

ARBEITSRECHT

BIG BOSS IS WATCHING YOU

Privates Mailen und Surfen ist vielen Chefs ein Dorn im Auge. Die Mitarbeiter verplumpen Arbeitszeit, fürchten die einen. Andere haben Angst vor Computerviren oder davor, dass geheime Infos nach außen dringen. Darum werden die Mitarbeiter immer genauer überwacht.

Text: Astrid Schwamberger

Es trifft selbst die Bosse. Boeing-Chef Harry Stonecipher stolperte über Liebes-E-Mails im Firmenetzwerk. Dem Vorstand waren Privatmitteilungen des 68-Jährigen an eine Kollegin zugespielt worden. Stoneciphers Verhalten stehe nicht im Einklang mit dem Verhaltenskodex des Konzerns, ließ man verlauten – das Aus für „Dirty Harry“. Dabei hatte man den alten Haudegen erst 15 Monate zuvor aus dem Ruhestand zurück in die Zentrale nach Chicago geholt. Er sollte das durch zahlreiche Skandale lädierte Image des Flugzeugbauers retten. Das ging nach hinten los. Wie die Korrespondenz überhaupt abgefangen werden konnte, wurde zunächst nicht bekannt. Doch der kritische US-Autor Dave Lindorff fand eine Erklärung: Das E-Mail-Überwachungsprogramm des Konzerns brachte den Boeing-Boss zu Fall.

Was wird in deutschen Büros ausspioniert?

Die Überwachung der E-Mails von Angestellten ist in den USA längst an der Tagesordnung. Wie die American Management Association in einer aktuellen Umfrage herausfand, prüfen und speichern 55 Prozent der 526 befragten Unternehmen den elektroischen Postverkehr ihrer Mitarbeiter. 76 Prozent nehmen das Surfverhalten unter die Lupe. Deutsche Firmen sind da noch etwas zurückhaltender. Doch das Misstrauen wächst. Bei einer Trendumfrage

der Unternehmensberatung Steria Mummert im Jahr 2005 gaben 38 Prozent der 289 Teilnehmer an, dass die Rechner ihrer Mitarbeiter überwacht würden. Zwei Jahre zuvor waren es erst 35 Prozent.

Eine Totalüberwachung von Beschäftigten ist nach dem deutschen Grundgesetz nicht erlaubt. Doch sobald man vom Firmencomputer aus ins Internet will, greift eine Vielzahl von Gesetzen. Oft reicht der Verdacht, dass mehr gesurft als gearbeitet wird, dass Raubkopien oder Pornos heruntergeladen, Viren eingeschleppt oder Betriebsgeheimnisse verraten

»SPY-SOFTWARE REGISTRIERT JEDE TASTATUREINGABE, MACHT SCREENSHOTS, PROTOKOLLIERT WEBSEITEN, ÜBERWACHT CHATS UND E-MAILS.«

wurden, um Stichproben zu rechtfertigen. Manche Chefs mögen Internetprotokolle auch nutzen, um unliebsames Personal loszuwerden.


Wie funktioniert die Überwachung?

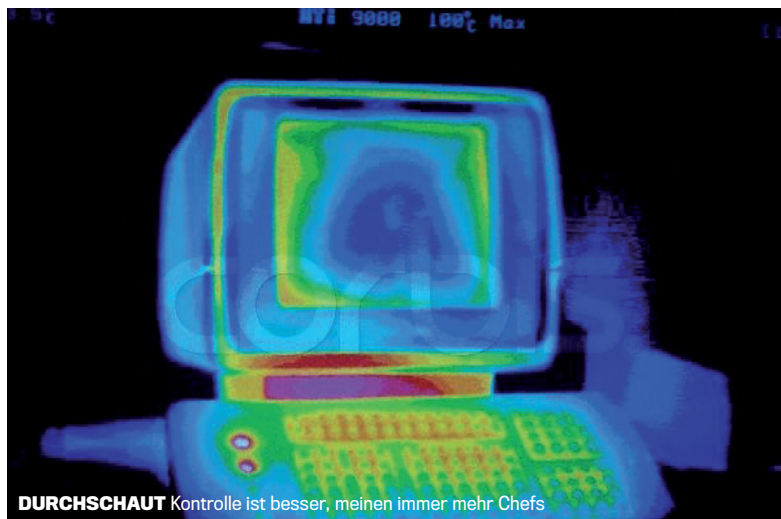
Um die Streifzüge der Belegschaft im World Wide Web auszukundschaften, reicht schon der Blick in den Verlauf des Webbrowsers. Je nach Einstellung sind dort die Surfstationen mehrerer Tage aufgeführt. Auskunft geben auch Zwischenspeicher wie der Cache oder der Ordner „Temporäre Dateien“ und die Ein-

gabehilfe „Autovervollständigen“, die alle bekannten Adressen oder Suchbegriffe auflistet, sobald ein Buchstabe eingetippt ist: Ein E genügt, um beispielsweise alle Ebay- oder Expedia-Seiten anzuzeigen zu lassen, die der Nutzer aufgerufen hat. Gegenmaßnahme: Spätestens am Abend die entsprechenden Daten im Browser (unter „Extras“) löschen. In Netzwerken mit einem Proxy-Server genüge dies jedoch nicht, warnen Experten. Hier werden alle Verbindungen ins Internet gespeichert, damit der Nutzer beim nächsten Mal schneller surfen kann. Endgültig löschen kann diese Spuren nur der Administrator.

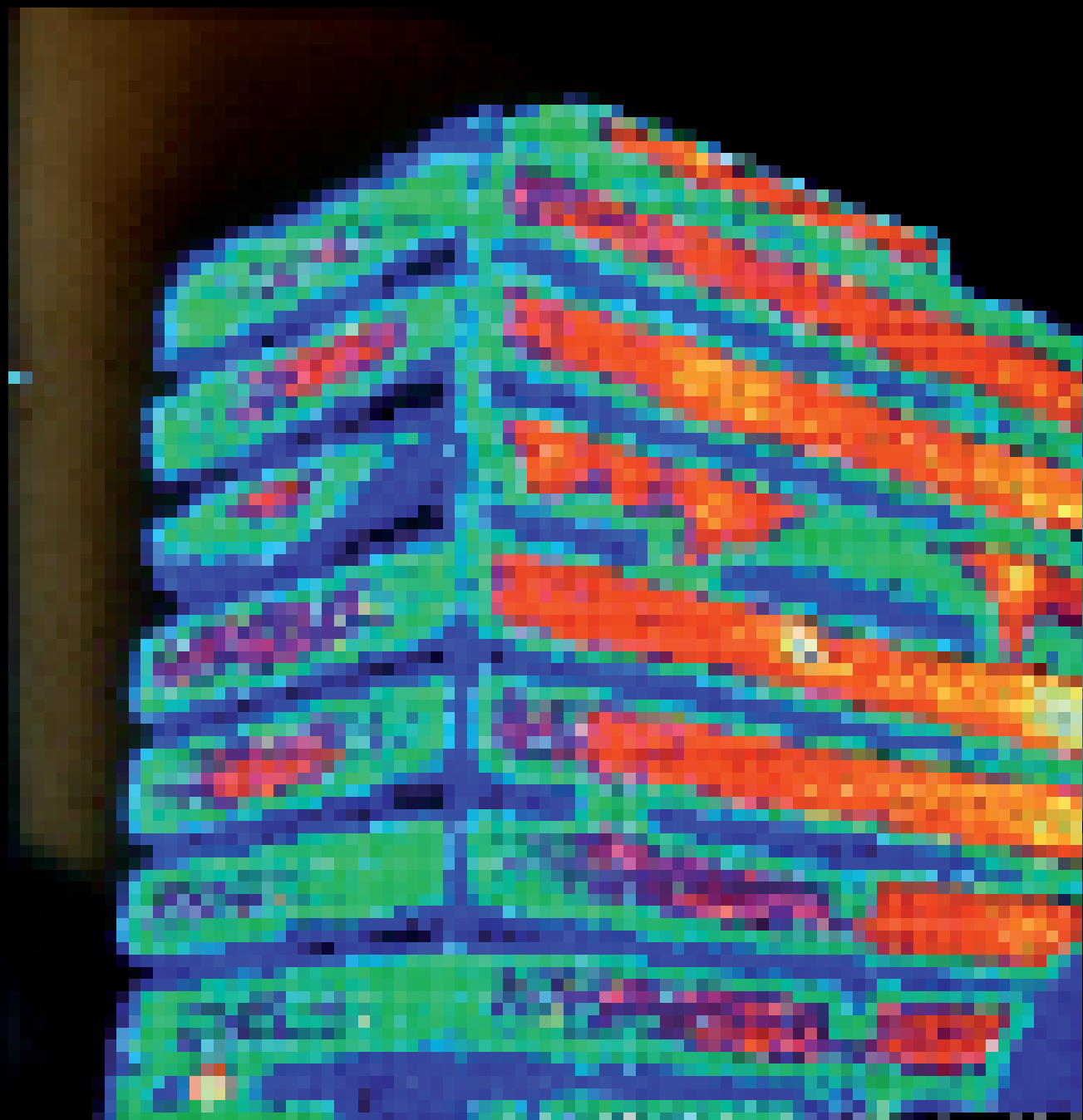
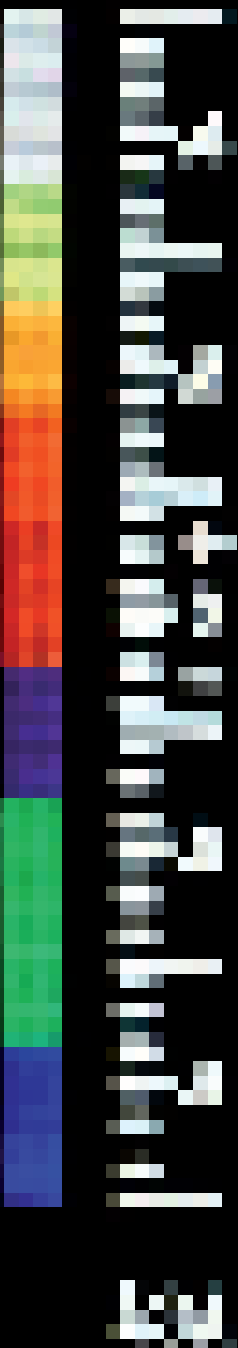
Er ist der eigentliche Big Brother, der – wenn er will – alles sieht. Auch mit spezieller Hardware können Chefs herausfinden, was ihre Mitarbeiter am Rechner treiben. Doch am umfassendsten ist die Überwachung durch Spy-Software. Sie registriert nicht nur jede Tastatureingabe, sondern macht zudem Screenshots, protokolliert die besuchten Webseiten, überwacht Chats und E-Mails und schlägt bei bestimmten Stichworten Alarm.

Womit kann man die Schnüffler ertappen?

Neugierigen Chefs auf die Schliche zu kommen ist nicht leicht. Am ehesten fällt Hardware auf. Doch manch verdächtiges Teil ist nur ein harmloser Adapter. Spyware verwischt ihre Spuren. Durchnummerierte Dokumente oder Aussetzer der Maus können Indizien für fragwürdige Aktivitäten sein, sagen Fachleute. Doch ohne technisches Know-how steht der Laie auf verlorenem Posten. Die Gefahr, falsche Dateien zu löschen, ist groß. Auch der Gegenangriff mit Software zur Enttarnung der Spione ist problematisch. Eine entsprechende Eigeninitiative kann den Job kosten. Angestellte ohne Administratorrechte kommen erst gar nicht in diese Gefahr, weil sie die Programme nicht installieren dürfen. Außerdem würde die Gegenseite das Manöver registrieren. Also: Konfrontation am besten vermeiden und mit offenen Karten spielen. 



DURCHSCHAUT Kontrolle ist besser, meinen immer mehr Chefs



Kreitz & Strunk in Kiel. Zu seinen Spezialgebieten gehören Arbeitsrecht und IT-Recht.

PLAYER: Inwieweit darf der Chef die Internetnutzung seiner Angestellten überwachen?

Jan A. Strunk: Wenn er privates Surfen duldet, darf er es nur dann individuell überwachen, wenn die Betroffenen vorher ihr Okay gegeben haben. Sogar bei einem konkreten Verdacht auf eine Straftat muss der Arbeitgeber vorab

Wie viel Bespitzelung müssen Arbeitnehmer sich gefallen lassen? Und wie können sie sich wehren? Darüber sprach PLAYER mit Jan Alexander Strunk, Rechtsanwalt in der Kanzlei Prof. Dr. Weiß,

ankündigen, dass er verschärft kontrollieren wird. Auch der Betriebsrat muss informiert sein. E-Mails darf der Chef keinesfalls lesen.

Und wenn der Chef heimlich späht - wie kann sich ein Arbeitnehmer dagegen wehren?

Er könnte den Arbeitgeber zunächst schriftlich um eine Stellungnahme und eventuell um Unterlassung bitten. Oder er wendet sich an den Betriebsrat. Der kann dafür sorgen, dass die Spielregeln in einer Betriebsvereinbarung festgehalten werden. Im Notfall ist auch eine Unterlassungsklage denkbar. Doch das sollte man sich wirklich zweimal überlegen.

Darf ein Mitarbeiter Anonymisierungs- bzw. Abwehrsoftware installieren?

Das hängt zunächst von seinen Benutzerrechten ab. Ist es ihm verboten, Software zu installieren, könnte er dafür abgemahnt oder sogar fristlos gekündigt werden. Gibt es das

Verbot nicht oder tarnt er die Aktion - etwa durch einen USB-Stick mit Anonymisierungsfunktion -, ist die Situation uneindeutig: Dem Interesse des Arbeitgebers an einer Kontrolle steht das Grundrecht des Arbeitnehmers, über seine personenbezogenen Daten zu bestimmen.

Droht auch dann schon Ärger, wenn man nur den Verlauf der Internetnutzung löscht?

Das kam so noch nicht vor. Und solange der Mitarbeiter sich an die vorgesehenen Möglichkeiten hält, sehe ich darin auch kein Problem. Im Grunde sammelt hier der Chef - unerlaubt oder zumindest ungefragt - automatisch Daten, die der Computernutzer zum Teil gar nicht bewusst aufgerufen oder heruntergeladen hat.