also Ihr Password über einen Keylogger in Ihrer Firma mitgeloggt wird, ist das außerhalb der sicheren Verbindung. Daher empfiehlt es sich, Bankgeschäfte vom Heim-PC aus zu erledigen – dort loggt mit großer Wahrscheinlichkeit niemand mit.

Software zum Überwachen

Bei den Quellen handelt es sich um Beispiele aus dem umfangreichen Angebot an Produkten und Lösungen. Die Liste ist keinesfalls vollständig, sie stellt nur einen geringen Auszug aus dem Gesamtangebot dar.

Remcon-PC-Duo Fernwartung
www.netsupportmanager.com/DE/downloads.asp
Keylogger und PC-Überwachung
www.key-logger.de/
www.digitalfuturesoft.com/keyboardlogging.php
www.keelog.com/
www.keyghost.com
www.spectorsoft.de
www.gdata.de
www.trisys.com/products.htm
www.webroot.com
www.iambigbrother.com

Auffinden gestohlener Notebooks
www.webtrackingcenter.com
PC-Device-Kontrolle
www.magelan.at/produkte/landesk/ldss
GPS-Überwachung Fahrzeuge
www.peilsender.de/content/view/35/82
www.baumaschinenortung.de
www.ort24.de
www.omegasol.at/s_more_mobileObjects.htm
www.virtic.net
www.enaikoon.at
www.e-tronic.at/et_2006/html/securityscout.cfm

Überprüfung Passwortsicherheit
www.microsoft.com/athome/security/privacy/password_checker.mspx
Handy-Ortung
www.corscience.de/flottenmanagement.html
www.handytracking.net
Zutrittskontrolle, Keycard, Einmal-Passwörter
www.key-card.at/
www.rsa.com/
Spionage-/Web-Filter-/Aufzeichnung-des-Surfverhaltens-Software
www.surfcontrol.de
www.websense.com
www.symantec.de
www.protectcom.de
www.internetwatcher.de
www.bluecoat.de
Kontrolle externer Anschlüsse
www.kuert.at

Apropos Pornoseiten: Diese werden – so gut es geht – von den meisten Systemadministratoren geblockt, was verständlich ist (Ablenkung und Vergeudung von Arbeitszeit).

Allerdings hört man bereits von Firmen, die Internet-Seiten wie Herold (Auskunft), orf.at (Information) und eBay (Online-Auktion) ebenfalls blocken ...

Natürlich ist auch der komplette Datenverkehr auf dem Gerät transparent. Die Security-Varianten reichen vom einfachen Mitloggen von Versand, Speichern und Ausdruck von Dokumenten bis zur Komplettsperre, die verhindert, dass Daten den Laptop verlassen können, wenn dieser aus dem Firmennetz entfernt wird.

Erinnern Sie sich an die medienwirksame Verhaftung des Saliera-Diebes? Er konnte dank Handy-Ortung aufgespürt werden. Theoretisch lässt sich auch jederzeit feststellen, in welchem Funkgebiet Sie sich wann befunden haben. Da dieser Telekom-Service aber extra kostet, wird er nur bei begründetem Verdacht in Anspruch genommen. Sie sollten aber wissen, dass alle Ihre Telefonate mit Handy und Festnetz via Nummernliste täglich nachvollziehbar sind. Das Festnetz wird in Firmen so gut wie immer mitgeloggt: bei neuen Anlagen ein- und ausgehende, bei älteren nur ausgehende Anrufe. Bei Internet-Telefonie (Skype) wird grundsätzlich alles mitgeschrieben. Skype bedingt allerdings, dass man generell Programme selbst auf den PC installieren darf. Und das unterbinden die großen Firmen sowieso immer häufiger!

Handy-Ortung ist meist abhängig vom Service-Provider und in Österreich noch kaum möglich. Außerdem muss hier immer der Eigentümer des Handys zu einer Ortung über GPS oder Handy-Provider zustimmen. Eine Überwachung erfolgt hauptsächlich über zusätzliche GPS-Empfänger, eingesetzt wird dies vielfach bei Transportunternehmen zur Überwachung der Fahrzeugflotte.

Kann man kontrollieren, ob ich vertrauliche Informationen auf einen USB-Stick oder die Speicherkarte einer Digitalkamera speichere?
Durch entsprechende Software kann nicht nur kontrolliert, sondern auch verhindert werden, dass bestimmte Dateien auf externe Speichermedien wie etwa USB-Sticks, externe Festplatten oder auch SD-Karten (Stichwort: Digitalkamera) kopiert werden. Diese Lösungen sind aber meist sehr komplex und nur im Firmenumfeld bei sensiblen Daten denkbar und sinnvoll.

Kommt die Amerikanisierung der Betriebsvereinbarungen?

Rechtsanwalt Dr. Robert Gerlach über typische Beispiele, die Firmen immer häufiger in ihren Betriebsvereinbarungen verankert wissen wollen und die seines Erachtens die Kontrollbefugnisse überschreiten: „Ich hielte es etwa für unzulässig, in Dienstautos ein Programm zu installieren, mit denen das Fahrverhalten ständig analysiert wird. Aus meiner Praxis ist mir etwa folgende einseitige Anordnung des Arbeitgebers bekannt: ‚Der Arbeitgeber ist berechtigt, ein elektronisches Programm zur Analyse des Fahrverhaltens des Dienstnehmers zu installieren, das aus einem Monitorsystem und aus einem Datenaufzeichnungssystem besteht. Diese Systeme werden über den Zündschlüssel automatisch aktiviert und zeichnen laufend zumindest die Geschwindigkeit, das Beschleunigungs- und Bremsverhalten auf. Diese Daten über das Fahrverhalten werden monatlich ausgewertet und können allenfalls zu einer verpflichtenden Nachschulung des Mitarbeiters führen.'

In einer derartig einseitigen Richtlinie hat sich einmal auch die Anweisung gefunden, dass beim Einparken des Autos alle Anstrengungen unternommen werden sollen, das Dienstauto so einzuparken, dass es in derselben Bewegung ausgeparkt werden kann, wie es vordem eingeparkt worden ist.

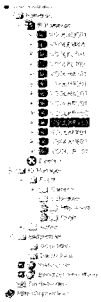

Foto: Michael Hetzmannseder

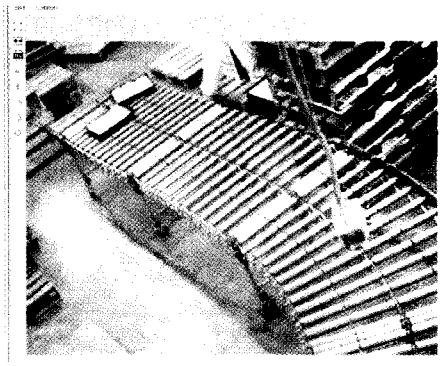
Dr. Robert Gerlach: „Whistleblowing-Hotlines sind in Amerika gang und gäbe."

Problematisch sind weiters Verpflichtungen, das Fehlverhalten anderer Mitarbeiter der Unternehmensleitung anzuzeigen. Solche „Whistleblowing-Hotlines" werden von US-amerikanischen Konzernen verpflichtend bei europäischen Tochtergesellschaften eingerichtet, damit Unregelmäßigkeiten von Kollegen sofort direkt bei der Konzernleitung angezeigt werden können. Hintergrund dafür ist der Sarbanes-Oxley-Act (SOX), der im Jahr 2002 im Zuge der Bilanzfälschungsskandale vom US-amerikanischen Kongress verabschiedet worden ist.

Für den österreichischen Rechtsbereich wird man annehmen dürfen, dass solche Whistleblowing-Systeme nur auf freiwilliger Basis verwendet werden dürfen. Alle Mitarbeiter und der Betriebsrat sind von solchen Systemen zu informieren, wobei Betriebsvereinbarungen notwendig sein können. Einseitige Anordnungen, mit welchen die Mitarbeiter verpflichtet werden, Verstöße anderer Mitarbeiter anzuzeigen und selbst mit Sanktionen bedroht werden, wenn sie dies unterlassen, sind ohne Abschluss einer Betriebsvereinbarung jedenfalls unzulässig.

Eine einseitige Anordnung, wonach alle Mitarbeiter verpflichtet sind, jeglichen Verdacht eines Verstoßes gegen einen Ethik-Kodex zu melden, wobei das Unterlassen einer solchen Meldung per se gegen den Ethik-Kodex verstößt, werden daher nach österreichischem Arbeitsrecht unzulässig sein.





Videoüberwachung kostet heute kaum noch Geld. Die Webcams sowie die notwendige Software sind bereits unter 100 Euro erhältlich. Nur müssen Sie rechtlich darauf achten, dass Sie die Mitarbeiter „nicht vordergründig in den Mittelpunkt" stellen, sondern irgendwelche Objekte, mit denen was passieren könnte

Außendienst, GPS und Dienstautos

Mitarbeiter im Außendienst sind schwieriger zu überwachen als im Haus tätige. Wie stellt der Chef fest, ob diese Kollegen auch tatsächlich beim Kunden sind? Am einfachsten ist es, ihnen eine lückenlose Tagesroute vorzuschreiben. Via Dispatching, Kilometeraufzeichnungen und beim Kunden verrechnete Arbeitszeit lassen sich mit relativ geringem Aufwand Zeit-Weg-Diagramme für Verkauf und Service erstellen.

Ist der Tagesablauf nicht vorhersehbar, lässt sich der Außendienstmitarbeiter jeden Aufenthalt vom Kunden bestätigen und schickt die Liste am Ende des Tages in die Zentrale. Das geschieht meist via Laptop, Modem oder Scanner. In Kombination mit seinem Fahrtenbuch wird damit nicht nur völlig klar, wann er wohin gefahren ist, sondern auch, wie viel Benzin er dafür verbraucht hat. Und glauben Sie bloß nicht, dass Ihr Treibstoffverbrauch nicht regelmäßig mit dem Ihrer Kollegen verglichen wird!

Es soll Zeiten gegeben haben, in denen Dienstwagenbesitzer einen zusätzlichen Privatkanister mit Benzin befüllt und mittels Tankbeleg abgerechnet haben. Heute gibt es relativ häufig bereits einfach zu installierende Geräte, mit deren Hilfe der Fuhrparkleiter auch tausende Kilometer entfernt bereits vor (!) der Zufahrt zur Tankstelle sehen kann, wie viel Treibstoff noch im Tank ist.

Noch einem Überwachungsgrad mehr unterliegt man, wenn im Dienstauto ein Fahrtenschreiber montiert ist. Der loggt nicht nur mit, wann man wo ist, sondern auch Geschwindigkeit, Drehzahl und Gang. Wenn man also im dritten Gang auf der Autobahn fährt, um möglichst schnell zu einem neuen Dienstwagen zu kommen, ist das nachvollziehbar. Umgekehrt kann man auch beweisen, dass man artige 130 km/h gefahren ist, wenn eine Anzeige wegen 150 km/h in die Firma flattert.

Die Hightech-Variante ist ein GPS-Sender, mit dem sich die Position haargenau feststellen lässt. Das ist heute gängige Praxis bei teuren Lkws und Baumaschinen. Erst kürzlich ging die

Geschichte eines Raupenbaggers durch die Zeitungen, der in Schleswig-Holstein gestohlen und dank Telematik an der tschechischen Grenze wiedergefunden wurde. Immer öfter werden auch Mietautos und Firmenflotten mit GPS-Sendern ausgestattet. Da die Versicherungsprämien aufgrund des verringerten Diebstahlrisikos sinken, amortisiert sich die Investition relativ rasch und ist auch für Privatpersonen interessant.

Blick über den großen Teich

Sie glauben, das ist schon Überwachung total? In den USA geht noch viel mehr. In großen Konzernen kontrolliert Ihre ID-Card etliches mehr als nur Ihre Identität. Natürlich bezahlen Sie auch im firmeneigenen Restaurant mit Karte. Dort wird mitgeloggt, was und wie viel Sie gegessen haben. Der Firmenarzt wertet diese Informationen aus und stellt fest, welche Ihrer Krankheiten auf die Ernährung zurückzuführen ist. Das kann zur Abmahnung führen und sogar zur Kündigung, wenn Ihre Leiden als selbst verschuldet eingestuft werden. Genauso wird Ihr Warenkorb im hauseigenen Supermarkt überwacht, den Sie mit Firmenkarte bezahlen. Auch im Fitness-Center, zu dem Sie natürlich mittels ID-Card Zutritt haben, stehen Sie unter Beobachtung: Wer nicht hingeht, lebt nicht gesund. Vollends paranoid dürfen Sie beim Gedanken an Satellitenüberwachung des Konzernparkplatzes werden.

Foto: Privat

Dr. Eva Angerler, GPA: „Ich rate zum Abschluss einer EDV-Rahmenbetriebsvereinbarung und diese dann um einzelne Module zu erweitern."

Und das alles bei Firmen, die jedermann auch hierzulande kennt . . .

Und in Österreich?

Zahlreiche Betriebsvereinbarungen sind aus dem Jahre Schnee. Immer mehr Firmen aktualisieren diese daher, wobei Angerler dabei jedem Betriebsrat zu folgender Vorgangsweise rät: „Am besten nur eine EDV-Rahmenbetriebsvereinbarung abschließen und diese dann um einzelne Module erweitern, wenn zum Beispiel eine neue Software angeschafft wird. Was ist das Ziel des Systems, wer hat Zugriff etc.?" Und was sagen die Unternehmer dazu, schließlich müssten diese sich ja wegen jeder solchen Anschaffung in Verhandlungen mit dem Betriebsrat oder den Mitarbeitern stürzen. Angerler: „Natürlich gefällt ihnen das nicht. Aber nicht näher definierte Formulierungen wie ‚. . . das Leistungsmanagement zu verbessern . . .', die alles beinhalten können, können es auch nicht sein!"

Chef lauscht mit – was ist mitbestimmungspflichtig?

VON HANS ZEGER, OBMANN ARGE DATEN

Foto: ARGE Daten

Hans Zeger, Obmann ARGE Daten, über die rechtlichen Grundlagen

Grundsätzlich gilt: der Arbeitgeber darf viele der Möglichkeiten nicht ohne schriftliche Zustimmung des Betriebsrats oder, falls keiner vorhanden ist (nur 14 Prozent der heimischen Firmen haben einen), des Arbeitnehmers einsetzen. Die Grundlage zur Mitbestimmung: Bei privaten Dienstverhältnissen § 96 bzw. 96a ArbVG, bei öffentlichen Dienstverhältnissen PVG § 9 Abs. 2 Z f bzw. in vergleichbaren landesgesetzlichen Regelungen – vereinfacht gesagt, darf keine Kontrollmaßnahme die Menschenwürde, die Bestimmungen des Datenschutzgesetzes sowie des Telekommunikationsgeheimnisses verletzen, auch nicht, wenn es eine Betriebsvereinbarung darüber geben sollte.

Der OGH hat mehrmals allgemein die Grenze bei der technischen Eignung eines Systems zur Überwachung/Kontrolle gezogen bzw. wenn mehr Mitarbeiterdaten ermittelt/verwendet werden, als zur betrieblichen Führung unbedingt erforderlich sind.

Typischerweise ist keine Mitbestimmung gegeben, wenn Mitarbeiterdaten zur Lohnverrechnung oder zur Feststellung der An- und Abwesenheitszeiten verwendet werden. Auch Leistungsaufzeichnungen (zum Beispiel Akkordleistung) sind dann nicht mitbestimmungspflichtig, wenn sie Teil der dienstrechtlichen Vereinbarung sind (Arbeits- oder Kollektivvertrag, in dem Leistungsentlohnung vereinbart ist). Weiters besteht keine Mitbestimmungspflicht, wenn Daten aufgrund gesetzlicher Bestimmungen erhoben, verwendet oder weitergegeben werden (typischerweise Sozialversicherungsmeldung, Lohnsteuermeldung usw.).

Aber auch bei Lohnverrechnung, Anwesenheitskontrolle oder Leistungskontrolle kann, auch wenn diese betrieblich notwendig oder arbeitsvertraglich vereinbart sind, Mitbestimmungspflicht entstehen. Ein wesentliches Kriterium ist nach ständiger Judikatur die Kontrolldichte und der Umfang des Eingriffs in die Privatsphäre des Mitarbeiters.

Können sich Betriebsrat und Arbeitgeber nicht über eine Vereinbarung einigen, kann eine Schlichtungsstelle angerufen werden.

Wo findet die Betriebsvereinbarung ihre Grenze? Einerseits kann nichts vereinbart werden, was die Menschenwürde verletzt (siehe oben), andererseits können aber auch höchstpersönliche Datenschutzrechte der Mitarbeiter nicht außer Kraft gesetzt werden. So kann eine Betriebsvereinbarung keinen Verzicht der Mitarbeiter auf das Auskunftsrecht nach DSG 2000 festschreiben. Auch wird eine Betriebsvereinbarung nicht die Mitarbeiter verpflichten können, persönliche Ereignisse (Hochzeiten, Geburt eines Kindes, ...) oder Fotos, die sie darstellen, im Intranet oder gar im Internet zu veröffentlichen („weil das zum Image des Betriebs gehört"). Hier könnte eine Betriebsvereinbarung bloß einen Rahmen festlegen, innerhalb dessen auf freiwilliger Basis Mitarbeiter persönliche Angaben veröffentlichen bzw. bekannt geben.

Ein wichtiger Komplex sind Kommunikationseinrichtungen, sofern dazu mitarbeiterbezogene Daten aufgezeichnet werden:

- Telefonanlagen, Mobiltelefonnutzung, E-Mail- und Internet-Nutzung, gemeinsam genutzte Terminkalender oder Projektdatenbanken, Notebook-, PDA- oder Blackberry-Nutzung, sofern deren Daten mitarbeiterbezogen ausgewertet werden.
- Der Zugang zum unternehmenseigenen Computersystem, sowohl innerhalb des Betriebes als auch von außerhalb (Remote Login, Extranet-Zugang). Es muss dabei im Einzelfall gar nicht erforderlich sein, dass ein Unternehmen tatsächlich mitarbeiterbezogene Daten aufzeichnet, es genügt, wenn das System technisch dazu in der Lage ist.

Klassische Beispiele für mitbestimmungspflichtige Erfassungen:

- Garagenplatz- und einfahrtsverwaltung, Kantinenabrechnung, elektronische betriebliche Einsatzplanung, Verwaltung freiwilliger Leistungen (z. B. Nutzung von Freizeit- und Sporteinrichtungen, Kindergartenplätze), Schulungsdatenbank (sofern sie über die bloße Aufzeichnung von betrieblich veranlassten Kursteilnahmen hinausgeht, etwa Erfolge aufzeichnet oder zur Karriereplanung dient), Lohnabrechnung, sofern mehr Daten als minimal erforderlich verwendet werden (etwa Lohnzetteldruck bei der auszahlenden Bank). Biometrische Zutrittskontrollsysteme (Gesichts-, Sprach- oder Fingerabdruckerkennung), sonstige elektronische Zutrittskontrollsysteme (Chipkarten, RFID, Magnetkarten), elektronische Dienstausweise (SinglSignOn), Mitarbeiter-Ortungssysteme (GPS, Handy-Ortung, innerbetriebliche Ortungssysteme).
- Leistungsauswertungen bei Computerarbeit und Sachbearbeitertätigkeit (Keylogger, Aufzeichnung von Eingabefehlern, Geschwindigkeit der Fallbearbeitung, Effizienz in der Systemnutzung) – hier stellen viele ERP-Systeme Zusatzmodule zur Verfügung. HR-Systeme, die der Karriereplanung dienen. Personalinformationssysteme ganz allgemein. Produktionsanlagen mit Betriebsdatenerfassung, die mitarbeiterbezogene Aufzeichnungen über Maschinenauslastung, Stillstandszeiten, Produktivität und Umfang der Fehlproduktion führen, sowie zusätzliche betriebliche Mitarbeiteraufzeichnungen, die über ein Intra- oder Extranet-System zugänglich sind, beispielsweise betrieblich erforderliche Gesundheitsdaten, Qualifikationsdaten. Mitarbeiterbefragungen, insbesondere wenn sie elektronisch oder online durchgeführt werden.