

INTERNET AM ARBEITSPLATZ

# Achtung: Kontrolle!



Dr. Elmar Weißnicht  
IHK Hannover  
Tel. (0511) 3107-506  
weissnicht@hannover.ihk.de

**Nutzen Beschäftigte das Internet im Unternehmen auch privat, geht nicht nur Arbeitszeit verloren: Bei Rechtsverstößen durch Mitarbeiter drohen dem Arbeitgeber auch unangenehme rechtliche Konsequenzen. Internetkontrollen schaffen Abhilfe, scheitern aber oft an rechtlichen Hürden.**

Noch schnell eine E-Mail an Freunde und Bekannte versenden, einen Beitrag im aktuellen Blog schreiben oder die in Kürze auslaufende Internetauktion mitverfolgen? Diese Liste privater Internetnutzung während der Arbeit ließe sich beliebig fortsetzen. Zur verlorenen Arbeitszeit kommt hinzu, dass die Beschäftigten die Sicherheit der Unternehmens-IT massiv gefährden, wenn sie die Anhänge unseriöser, privater E-Mails öffnen oder dubiose Websites aufrufen.

Schwerer noch wiegt der Umstand, wenn Arbeitnehmer das Internet rechtsmissbräuchlich verwenden, indem sie beispielsweise kinderpornografische Dateien herunterladen, rechtsextremistische Propaganda verbreiten oder Urheberrechte verletzen. Für derartige Vergehen kann ein Arbeitgeber unter Umständen straf- und/oder zivilrechtlich zur Verantwortung gezogen werden. Um dem vorzubeugen und um zu sicherzustellen, dass eventuell bestehende Nutzungsregeln seitens der Belegschaft auch tatsächlich eingehalten werden, tendieren viele Arbeitgeber dazu, die Internetaktivitäten ihrer Mitarbeiter zu überwachen. Die Technik setzt hier kaum Grenzen. Jegliche Nutzung des Internets hinterlässt Spuren, die mit entsprechender

Software nahezu vollständig – von den Mitarbeitern oft unbemerkt – ausgewertet werden können. Bereits die vom Browser angelegten Protokolldateien lassen Rückschlüsse auf das Surfverhalten zu. Daneben existieren spezielle Spionageprogramme. Filtersoftware ermöglicht es wiederum, E-Mails und Anhänge auf Virensignaturen und bestimmte Schlagwörter bzw. Kategorien (zum Beispiel Pornografie) systematisch zu durchsuchen, um sie im zweiten Schritt gegebenenfalls zu separieren. Auch kann der Zugang zu bestimmten Websites dadurch unterbunden werden.

Doch wie steht es um die Zulässigkeit solcher Kontrollen? Eine Antwort darauf liefert ein Blick auf das Datenschutz- und Telekommunikationsrecht. Ob sich der Arbeitgeber durch das manuelle Öffnen einer E-Mail Zugang zu deren Inhalt verschafft oder ob die Kontrolle mit Hilfe so genannter Content-Filter automatisiert erfolgt, spielt letztendlich keine Rolle: Grundsätzlich wird die Zulässigkeit der Internetkontrollen in Deutschland davon abhängig gemacht, ob die private Nutzung erlaubt ist oder ob das Internet im

Unternehmen ausschließlich für dienstliche Zwecke genutzt werden darf. Des Weiteren hängt die Intensität des Eingriffs grundsätzlich davon ab, ob lediglich die Verbindungsdaten (etwa E-Mail-Absender, Adressat, Versand – oder auch Empfangsuhrzeit und –datum) überwacht werden oder ob gar eine inhaltliche Kontrolle von E-Mails bzw. heruntergeladener Inhalte stattfindet. Letzteres wiegt in der Regel schwerer.

Beschäftigte haben grundsätzlich keinen Anspruch darauf, das Internet am Arbeitsplatz privat zu verwenden. Dem Arbeitgeber allein steht es zu, die private Nutzung zu erlauben, im Regelfall durch eine Klausel im Arbeitsvertrag oder durch eine Betriebsvereinbarung. Allerdings kann die Erlaubnis unter anderem auch durch so genannte „betriebliche Übung“ hergeleitet werden.

Besteht eine private Nutzungserlaubnis, schrumpft der legale Spielraum für eine Online-Überwachung auf ein Minimum: Durch die Erteilung der privaten Nutzungserlaubnis wird auch der „gewöhnliche“ Arbeitgeber nach nahezu einhelliger Meinung zum Telekommunikationsanbieter, der an die strengen Vorgaben des Fernmeldegeheimnisses nach § 88 Abs. 3 des Telekommunikationsgesetzes (TKG) gebunden ist. Wenngleich die Meinungen der Rechtsexperten in Bezug auf die konkreten Kontrollbefugnisse auseinandergehen, zeichnet sich doch ab, dass eine inhaltliche Kontrolle von E-Mails dann weitgehend ausgeschlossen ist und allenfalls im Ausnahmefall, zum Beispiel bei einem konkreten Verdacht auf Straftaten, gestattet ist. Ähnliches gilt für die Protokollierung der Verbindungsdaten.

Einen Ausweg bietet hier nur die Einwilligung eines jeden Mitarbeiters, die jedoch freiwillig erfolgen muss. Allerdings ist man sich

## Eine Erlaubnis für die private Nutzung lässt die Kontrollrechte schrumpfen.



Fotos: panthermedia

## MITARBEITERÜBERWACHUNG

## Seminar: Was darf der Arbeitgeber?

Die Überwachung von Mitarbeitern ist in der letzten Zeit verstärkt in den Mittelpunkt der Medienberichterstattung gerückt. Die Gründe, die Beschäftigten zu kontrollieren, können aus Sicht des Arbeitgebers - wie im vorliegenden Artikel beschrieben - durchaus vielfältig sein: Um einem Verdacht im Hinblick auf Korruption nachzugehen, zur Leistungskontrolle und um generell festzustellen, ob die Mitarbeiter ihren Arbeitspflichten nachkommen.

Oft sind derartige Überwachungsmaßnahmen allerdings nicht mit dem Gesetz vereinbar. Im Seminar am 19. Februar in Hannover wird deshalb die Zulässigkeit von Internetkontrollen und der Videoüberwachung (zum Beispiel durch Webcams) im Unternehmen erörtert. Auch wird auf die Kontrolle von Telefonaten, wie sie häufiger in Call-Centern praktiziert wird, eingegangen.

Die Veranstaltung richtet sich an Geschäftsführer, leitende Mitarbeiter, insbesondere IT-Verantwortliche, und an Mitarbeiter von Rechtsabteilungen.

**INFO:** Seminar am 19. Februar in der IHK Hannover. Die Teilnahme kostet 65 Euro zzgl. 19 % USt. (brutto 77,35 €). Referent ist Rechtsanwalt Thomas Feil, Hannover. Weitere Informationen und Anmeldung:

[www.begin.de/seminar](http://www.begin.de/seminar)

in Fachkreisen uneinig, ob neben dem Mitarbeiter auch der externe Kommunikationspartner - also derjenige, der etwa von außen eine (später kontrollierte) E-Mail an einen Mitarbeiter sendet - in die Überwachung ebenfalls einwilligen müsste. Ein vergleichbares Bild ergibt sich bei der Protokollierung der Internetseiten. Auch hier greifen die strengen Vorgaben des Fernmeldegeheimnisses.

Probleme bereitet zudem die so genannte Mischnutzung. Ist eine Trennung zwischen privater und dienstlicher Kommunikation nicht möglich, weil etwa keine separaten privaten und dienstlichen E-Mail-Accounts existieren, ist nicht klar, ob in dem Fall sämtliche, das heißt auch geschäftliche E-Mails, den strengen Vorgaben des § 88 Abs. 3 TKG unterliegen.

Ist ausschließlich die dienstliche Nutzung erlaubt, zeichnet sich ein ganz anderes Bild ab: Das Fernmeldegeheimnis ist nicht anwendbar; die Zulässigkeit der Internetkontrollen richtet sich stattdessen nach dem Allgemeinen Persönlichkeitsrecht und dem Bundesdatenschutzgesetz (BDSG). Danach wäre eine Kontrolle zulässig, wenn die Voraussetzungen des § 4 Abs. 1 BDSG vorliegen. Das bedeutet, dass der Mitarbeiter in die Kontrolle eingewilligt haben muss oder dass optional eine „andere Rechtsvorschrift“, zum Beispiel eine Betriebsvereinbarung, die Internetüberwachung legitimiert. Als dritte Alternative verbleibt nach § 4 Abs. 1 BDSG, dass eine Vorschrift des BDSG selbst die Kontrollmaßnahmen gestattet. Heranzuziehen ist hier der durch die Novellierung des BDSG neu eingeführte § 32 BDSG. Nach dessen Abs. 1 ist die Kontrolle zulässig, wenn sie unter anderem für die Durchführung des Arbeitsverhältnisses erforderlich ist. Es ist jedoch davon auszugehen, dass dabei weiterhin auf die hinsichtlich des § 28 BDSG entwickelten Grundsätze zurückzugreifen ist, wonach dem Arbeitgeber insgesamt deutlich größere Kontrollrechte als bei der erlaubten privaten Nutzung zugestanden werden. Allerdings ist auch hier streitig, ob dies auch eine inhaltliche Überwachung von E-Mails bzw. heruntergeladener Dateien einschließt.

In jedem Fall muss der Arbeitgeber darüber hinaus die Mitbestimmungsrechte des Betriebsrates (sofern ein solcher besteht) beachten. Zwar ist das Verbot einer privaten Nutzung mitbestimmungsfrei. Beabsichtigt der Arbeitgeber allerdings Filterprogramme oder sonstige „technische Einrichtungen“ einzuführen oder anzuwenden, die zur Überwachung objektiv geeignet sind, hat der Betriebsrat insbesondere ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 des Betriebsverfassungsgesetzes (BetrVG).

Was aber passiert, wenn sich die Arbeitsparteien nicht an die gesetzlichen Vorgaben halten? Nutzen Arbeitnehmer das Internet trotz Verbotes für private Zwecke oder missachten sie etwaige Nutzungsbeschränkungen oder Richtlinien in diesem Zusammenhang, drohen arbeitsrechtliche Folgen. Die hohe Zahl gerichtlicher Auseinandersetzungen belegt die Relevanz des Themas. Neben einer Abmahnung ist in schweren Fällen eine Kündigung oder sogar eine fristlose Kündigung ohne vorherige Abmahnung durchaus



gerechtfertigt, was das Bundesarbeitsgericht (BAG) in mehreren Entscheidungen bereits bestätigt hat.

Kontrolliert der Arbeitgeber die Internetaktivitäten seiner Mitarbeiter, obschon bestehende Gesetze dem entgegenstehen, kann er die dadurch gewonnenen Daten nicht in einem möglichen Kündigungsschutzprozess verwerten. Erfolgen die Kontrollen unter Verletzung des Fernmeldegeheimnisses, droht ihm unter Umständen ein Strafverfahren nach § 206 Strafgesetzbuch (StGB), der das Fernmeldegeheimnis strafrechtlich schützt.

Ist die private Nutzung des Internet im Unternehmen erlaubt, ist eine rechtmäßige Kontrolle seitens des Arbeitgebers nahezu ausgeschlossen.

Hinzu kommt, dass sich

die Rechtsexperten in vielen Fragen rund um die Internetkontrolle uneinig sind und dass sich die Gerichte - zu Lasten der Rechtssicherheit - zur datenschutzrechtlichen Zulässigkeit derartiger Internetkontrollen (soweit erkennbar) bislang nicht geäußert haben. Aus rechtlichen Gründen ist daher ein privates Nutzungsverbot des Internet am Arbeitsplatz aus Sicht des Arbeitgebers naheliegend. Dass ein solches Totalverbot andererseits die Arbeitsmotivation, gerade bei überobligatorisch arbeitenden Mitarbeitern, torpedieren kann, soll nicht unerwähnt bleiben.

### Rechtswidrig gewonnene Daten lassen sich vor Gericht nicht verwenden.

Anzeige

#### Datenschutzseminar

Hannover (25.01. - 29.01.)

Bielefeld (01.02. - 05.02.)

Fachkundenachweis f.

Datenschutzbeauftragte,

Schulung f. Führungskräfte

und Mitarbeiter

ALLE BRANCHEN

Kedua GmbH



[www.datenschutzexperten.de](http://www.datenschutzexperten.de)

Tel 030 43 77 86 25

Alle Trainer sind aktive  
Datenschutzbeauftragte