Blickpunkt Management

Zu Kapitel 7: Überwachung von Angestellten im Netz – sittenwidrig oder gut?

Wie viele Minuten (oder Stunden) haben Sie heute auf der Arbeit mit Facebook verbracht? Vielleicht haben Sie ja auch persönliche E-Mails verschickt oder einige Sport-Websites besucht? Wenn ja, dann sind Sie nicht allein. Gemäß einer von Nucleus Research durchgeführten Studie nutzen 77 Prozent aller Mitarbeiter mit Facebook-Konto dieses soziale Netz auch während der Arbeit. Einer Studie von Ponemon Institute zufolge verbringt der durchschnittliche Mitarbeiter 30 Prozent seiner Arbeitszeit mit nicht arbeitsbezogenem Surfen im Internet, während andere Untersuchungen ergeben, dass fast 90 Prozent der Angestellten private E-Mails auf der Arbeit empfangen oder verschicken.

Dieses Verhalten verursacht ernsthafte wirtschaftliche Probleme. Das Lesen von E-Mails, das Beantworten von Instant Messages oder das kurze Reinschauen in ein YouTube-Video führen zu einer Reihe von endlosen Unterbrechungen, die den Mitarbeiter von seiner Arbeit ablenken. Laut Basex, einem New Yorker Marktforschungsinstitut, führen diese Ablenkungen jedes Jahr zu einem Produktivitätsverlust in Höhe von 650 Milliarden US-Dollar.

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter zu überwachen, manchmal sogar ohne deren Wissen, um zu sehen, ob sie auf der Arbeit ihre private E-Mail-Korrespondenz erledigen und das Internet für private Zwecke nutzen. Eine Untersuchung von Proofpoint Plus aus dem Jahre 2010 stellte fest, dass mehr als jeder dritte große US-Konzern Mitarbeiter dafür abstellt, die E-Mails der Kollegen zu lesen oder zu analysieren. Eine weitere aktuelle Umfrage der American Management Association (AMA) und des ePolicy Institute ergab, dass zwei Drittel der befragten kleineren, mittleren und großen Unternehmen die Webnutzung ihrer Angestellten kontrollierten. Die Überwachung von Instant Messaging und Textnachrichten nimmt ebenfalls zu. Und obwohl US-Unternehmen legal die Internet- und E-Mail-Aktivitäten ihrer Mitarbeiter bei der Arbeit überwachen dürfen, stellt sich die Frage ob ein solches Verhalten sittenwidrig oder einfach gut ist.

Manager machen sich Gedanken über den Verlust an Arbeitszeit und Mitarbeiterproduktivität, wenn die Mitarbeiter die digitalen Medien verstärkt für private Zwecke nutzen, anstatt ihrer Firmentätigkeit nachzugehen. Zu viel Zeit für Privates führt zu Umsatzeinbußen. Einige Mitarbeiter stellen den Kunden unter Umständen sogar Zeit in Rechnung, die sie privat online sind, und berechnen damit dem Kunden zu viel.

Wird der private Datenverkehr auf dem Unternehmensnetz zu hoch, kann er das Unternehmensnetz verstopfen, sodass der eigentlichen Unternehmenstätigkeit nicht mehr nachgegangen werden kann. Procter & Gamble (P&G) haben festgestellt, dass die Mitarbeiter an einem durchschnittlichen Tag 4.000 Stunden Musik auf Pandora hören und sich 50.000 Fünf-Minuten-Videos auf YouTube anschauen. Das bedeutet, dass über das unternehmensinterne Netz riesige private Datenmengen gestreamt wurden und folglich die Übertragungsgeschwindigkeit aller Daten bei P&G beeinträchtigt wurde.

Wenn Mitarbeiter E-Mail oder Web (einschließlich soziale Netzwerke) am Arbeitsplatz oder auf den Geräten des Arbeitgebers nutzen, erfolgt diese Nutzung, auch wenn sie illegal sein sollte, im Namen des Unternehmens. Das heißt, illegale Aktivitäten können zum Arbeitgeber zurückverfolgt werden, der dann dafür zur Verantwortung gezogen werden kann. Wenn zum Beispiel Mitarbeiter auf eindeutig pornografische, rassistische oder anderweitig beleidigende Inhalte zugreifen oder diese tauschen, könnte das, so die Furcht vieler Manager, Negativschlagzeilen für das Unternehmen bedeuten oder sogar rechtliche Konsequenzen haben. Auch wenn irgendwann festgestellt wird, dass das Unternehmen nicht haftbar ist, können die Kosten für die Anfechtung solcher Klagen erheblich sein. Symantec behauptet in seinem 2011 Social Media Protection Flash Poll, dass sich die durchschnittlichen Prozesskosten eines Unternehmens mit Social-Media-Vorfällen auf über 650.000 US-Dollar belaufen.

Außerdem könnten über E-Mail oder soziale Netzwerke, so die Furcht vieler Unternehmen, vertrauliche Informationen und Betriebsgeheimnisse ausgeplaudert werden. Eine weitere Umfrage von der American Management Association und dem ePolicy Institute ergab, dass 14 Prozent der befragten Mitarbeiter zugab, schon einmal vertrauliche oder potenziell peinliche E-Mails

▶ Forts.

aus dem Unternehmen an Außenstehende geschickt zu haben.

US-Unternehmen haben das Recht, das Verhalten der Mitarbeiter bei der Nutzung firmeneigener Computer zu überwachen. Die Frage bleibt jedoch, ob die elektronische Überwachung ein geeignetes Mittel ist, um eine effiziente und positive Arbeitsatmosphäre zu schaffen. Einige Unternehmen gehen so weit, dass sie sämtliche privaten Aktivitäten in den Unternehmensnetzen verbieten – Nulltoleranz. Andere sperren den Zugriff der Mitarbeiter auf bestimmte Websites oder soziale Sites, kontrollieren alle E-Mails oder beschränken die privat im Web verbrachte Zeit.

So hat zum Beispiel P&G die Netflix-Site gesperrt und seine Mitarbeiter aufgefordert, die Nutzung von Pandora zu beschränken. YouTube-Videos dürfen im vertretbaren Rahmen betrachtet werden und auch der Zugriff auf soziale Netzwerke ist frei, da die Mitarbeiter diese für digitale Marketing-Kampagnen nutzen. Ajax Boiler in Santa Ana, Kalifornien, verwendet Software von SpectorSoft Corporation, die aufzeichnet, welche Websites von den Mitarbeitern aufgerufen werden, wie viel Zeit sie auf den jeweiligen Websites verbringen und was sie in ihren E-Mails schreiben. Der Finanz- und Investitionsdienstleister Wedbush Securities kontrolliert bei seinen über 1.000 Mitarbeitern die täglichen E-Mails, die Instant Messages und die Aktivitäten in den sozialen Netzen. Die E-Mail-Überwachungssoftware dieser Firma markiert bestimmte Arten von Nachrichten und Schlüsselwörter in Nachrichten zur näheren Untersuchung.

Eine Reihe von Firmen haben Mitarbeiter entlassen, weil diese sich nicht an die Firmenrichtlinien gehalten haben. Eine Proofpoint-Umfrage ergab, dass jedes fünfte große US-Unternehmen im letzten Jahr einen Mitarbeiter entlassen hat, weil er die Firmenrichtlinien zur Nutzung von E-Mail verletzt hatte. Manager, die Mitarbeiter wegen Internetmissbrauch entlassen mussten, begründeten dies größtenteils damit, dass die E-Mails der Mitarbeiter sensible, vertrauliche oder heikle Informationen enthielten.

Keine dieser Lösungen ist perfekt, aber viele Unternehmensberater empfehlen, Richtlinien aufzusetzen, die die Nutzung von E-Mail, Web und soziale Medien am Arbeitsplatz regeln. Diese Richtlinien sollten Grundregeln enthalten, die nach Position oder Stellung eindeutig festlegen, unter welchen Umständen Mitarbeiter die firmeneigenen Computer zum Schreiben von E-Mails, Bloggen oder Surfen im Internet nutzen darf. Die Richtlinien sollten die Mitarbeiter auch darüber informieren, ob diese Aktivitäten überwacht werden, und erläutern warum.

IBM hat bei sich „Social Computing Guidelines“ eingeführt, die Vorgaben für die Aktivitäten der Mitarbeiter auf Sites wie Facebook und Twitter macht. Diese Richtlinien halten die Mitarbeiter dazu an, ihre Identität nicht zu verbergen, sich immer bewusst zu sein, dass sie persönlich für alles verantwortlich sind, was sie preisgeben, und keine kontroversen Themen zu diskutieren, die nichts mit ihrer Rolle im Unternehmen zu tun haben.

Die Regeln sollten auf die speziellen Organisationskulturen und Bedürfnisse der einzelnen Unternehmen zugeschnitten sein. Eine Investment-Firma wird sicherlich vielen seiner Mitarbeiter Zugriff auf andere Investment-Sites gewähren. Und ein Unternehmen, das auf regen Informationsaustausch, Innovation und Unabhängigkeit angewiesen ist, könnte schnell merken, dass es sich mit der Überwachung mehr Probleme einhandelt, als es löst.

Quellen: Emily Glazer, „P&G Curbs Employees' Internet Use“, The Wall Street Journal, 4. April 2012; David L. Barron, „Social Media: Frontier for Employee Disputes“, Baseline, 19. Januar 2012; Jennifer Lawinski, „Social Media Costs Companies Bigtime“, Baseline, 29. August 2011; Don Reisinger, „March Madness: The Great Productivity Killer“, CIO Insight, 18. März 2011; „Seven Employee Monitoring Tips for Small Business“, IT BusinessEdge, 29. Mai 2011; Catey Hill, „Things Your Boss Won't Tell You“, Smart Money, 12. Januar 2011.

FRAGEN ZUR FALLSTUDIE

1. Sollten Manager die E-Mail- und Internetnutzung ihrer Mitarbeiter überwachen? Warum beziehungsweise warum nicht?
2. Beschreiben Sie eine effektive Firmenrichtlinie für E-Mail- und Webnutzung.
3. Sollten Manager die Mitarbeiter darüber informieren, dass ihr Webverkehr überwacht wird? Oder sollten Manager ihre Mitarbeiter heimlich ausspionieren? Warum beziehungsweise warum nicht?