



Die Regeln der Überwachung

Ein wesentlicher Aspekt des Netzwerk-Monitorings ist auch die Überwachung der User in Unternehmen. Doch wie viel Überwachung ist erlaubt, und wie ist dabei vorzugehen?

VON UELI GRÜTER

Schon vor der Einführung der Informatik und insbesondere des Internets durften die Mitarbeiter eines Unternehmens überhaupt nicht oder sicher nicht den ganzen Tag am Arbeitsplatz Zeitung lesen oder mit Freunden telefonieren. Mindestens in Grossraumbüros war das Verhalten der Mitarbeiter leicht zu überwachen. Mit der Einführung der Informatik verschmolzen die Mittel für diese persönlichen Tätigkeiten mit den Arbeitswerkzeugen, die klare Trennung zwischen privater und geschäftlicher Tätigkeit aufgehoben. Und dadurch, dass nun alles im Netz

läuft, ist vieles – etwa die Tätigkeiten der Mitarbeiter, aber auch die Kontrolle derselben durch den Arbeitgeber – nicht mehr offensichtlich.

Für die rechtliche Beurteilung des Netzwerk-Monitorings in den Unternehmen und für vernünftige Regelungen ist das Bewusstsein dieser Veränderung in der Arbeitswelt wichtig. Die Verunsicherung durch den Einsatz von Informatik darf nicht zur Überreaktion führen, jedoch muss man sich der Problematik des technischen Umfelds im klaren sein.

Missbrauch der Informatik

Von einem Missbrauch der Informatik durch Mitarbeiter ist dann auszugehen, wenn die entsprechende Nutzung den Arbeitgeber schädigt. Wann dies der Fall ist, ist keine juristische Frage, sondern eine Frage der Informatik und der Unternehmensorganisation. Ein Schaden kann dem Unternehmen insbesondere durch eine Übernutzung der Systeme, durch die Schädigung der Systeme zum Beispiel durch das fahrlässige Herunterladen von Viren und Würmern, aber auch durch den Verlust von produktiver Arbeitszeit entstehen. Der Ruf des Unternehmens nimmt Schaden durch den Versand von E-Mails über einen Unternehmens-Account mit widerrechtlichen Inhalten oder mit Inhalten, die der Ansicht des Unternehmens zuwider laufen, sowie durch entsprechende Publikationen über die IP-Nummer des Unternehmens.

Zuerst Massnahmen, erst dann Überwachung

Auch beim Netzwerk-Monitoring gilt das Prinzip der Verhältnismässigkeit. Das bedeutet, dass nur Massnahmen getroffen werden dürfen, die notwendig und geeignet sind. Zudem ist bezüglich der Mitarbeiter dasjenige Mittel zur Abwendung von Schaden zu wählen, das am wenigsten in deren persönliche Freiheiten eingreift.



UELI GRÜTER, LL.M., IST RECHTSANWALT IN ZÜRICH UND LUZERN UND DOZENT AN DER HOCHSCHULE LUZERN MIT SPEZIALGEBIET KOMMUNIKATIONS- UND TECHNOLOGIERECHT. ER SCHARFT MIT SEINEN REGELMÄSSIGEN BEITRÄGEN AUS THEORIE UND PRAXIS DIE RECHTLICHE SICHT AUF DIE SCHWERPUNKTTHEMEN DES SWISS IT MAGAZINE.

IN KÜRZE

Eines der heissesten Themen des Netzwerk-Monitorings ist die Überwachung der User und deren Verhalten, insbesondere in Unternehmen. Diese ergreifen in letzter Zeit immer drastischere Massnahmen und sperren Seiten wie Facebook und Co. Obwohl der Arbeitgeber vor einer Sperre zuerst alle anderen, weniger einschneidenden Massnahmen ergreifen muss, kann er aufgrund seines gesetzlichen Weisungsrechts auch die Nutzung der Informatik und insbesondere des Internets einschränken. Auch die Überwachung der Informatiknutzung ist zulässig. Eine personenbezogene Auswertung der Protokollierung darf jedoch nur bei Verdacht auf Missbrauch und einer vorgängigen Information der Mitarbeiter erfolgen. Die geschieht am besten im Rahmen eines Nutzungs-, Kommunikations- und Überwachungsreglements für die Informatik.

Konkret heisst das, dass Unternehmen zur Verhinderung des Missbrauchs der Informatik durch ihre Mitarbeiter zuerst alle möglichen, ökonomisch vertretbaren technischen und organisatorischen Massnahmen treffen müssen, bevor die Informatik-Nutzung der Mitarbeiter zu diesem Zweck überwacht werden darf. Zu diesen technischen Massnahmen gehören die bereits üblichen Firewalls, Antiviren-Programme, aber auch die Verwendung von Passwörtern für den Zugang zu den Systemen. Zusätzlich möglich wäre, dass ein Unternehmen seinen Mitarbeitern neben dem Informationssystem für die Geschäftskommunikation ein separates für die persönliche Kommunikation zur Verfügung stellt. Da die Mitarbeiter jedoch für ihre persönliche Kommunikation zunehmend eigene Geräte wie Smartphones zur Arbeit mitbringen und diese auch unabhängig von der Unternehmensinfrastruktur nützen, entschärft sich möglicherweise die technische Gefahr einer Schädigung der unternehmenseigenen Informatikinfrastruktur durch die Internet-Kommunikation beträchtlich.

Zunehmend notwendig wird damit aber die generelle Regelung der Kommunikation im Unternehmen, vor allem der persönlichen.

Grundlage der Regelung bilden die rechtlichen Leitplanken. Geregelt wird die Kommunikation in einem unternehmenseigenen Kommunikationsreglement.

Einschränkung der Informatik-Nutzung

Der Arbeitgeber hat gegenüber dem Arbeitnehmer ein sogenanntes Weisungsrecht (Art. 321d Obligationenrecht, OR). Aufgrund dieses Rechts kann der Arbeitgeber gegenüber seinen Mitarbeitern die Art und Weise, wie eine Arbeit erledigt werden muss, vorschreiben, sowie weitere, die Arbeit betreffende Weisungen erlassen. Dabei ist er rechtlich gesehen grundsätzlich frei. Nach Treu und Glauben dürfen solche Vorschriften jedoch nicht unsinnig und schikanös sein.

Im Rahmen seines Weisungsrechts kann der Arbeitgeber auch die Nutzung der Informatik im Unternehmen und die persönliche Kommunikation regulieren. So kann er beispielsweise die Nutzung des Internets oder gewisser Inhalte (z.B. Facebook) einschränken und dies auch technisch durchsetzen.

Andererseits hat der Mitarbeiter gegenüber seinem Arbeitgeber eine Sorgfalts- und eine Treuepflicht (Art. 321a OR). Damit darf er die Informatik des Arbeitgebers – insbesondere das Internet – nur in einem Ausmass und in einer Art und Weise nutzen, die dem Arbeitgeber nicht schadet.

Um das Weisungsrecht des Arbeitgebers und die Sorgfalts- und Treuepflicht der Mitarbeiter unter einen Hut zu kriegen, empfiehlt sich, die Nutzung der Informatik – inklusive des Internets – im Rahmen eines Nutzungs- und Kommunikationsreglements für alle klar und verständlich festzulegen.

Rechtliche Leitplanken des Netzwerk-Monitorings

Schon immer gab es offenbar ein gewisses Misstrauen der Arbeitgeber gegenüber ihren Mitarbeitern. Seit es die entsprechende Möglichkeit gegeben hat, haben einige Arbeitgeber auch sogleich begonnen, ihre Mitarbeiter elektronisch zu überwachen. Dies veranlasste die Politik, entsprechende Regeln zum Schutz der Arbeitnehmer gegen die Verhaltensüber-

wachung in einer Verordnung zum Arbeitsgesetz festzuschreiben. So ist es dem Arbeitgeber grundsätzlich verboten, Überwachungs- und Kontrollsysteme einzusetzen, die das Verhalten der Mitarbeiter am Arbeitsplatz überwachen (Art. 26 ArGV 3). Zudem schreibt Art. 328b OR explizit vor, dass bei der Sammlung und Verarbeitung von Daten über Mitarbeiter der Grundsatz der Verhältnismässigkeit eingehalten werden muss. Das bedeutet, dass Daten über Mitarbeiter nur so weit erhoben und bearbeitet werden dürfen, als dies für die Durchführung des Arbeitsvertrages notwendig und geeignet ist. Schlussendlich haben Mitarbeiter jederzeit das Recht, beim Arbeitgeber Auskunft über die Sammlung und Verarbeitung von Daten über ihre Person zu verlangen (Art. 8 Datenschutzgesetz, DSG).

Legales Netzwerk-Monitoring

Aufgrund der rechtlichen Leitplanken darf ein Netzwerk-Monitoring grundsätzlich ohne Einschränkung durchgeführt werden, solange garantiert werden kann, dass keine personenbezogene Auswertung erfolgt – sprich von den erhobenen technischen Daten kein Bezug zu den einzelnen Mitarbeitern gemacht wird. Weil letzteres jedoch schwierig garantiert werden kann und je nach Motivation des Netzwerk-Monitorings auch keinen Sinn macht, sollte in der Praxis nur ein reglementiertes und kontrolliertes Netzwerk-Monitoring mit der Möglichkeit einer personenbezogenen Auswertung durchgeführt werden.

Dabei muss vor allem auch die Auswertung der Protokollierungen definiert werden. Man geht von drei Arten von Auswertungen aus: der anonymen, der pseudonymen und der personenbezogenen beziehungsweise namentlichen Auswertung. Bei einer anonymisierten Auswertung werden die protokollierten Daten nur statistisch analysiert. So wird zum Beispiel erhoben, welche Internet-Seiten von den Mitarbeitern am meisten besucht werden oder wie viele E-Mails pro Tag über den Unternehmens-Account versendet werden. Es gibt also keinen Bezug zu den einzelnen Mitarbeitern. Eine anonymisierte Auswertung ist aber nur möglich, wenn die Mitarbeiterzahl genügend gross ist. Bei der pseudonymen Auswertung wird ein Bezug zu den einzelnen Mitarbeitern als User eines Netzwerks gemacht. Die Mitarbeiter erhalten jedoch lediglich ein Pseudonym. Solange dieses Pseudonym nicht geknackt wird, handelt es sich auch bei dieser Methode um eine anonyme Protokoll-Auswertung. Damit muss hier vor allem auch auf ein stabiles Pseudonym

geachtet werden. Und letztlich gibt es die personenbezogene beziehungsweise namentliche Auswertung, bei der ein effektiver Bezug zu den einzelnen Mitarbeitern gemacht wird. Die personenbezogene beziehungsweise namentliche Auswertung von Netzwerk-Protokollen ist nur zulässig, wenn eine anonymisierte oder eine pseudonymisierte Auswertung ergibt, dass ein Missbrauch der Unternehmens-Infrastruktur erfolgt ist. Ausserdem müssen die Mitarbeiter vor der Auswertung generell in einem Überwachungsreglement über eine mögliche namentliche Auswertung bei Missbrauch informiert worden sein.

Werden bei der anonymisierten beziehungsweise pseudonymisierten Auswertung Straftatbestände (z.B. das Herunterladen von verbotenem pornografischem Material, Ehrverletzung) festgestellt, ist zu empfehlen, umgehend die Strafbehörden zu informieren; nicht zuletzt um zu verhindern, dass der Arbeitgeber der Mittäterschaft bezichtigt wird.

Nutzungs-, Kommunikations- und Überwachungsreglement

Die Erfahrung zeigt, dass Schriftlichkeit im Arbeitsverhältnis viel zur Klarheit und zur Streitprävention beiträgt. So ist es auch bei der Nutzung der Informatik und der persönlichen Kommunikation durch die Mitarbeiter und deren Überwachung durch den Arbeitgeber. Damit empfiehlt sich im Unternehmen ein Nutzungs-, Kommunikations- und Überwachungsreglement für die Informatik, das die Rechte und Pflichten der Mitarbeiter und des Arbeitgebers so detailliert wie möglich regelt. Soll eine namentliche Auswertung von Protokollaten erfolgen, ist das Überwachungsreglement wie erwähnt sogar zwingend zu erlassen.

Löschung der Daten nicht vergessen

Viel Aufsehen gibt es im Datenschutz bekanntlich vor allem bezüglich der Erhebung und Verarbeitung von Daten. Was dabei jedoch häufig vergessen wird ist die Löschung dieser Daten. Löschung im Rechtssinne heisst nicht einfach, die «Delete»-Taste zu drücken, sondern die Daten unwiederbringlich zu vernichten. Der eidgenössische Datenschutzbeauftragte empfiehlt, Protokollaten nach rund einem Monat zu löschen. Dabei ist auch an die Backups zu denken. Da eine Löschung in den Backups oft schwierig ist, empfiehlt es sich, gewisse Protokollierungen entweder überhaupt nicht in das Backup einzubeziehen oder zumindest separat zu sichern. ■

WEITERE INFOS ZUM THEMA

Zusätzliche Infos zum Thema Überwachung am Arbeitsplatz finden sich unter anderem auf der Website des eidgenössischen Datenschutzbeauftragten (www.edoeb.admin.ch).