

Rechtsgutachten zur Internetnutzung am Arbeitsplatz

Symantec Switzerland AG
Flugplatzstrasse 5 • CH-8404 Winterthur
Home Page : www.symantec.ch
Tel: (052) 244 • 39 • 39 • 0
Fax: (052) 244 • 39 • 99

SYMANTEC.

Was ist zulässig?
Wie vorgehen?
Wie organisieren?

SYMANTEC.

In Zusammenarbeit mit David Rosenthal und SYMANTEC Switzerland AG.

Executive Summary	2
Einleitung	3
Gesetzliche Grundlagen	3
Prävention	4
Organisatorische und rechtliche Massnahmen	4
Technische Massnahmen	5
Speicherung und Überwachung	6
Unpersönliche Daten	6
Missbrauchsfälle	7
Andere Gründe	8
Hinweise für Provider	9
Weitere Fragen?	9

Executive Summary

Die Überwachung und Kontrolle der Internet- und E-Mail-Aktivitäten der Mitarbeiter ist grundsätzlich zulässig, doch müssen dabei von Gesetzes wegen (vor allem Datenschutzgesetz und Arbeitsrecht) gewisse Regeln eingehalten werden. Es gilt im Grunde dasselbe wie für die Überwachung von Telefonaten der Angestellten.

Diese Regeln sollen die Interessen des Arbeitgebers wahren, aber ebenso die Privatsphäre der Mitarbeiter schützen und unnötigen Stress durch Überwachungen verhindern. Eine Verhaltenskontrolle ist daher verboten, eine Leistungskontrolle dagegen zulässig. Grundsätzlich müssen jeweils die Interessen der Arbeitgeber mit jenen der Arbeitnehmer abgewogen werden.

Die Überwachung oder Auswertung von Internet- und E-Mail-Daten von einzelnen Mitarbeitern muss daher

sich auf konkrete Verdachtsmomente eines Missbrauchs stützen,
vorher angekündigt bzw. angedroht werden,
auf das nötige Mindestmass beschränkt werden (z.B. Stichproben) und
vertraulich erfolgen.

Liegt eine Straftat vor, braucht eine Überwachung nicht vorher angekündigt zu werden, doch sind stattdessen die Strafverfolgungsbehörden einzuschalten.

Sofern sich Überwachungsmaßnahmen oder Auswertungen nicht auf bestimmte oder bestimmbar Personen beziehen, sind sie ohne weiteres zulässig. Anonymisierte Statistiken des Internet-Verkehrs sind erlaubt (z. B. um generell festzustellen, ob es im Betrieb zu Missbräuchen kommt), ebenso sind es Aufzeichnungen aus Sicherheitsgründen, zur Systemwartung oder zur Leistungsabrechnung.

Erlaubt ist grundsätzlich auch die Überwachung von geschäftlichen E-Mails, die über nicht personenbezogene E-Mail-Adressen abgewickelt werden, sofern nicht das Verhalten der einzelnen Arbeitnehmer kontrolliert wird. Dagegen dürfen persönliche Postfächer nur unter den genannten Bedingungen überwacht werden, weil mit privater Post zu rechnen ist.

Der Arbeitgeber hat aber das Recht, seinen Angestellten vorzuschreiben, ob und wie sie das Internet, E-Mails und andere Angebote wie etwa Diskussionsforen benutzen dürfen. Er kann eine private Nutzung des Internets und von E-Mails verbieten (genauso wie er Privattelefonate untersagen kann). Ohne weiteres erlaubt ist auch der Einsatz von Scannern (z. B. gegen Viren). Wichtig ist, dass die Benutzer darüber informiert sind, der Vorgang vollautomatisch abläuft (d. h. ohne menschlichen Eingriff) und Protokolle nicht personenbezogen ausgewertet werden.

Schliesslich hat der Arbeitgeber dafür zu sorgen, dass überall dort, wo Daten von bestimmten oder bestimmbar Personen aufgezeichnet werden, diese gegen unbefugte Zugriffe geschützt sind. Dabei sollte der Zugriff auf Logbuch- und E-Mail-Daten genau geregelt und auf ein Mindestmass beschränkt werden.

Einleitung

Das Internet und speziell die elektronische Post ist in vielen Betrieben ein unverzichtbares Arbeitsmittel geworden. Richtig eingesetzt steigert es die Produktivität und ermöglicht den Zugang zu Informationen, die bisher nicht verfügbar waren. Doch diese neuen Techniken bergen auch etliche Risiken: Die Mitarbeiter können sie für private Zwecke nutzen, sie erledigen ihre Arbeit deswegen womöglich nicht mehr oder gefährden den Betrieb durch das Einschleusen von Viren und Würmern.

Ist ein Betrieb gross, gibt es immer auch Mitarbeiter, die sich nicht an vorgegebene Regeln halten, die Pornografie und andere verbotene Inhalte konsumieren oder verbreiten und damit sogar andere belasten oder E-Mails mit unzulässigen Inhalten versenden. Das kann nicht nur störend und Imageschädigend sein, sondern durchaus auch zur Haftung des betreffenden Unternehmens führen. Aus diesem Grund entsteht in den meisten mittleren und grösseren Betrieben früher oder später das Bedürfnis, den Einsatz des Internets inklusive elektronischer Post auf die eine oder andere Weise zu beschränken, zu überwachen und die nötigen Informationen zu sammeln, um im Falle von Missbräuchen gegen die Schuldigen vorgehen zu können.

Es ist jedoch wichtig, dass sich ein Arbeitgeber an das geltende Recht hält. Das ist nicht immer einfach: die Regeln sind von Land zu Land verschieden. In den USA haben Arbeitgeber zum Beispiel mehr oder weniger freie Hand bei der Überwachung ihrer Mitarbeiter. In Europa und speziell in der Schweiz ist der Gesetzgeber restriktiver, indem er die Privatsphäre, die Persönlichkeit und das Wohlbefinden des Arbeitnehmers in diesem Bereich explizit schützt.

Davon profitiert der Arbeitgeber indirekt zwar ebenso. Dies heisst aber auch, dass der Arbeitgeber, der Internet-Aktivitäten im Betrieb überwachen und gegen Missbräuche vorgehen will, sich dabei an bestimmte Regeln und Prozeduren halten muss. Das hat durchaus auch eigennützige Gründe: Sollte es trotz allem zu einem Rechtsstreit kommen, wäre es unangenehm, wenn Beweismaterial gegen einen fehlerhaften Mitarbeiter nicht benutzt werden könnte, weil es unrechtmässig beschafft wurde. Es ist sogar denkbar, dass ein Arbeitgeber sich zivil- und strafrechtlich verantworten müsste oder andere Nachteile (z. B. bei der Erteilung von Betriebsbewilligungen) erfahren muss, falls er sich nicht an diese Regeln hält.

Die folgenden Ausführungen sind als Hinweise dafür gedacht, wie und unter welchen Umständen Überwachungs- und Kontrollmassnahmen in einer Firma oder der Verwaltung durchgeführt werden können. Da eine Rechtspraxis in diesem Bereich bis anhin fehlt, sind keine «gesicherten» und für alle Fälle geeigneten Antworten möglich.

Gesetzliche Grundlagen

Der Gesetzgeber schützt den Arbeitnehmer in diversen, zum Teil überlappenden Bestimmungen. Zu beachten sind insbesondere folgende Regelungen:

- Nach Art. 328 OR muss der Arbeitgeber alle nötigen Vorkehrungen treffen, um die Privatsphäre des Arbeitnehmers zu schützen und zu achten. Art. 328b OR schreibt vor, dass der Arbeitgeber nur Daten über den Arbeitnehmer bearbeiten darf, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind; im weiteren gilt das Datenschutzgesetz. Diese beiden Bestimmungen sind zwingend, d. h. der Arbeitgeber darf davon nicht zu Ungunsten des Arbeitnehmers abweichen, selbst wenn er den Arbeitnehmer vorab informiert oder sogar seine Einwilligung einholt (Art. 362 OR).
- Das Datenschutzgesetz (DSG) stellt generelle Regeln für die Bearbeitung von Daten über bestimmte oder bestimmbar Personen auf. Es schreibt zum Beispiel in Art. 4 vor, dass Daten nur «rechtmässig» beschafft werden dürfen, deren Bearbeitung verhältnismässig sein muss und nach Treu und Glauben zu erfolgen hat. Zudem dürfen Daten nur zu den Zwecken benutzt werden, die angegeben wurden, die sich aus den Umständen oder dem Gesetz geben. Das DSG definiert im weiteren die Pflicht, sich über die Richtigkeit der Daten zu vergewissern (Art. 5), die Pflicht, die Datensammlungen vor unbefugtem Zugriff zu schützen (Art. 7), das Auskunftsrecht (Art. 8 ff.) sowie das Prinzip, wonach Personendaten gegen den Willen der betroffenen Person oder entgegen den genannten Grundsätzen von Art. 4 und 5 nur dann bearbeitet werden dürfen, wenn ein Rechtfertigungsgrund, wie z. B. ein überwiegendes privates Interesse des Arbeitgebers oder durch Gesetz, vorliegt (Art. 12 ff.).
- Das DSG versteht unter «Personendaten» nicht nur den Inhalt von E-Mails, sondern auch deren Randdaten, ebenso Listen der von einer bestimmten oder bestimmbar Person angewählten Internet-Adressen. Die Bestimmungen des DSG gelten nicht nur für Daten über Arbeitnehmer, sondern für Angaben im Zusammenhang mit beliebigen anderen Personen.
- Nach Art. 26 der Verordnung 3 zum Arbeitsgesetz dürfen keine Überwachungs- und Kontrollsysteme zur Überwachung des Verhaltens des Arbeitnehmers am Arbeitsplatz eingesetzt werden. Sind solche Systeme nötig, so müssen sie so eingesetzt werden, dass sie die Gesundheit und Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigen.

Prävention

- Das Strafgesetzbuch stellt ferner in Art. 179 das unberechtigte «Öffnen» einer «verschlossenen» Schrift, in Art. 179 bis das «Abhören» und «Aufnehmen» fremder Gespräche und in Art. 179ter das unbefugte Aufzeichnen im Privat- und Geheimbereich einer Person auf einen «Bildträger» unter Strafe. Eine Anwendung dieser Bestimmungen auf Überwachungsmaßnahmen des Arbeitgebers bezüglich Internet ist zwar denkbar (z. B. im Falle von Internet-Telefonaten), steht in der Regel aber nicht zur Diskussion. In Art. 179novies sieht das Strafgesetzbuch ferner eine Strafe für das unbefugte Beschaffen von Personendaten vor.

Auch der Arbeitnehmer hat Pflichten. Er muss die ihm übertragenen Arbeiten sorgfältig ausführen und die berechtigten Interessen des Arbeitgebers wahren, d.h. er darf das in ihn gesetzte Vertrauen nicht ausnützen oder verletzen (Art. 321a OR). Er muss auch die Weisungen des Arbeitgebers befolgen (Art. 321d OR) und ist für Schäden verantwortlich, die er dem Arbeitgeber absichtlich oder fahrlässig zufügt (Art. 321e OR). Stellt sich die Frage, ob eine bestimmte Form der Überwachung oder Kontrolle zulässig ist, so werden diese verschiedenen Rechte, Pflichten und berechtigten Interessen des Arbeitgebers und des Arbeitnehmers gegeneinander abgewogen.

Berechtigte Interessen des Arbeitgebers im Zusammenhang mit den hier diskutierten Massnahmen werden in den meisten Fällen die Wahrung der Sicherheit, die Vermeidung von Haftungsfällen, der zweckgemässe Umgang mit den Ressourcen sowie die Geschäfts- und Leistungskontrolle sein. Die Interessen des Arbeitnehmers sind vor allem der Schutz seiner Privatsphäre und die Verhinderung von psychischem Stress durch Überwachungsmaßnahmen.

Verletzt somit ein Arbeitnehmer gewisse Pflichten, so können in einer bestimmten Situation Überwachungs- und Kontrollmassnahmen zulässig sein, die es unter anderen Umständen nicht wären. In einem anderen Fall wiegen die Interessen des Arbeitgebers so schwer, dass auch in die Privatsphäre des Arbeitgebers eingegriffen werden darf, ohne ihn vorher zu informieren. Es gibt für solche Fälle keine schematische Lösung, sondern höchstens gewisse Grundsätze.

Immerhin lässt sich sagen, dass für die Nutzung des Internets ähnliche Regeln wie für die Nutzung des Telefons gelten. Ist daher in einem Betrieb der private Gebrauch des Telefons aus Gründen der Produktivitätsverluste verboten, darf angenommen werden, dass dies analog für den privaten Internet-Verkehr gilt.

Die Verhinderung von Missbräuchen und Schadensfällen beginnt bereits mit den richtigen Vorbereitungs- und Präventionsmassnahmen. Von ihnen hängt aber auch ab, welche Überwachungs- und Kontrollmassnahmen benutzt werden dürfen.

Organisatorische und rechtliche Massnahmen

In jeder Firma und Verwaltung sollten die Verantwortlichen Regeln aufstellen, wie der Internet-Zugang und das E-Mail-System für private wie auch für geschäftliche Zwecke benutzt werden dürfen. Dies kann im Arbeitsvertrag, in Betriebsordnungen oder durch einzelne Anweisungen seitens des Arbeitgebers (bzw. der jeweiligen Vorgesetzten) geschehen.

Die meisten Betriebe regeln die private Nutzung nach den folgenden Varianten:

Private Nutzung auf Zusehen erlaubt
Private Nutzung nur ausserhalb der Arbeitszeit
Private Nutzung vollständig verboten (ausser in Notfällen)

Wird nichts festgehalten, so bedeutet dies normalerweise, dass die Benutzer die zur Verfügung stehenden Mittel und Systeme auch für private Zwecke benutzen dürfen, sofern die Arbeit darunter nicht leidet und die Ressourcen des Arbeitgebers nicht beeinträchtigt werden. Besteht allerdings eine Regelung für den privaten Telefonverkehr, so ist diese analog anzuwenden. Es ist auch denkbar, dass Unternehmen die private Nutzung zwar zulassen, dies jedoch nur an spezifischen Internet-Stationen, oder aber die Mitarbeiter verpflichtet sich, private E-Mails über E-Mail-Systeme abzuwickeln, die via Browser vom betriebseigenen E-Mail-System unabhängig funktionieren (wie Hotmail, GMX etc.).

Auch die Beschränkung (und Kontrolle) der geschäftlichen Nutzung kann nötig oder sinnvoll sein. Folgende Varianten werden benutzt:

Nutzung nur mit Erlaubnis des Vorgesetzten
Nutzung nur dort, wo dies geschäftlich sinnvoll und angemessen erscheint

Wird nichts festgehalten, ist jede geschäftliche Nutzung erlaubt, die sich aus dem Arbeitsauftrag des Arbeitnehmers ergibt.

Der Arbeitgeber darf und sollte auch Vorschriften aufstellen, wie die verschiedenen Internet- und E-Mail-Dienste benutzt werden dürfen. Er kann zum Beispiel Kettenbriefe ver-

bieten, den Versand von Werbung, das Öffnen von Programmen aus dem Internet oder E-Mail-System, das Versenden zu grosser Dateien, E-Mails an zahlreiche Empfänger gleichzeitig, den Einsatz von dem Betrieb nicht angemeldeten Verschlüsselungsprogrammen, das Eintragen von Firmenadressen in irgendwelchen Internet-Datenbanken, die Verwendung firmeninterner Passwörter etc.

Nebst dem reinen «Surfen» und Verkehr mit E-Mails gelten die Vorschriften des Arbeitgebers auch für andere Nutzungsformen wie etwa den Einsatz von Newsgroups oder das «Chatten» über Plauderboxen oder Kurzmittelungsdienste wie ICQ. Gegebenenfalls ist darauf hinzuweisen, dass nicht nur das Plaudern mit externen Personen untersagt ist, sondern auch betriebsinternes «Chatten» zu Produktivitätsverlusten führen kann und daher nicht erlaubt wird.

Will sich eine Firma oder Verwaltung auf solche Vorschriften berufen können, ist es wichtig, dass sie diese klar kommuniziert und für deren Einhaltung sorgt. Wichtig ist auch, dass ein Betrieb die Mitarbeiter über die Risiken der verbotenen Handlungen aufklärt. Schliesslich sollen Unternehmen darauf achten, dass disziplinarische Sanktionen bei Verstössen gegen Nutzungsregeln nur dann möglich sind, wenn diese genügend konkret «angedroht» wurden, der Arbeitnehmer den «Tarif» also kennt.

Technische Massnahmen

Nebst Vorschriften zur Nutzung empfiehlt sich auch der Einsatz von technischen Mitteln, um die Nutzung des Internets und der E-Mail-Systeme zu beschränken und Missbräuche zu verhindern.

Typische rechtlich zulässige Vorkehrungen zur Erkennung und Vermeidung von Missbräuchen und Gefahren in einem Betrieb sind:

- **Sperren:** Es ist dem Arbeitgeber erlaubt, die Nutzung seiner Internet-Zugänge und E-Mail-Systeme teilweise oder vollständig zu sperren oder mit Filtern zu versehen.
- **Protokollierung:** Es ist dem Arbeitgeber erlaubt, die Nutzung seiner Internet-Zugänge und E-Mail-Systeme zu protokollieren, sofern dabei keine Daten über die einzelnen Benutzer (oder einzelne, persönliche Arbeitsstationen bzw. feste IP-Adressen) aufgezeichnet werden. Weitergehende Protokollierungen sind möglich, aber nur unter bestimmten Voraussetzungen zulässig (siehe nachfolgend «Speicherung und Überwachung»).

■ **Scanning:** Es ist dem Arbeitgeber grundsätzlich erlaubt, alle Inhalte, die seine Systeme oder Netzwerke passieren sollen, von einem Computer schematisch nach Inhalten abzusuchen, die auf Gefahren (Viren, Würmer, Systemüberlastung etc.) oder Missbräuche (Betrügereien, Verrat von Firmengeheimnissen, Kettenbriefe etc.) hindeuten. Werden die Benutzer darüber vorab informiert, läuft der Vorgang vollautomatisch ab und werden die Inhalte bzw. etwaige nicht anonymisierte Auswertungen nicht aufbewahrt und auch keinen weiteren Personen (einschliesslich Systemverwalter) zugänglich gemacht, so ist dies aus Sicht des Datenschutzes problemlos. Will ein Betrieb mehr tun, so ist dies zwar durchaus möglich und kann auch erlaubt sein, doch müssen gewisse Voraussetzungen dafür erfüllt sein (siehe nachfolgend «Speicherung und Überwachung»).

■ **Zusätze:** Es ist dem Arbeitgeber grundsätzlich erlaubt, allen E-Mails, die über sein System bzw. Adresse versandt werden, Zusatzinformationen zur Vertraulichkeit, zur Bedeutung oder zur Rechtswirkung des Inhalts oder Kontaktangaben etc. anzufügen, sofern dies vollautomatisch und ohne Eingriff (bzw. Einsichtnahme) durch eine Person geschieht. Geschieht dies auch bei E-Mails, müssen die Mitarbeiter vorab informiert werden.

Wichtig: Systeme, die in einem Betrieb E-Mails verarbeiten oder Zugriffe auf Internet-Adressen verwalten, verarbeiten in der Regel auch Personendaten. Diese Systeme müssen daher gemäss Art. 7 DSGVO vor unbefugten Zugriffen und Manipulationen ausreichend geschützt sein. Das gilt für Zugriffe von innerhalb wie von ausserhalb des Betriebs und erfordert technische sowie organisatorische Massnahmen. Der Eidgenössische Datenschutzbeauftragte (3003 Bern, <http://www.edsb.ch>) bietet zu diesem Thema kostenlos einen «Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes» an.

Speicherung und Überwachung

Die Speicherung, Überwachung sowie die Kontrolle von E-Mails und Internet-Zugriffen der Arbeitnehmer durch den Arbeitgeber ist grundsätzlich nicht erlaubt, weil der Arbeitgeber damit auch

■ auf private Inhalte und Angaben stossen und
■ das Verhalten seiner Mitarbeiter überwachen kann.

Von dieser Grundregel gibt es aber drei wichtige Ausnahmen. Eine Speicherung bzw. Überwachung ist grundsätzlich zulässig

■ anhand unpersönlicher Daten,
■ bei einem konkreten Verdacht auf Missbrauch,
■ bei Vorliegen eines anderen, ausreichend guten Grundes.

Auch in diesen Fällen ist der Eingriff in die Privatsphäre auf ein Mindestmass zu beschränken, die gewonnenen Daten müssen vertraulich behandelt (und entsprechend gesichert) werden, und der Arbeitnehmer ist über die ihn betreffenden Aktivitäten zu informieren. Der Arbeitnehmer kann zudem jederzeit vom Arbeitgeber Auskunft darüber verlangen, ob Daten über ihn bearbeitet werden (Art 8 Abs. 1 DSGVO).

Unpersönliche Daten

Sowohl das Datenschutzgesetz wie auch das Arbeitsrecht schützen Arbeitnehmer als Individuen, aber nicht als Gruppe von Personen und nicht in ihrer betrieblichen Funktion als «Leistungserbringer».

Die Speicherung und Überwachung von E-Mails und Internet-Zugriffen ist somit überall dort zulässig, wo es nicht um den konkreten Menschen geht, sondern um eine ganze Gruppe von Personen (Abteilungen, ganzes Unternehmen) oder ausschliesslich um eine betriebliche Funktionsstelle (z. B. Support, Verkauf, Lager). Sobald aber private Inhalte oder Aktivitäten im Spiel sind oder das Verhalten (statt blosser Leistung) einer einzelnen Person kontrolliert werden kann, darf grundsätzlich nicht mehr überwacht werden.

Konkret heisst dies:

■ Die systematische, dauernde Überwachung der Internet-Zugriffe ist zulässig, sofern sie in Form einer Statistik erfolgt, aus der nicht ersichtlich ist, welche spezifische Person welche Inhalte oder Adressen abgerufen hat (siehe vorstehend). Dass einer solchen Statistik normalerweise Logbücher zugrunde liegen, mit denen der jeweilige

Benutzer sich sehr wohl ermitteln liesse, wird in der Regel akzeptiert, sofern diese Daten in der Auswertung anonymisiert werden (Art. 13 Abs. 2 lit e DSGVO).

■ Die Überwachung der Internet-Zugriffe einer einzelnen Person ist zulässig, soweit und sofern dies aus betrieblichen Gründen unbedingt erforderlich ist (z. B. zur Leistungskontrolle), der Betrieb eine private Nutzung vollständig untersagt hat und deshalb nicht mit privaten Zugriffen rechnen muss sowie der betroffene Arbeitnehmer vorab informiert wurde (ob im Einzelfall oder generell, ist umstritten). Eine systematische Überwachung einzelner Personen ist in der Regel nicht zulässig, weil dies einerseits eine verbotene Verhaltenskontrolle bedeuten würde und andererseits normalerweise nicht nötig ist. Meist genügt vorübergehende, stichprobenartige Kontrolle.

■ Die Speicherung und Überwachung der ein- und ausgehenden E-Mails mit der Empfänger- bzw. Absenderadresse einer Funktionsstelle (z. B. verkauf@firma.ch oder info@firma.ch) ist zulässig, weil der Arbeitgeber hier nicht mit privaten E-Mails rechnen muss. Kommt ein solches dennoch vor, muss dieses nach Möglichkeit ungelesen dem betreffenden Mitarbeiter weitergereicht und alle Kopien gelöscht werden. Eine Verhaltenskontrolle ist auch im Falle von unpersönlichen E-Mails nicht erlaubt.

■ Die Speicherung der ein- und ausgehenden E-Mails des Postfachs einer spezifischen Person ist zulässig, sofern dafür gesorgt wird, dass normalerweise nur diese Person auf die Daten Zugriff hat.

■ Die Überwachung des E-Mail-Ausgangs einer spezifischen Person (z. B. vorname.name@firma.ch) ist nur dann zulässig, soweit und sofern dies aus betrieblichen Gründen wirklich nötig ist (z. B. zur Dokumentation von Geschäftsvorgängen), der Betrieb das Versenden privater E-Mails vollständig untersagt hat oder er bei den überwachten E-Mails nicht mit privaten Inhalten rechnen muss und der betroffene Arbeitnehmer vorab informiert wurde. Diese Überwachung darf nicht für eine Verhaltenskontrolle benutzt werden. Nicht mit privaten Inhalten gerechnet werden muss, wenn das E-Mail-System zum Beispiel nur jene E-Mails der Überwachung zuführt, die über eindeutige Kennzeichen verfügen, die sie als geschäftliche Post ausweisen (z. B. eine Bearbeitungsnummer oder Geschäftsreferenz). Es wäre jedoch nicht zulässig, wenn der Überwachende die E-Mails von Hand aussortiert, weil er dabei auch von etwaigen privaten E-Mails Kenntnis nehmen würde.

■ Der E-Mail-Eingang einer spezifischen Person (z. B. vorname.name@firma.ch) darf in der Regel nicht überwacht werden, weil damit gerechnet werden muss, dass die genannte Person auch persönliche E-Mails erhält und solche den (betriebsexternen) Absendern nicht verboten werden kann. Soll auch eingehende Post überwacht werden können, so könnten zum Beispiel «anonyme» Empfangsadressen mit reinen Funktionsbezeichnungen verwendet werden. Möglich ist auch eine vollautomatische Aussortierung von eindeutig als geschäftlich gekennzeichneten E-Mails (z. B. solche, die über eine Bearbeitungsnummer verfügen). Dies muss maschinell und nicht durch Dritte geschehen, denn bereits die Information, dass eine bestimmte Person eine private E-Mail von einer bestimmten anderen Person erhalten hat, ist als Privatsache durch das Datenschutzgesetz geschützt.

■ Die allgemeine Überwachung von Chat-Boards (Plauderboxen) und Diskussionsforen ist zulässig, sofern und soweit sie «öffentlich» (z. B. in Form einer Support-Diskussionsdatenbank auf der Website eines Unternehmens) oder firmenintern für alle Mitarbeiter offen sind. Es darf dabei aber keine Verhaltenskontrolle der Mitarbeiter stattfinden. Private Chats sind wie E-Mails zu behandeln; auch hier darf der Arbeitgeber gegen Missbrauchsfälle vorgehen, muss aber ansonsten die Privatsphäre seiner Mitarbeiter wahren.

Hat der Arbeitgeber personenbezogene Daten gesammelt, so muss er diese löschen, sobald er sie nicht mehr benötigt. Mit einer Überwachung gleichgesetzt ist die Weiterleitung von persönlicher Post an andere Mitarbeiter im Betrieb, so etwa im Falle von Abwesenheiten des Empfängers. Es bleibt diesem natürlich unbenommen, selbst eine automatische Weiterleitung seiner Post zu aktivieren, die dann eben auch möglicherweise persönliche E-Mails weiterleitet. Ohne sein Einverständnis ist eine automatische Weiterleitung aber normalerweise nicht zulässig.

Werden auf diese Weise Missbrauchsfälle entdeckt, so ist eine weitergehende Überwachung zulässig, die jedoch nach einem spezifischen Schema ablaufen muss (siehe nachfolgend).

Missbrauchsfälle

Kommen Missbräuche vor oder werden solche vermutet, so können diese Überwachungs- oder Sicherheitsmassnahmen rechtfertigen, bei denen in die Privatsphäre eines Arbeitnehmers eingegriffen wird. Wiederrum muss eine Interessensabwägung vorgenommen werden, wobei neben den privaten Interessen des Arbeitgebers auch die öffentlichen Interessen berücksichtigt werden können (namentlich im Falle einer Straftat).

Zu unterscheiden ist zunächst nach der Missbrauchsart:

■ Arbeitsvertragswidriges Verhalten: Gemeint sind Fälle, in denen ein Mitarbeiter «nur» gegen Internet-Nutzungsbestimmungen des Betriebs oder direkte Weisungen des Arbeitgebers verstösst (z. B. privates Surfen trotz Verbot).
■ Rechtswidriges Verhalten: Gemeint sind Fälle, in denen ein Mitarbeiter das Internet für Straftaten oder andere unerlaubte Handlungen benutzt (z. B. Verbreiten von Computerviren, Betrug etc.).

Wird nicht ein rechtswidriges Verhalten, sondern lediglich ein Verstoß gegen die Internet-Nutzungsregeln vermutet, so dürfen auf diesen Verdacht hin nicht die bereits bestehenden Aufzeichnungen nach «Beweisen» durchforstet werden. Im Falle von Internet-Zugriffen ist stattdessen folgendes Vorgehen nötig:

1. Die Mitarbeiter werden darauf aufmerksam gemacht, welche Nutzungsarten toleriert werden und welche nicht. Das kann in allgemeiner Form an alle Arbeitnehmer geschehen.
2. Die Internet-Nutzung wird zwar im üblichen Rahmen protokolliert, die Auswertung erfolgt jedoch in anonymer Form, d. h. nicht bezogen auf spezifische Anwender.
3. Zeigt die Auswertung, dass es im Betrieb zu Missbräuchen kommt, die nicht geduldet werden sollen, so muss dieser Umstand den Mitarbeitern erneut mitgeteilt werden. Zugleich wird angekündigt, dass fehlbare Mitarbeiter fortan persönlich ermittelt und disziplinarisch bestraft werden.
4. Halten die Missbräuche an, so hat eine dafür verantwortliche Person anhand der (seit der letzten Warnung erstellten) Protokolle die fehlbaren Mitarbeiter zu ermitteln. Deren Namen dürfen aber nur den für die Disziplinierung verantwortlichen Vorgesetzten genannt werden, nicht aber an andere Mitglieder des Kaders noch an andere Personen.

Missbräuche elektronischer Post sind schwieriger zu ermitteln. In gewissen Fällen decken sich diese Missbräuche von selbst auf, so etwa wenn fehlbare Mitarbeiter unerlaubte E-Mails versehentlich an falsche Adressen versenden.

Grundsätzlich darf der Arbeitgeber von sich aus aber nur aktiv werden, wenn konkrete Verdachtsmomente gegen einen Mitarbeiter vorliegen (z. B. einen besonders hohen Speicherplatzbedarf für das Postfach, wie es Bild-, Musik- und Videodateien verursachen).

In solchen Fällen muss einerseits der betroffene Mitarbeiter vorab über den Verdacht informiert und dazu angehört werden. Er kann aber nicht gezwungen werden, etwaige persönliche E-Mails preiszugeben. Wird der Verdacht nicht ausgeräumt, so muss dem Mitarbeiter angekündigt werden, dass seine E-Mail-Aktivitäten künftig stichprobenweise überprüft werden. Diese Überwachung ist abzubrechen, sollte sich der bestehende Verdacht als unbegründet erweisen oder keine Verdachtsmomente mehr vorliegen.

Werden Missbräuche von Chat-Boards und Diskussionsforen vermutet, kann in derselben Weise wie bei der Überwachung von Internet-Zugängen und E-Mails verfahren werden. Ist ein übermässiger Gebrauch von Foren und Chat-Systemen das Problem, sollte wie bei exzessivem bzw. nicht zulässigem Surfen vorgegangen werden, weil eine systematische Überwachung der Forumsaktivitäten einzelner Mitarbeiter ohne Verdacht und Ankündigung nicht zulässig wäre. Das gilt für hausinterne wie für externe Foren. Werden in einem konkreten Fall widerrechtliche Inhalte vermutet und handelt es sich um private Foren oder Chat-Boards, so können die Regeln zur E-Mail-Überwachung zur Anwendung.

Für alle Fälle gilt also grundsätzlich: Eine Überwachung auf gut Glück ist nicht zulässig. Zudem muss der Mitarbeiter informiert und ihm die Möglichkeit zur Stellungnahme gewährt werden. Zwar können Verdachtsmomente es durchaus rechtfertigen, in die Privatsphäre des betreffenden Arbeitnehmers einzudringen, doch sollte auch dies nur soweit wie nötig geschehen. Was im Rahmen einer Überwachung in Erfahrung gebracht wird, muss vertraulich behandelt werden; es darf nur im Zusammenhang mit einer Disziplinierung des Missbrauchs benutzt werden.

Liegt ein konkreter Verdacht auf ein rechtswidriges Verhalten vor, so ist eine Überwachung normalerweise auch ohne vorherige Information des Betroffenen zulässig, doch sind ebenfalls Regeln einzuhalten.

■ Liegen Anzeichen für eine strafbare Handlung (z. B. Betrug, Rassismus, harte Pornografie, Ehrverletzung, Computerviren, Hacking) vor, die über die E-Mail- oder Internet-Systeme einer Firma oder Verwaltung begangen wurde, so sind die Strafverfolgungsbehörden einzuschalten. Sie entscheiden über das weitere Vorgehen und die nötigen Überwachungsmaßnahmen.

■ Besteht ein Verdacht auf unerlaubte, aber nicht strafbare Handlung (z. B. eine Persönlichkeitsverletzung in einem anonymen, betriebsinternen E-Mail), so ist es nicht zulässig, aus diesem Grund auf gut Glück die Postfächer oder Verbindungsdaten sämtlicher Mitarbeiter zu durchsuchen. Erforderlich ist auch hier ein konkreter Hinweis auf einen bestimmten Mitarbeiter. Wie in der Folge im einzelnen zu verfahren ist, ist bisher nicht geklärt worden. Eine sinnvolle Lösung wird sein, dass eine Überwachung bzw. Speicherung des Inhalts des Postfachs oder der Internet-Zugriffe der betreffenden Person zwecks Beweissicherung durch eine neutrale Drittperson vorgenommen wird. Diese Person muss dann feststellen, ob der Verdacht gerechtfertigt war und kann in diesem Fall ebenso als Zeuge bzw. Sachverständiger in einem Zivilprozess auftreten.

Der Arbeitgeber ist ausnahmsweise berechtigt, im Verdachtsfall selbst Massnahmen vorzunehmen (z. B. Backups), um etwaige Beweise zu sichern, falls ansonsten der Verlust der Daten droht. Deren Auswertung ist aber Sache der zuständigen Strafverfolgungsbehörden bzw. der neutralen Drittperson. Diese haben die Erkenntnisse vertraulich zu behandeln.

Andere Gründe

Es sind noch eine Reihe weiterer Fälle denkbar, in denen der Arbeitgeber die E-Mail-Daten und Internet-Zugriffsinformationen von Mitarbeitern speichern oder auswerten darf.

■ Systembetrieb: E-Mail- und Internet-Zugriffsdaten dürfen mitaufgezeichnet werden, soweit dies für den normalen Systembetrieb erforderlich ist. Dazu gehört etwa das Erstellen von Sicherheitskopien der Mail-Server-Daten oder die Protokollierung der Server- und Kommunikationsaktivitäten etwa zwecks Überwachung, Unterhalt und Verwaltung der Technik.

■ Sicherheit: Sicherheitsgründe können einen Eingriff in die Privatsphäre des Arbeitnehmers ebenfalls rechtfertigen, jedoch wiederum nur, soweit dies erforderlich ist. Ein

typischer Fall kann zum Beispiel die Auswertungen von Logbüchern zur Untersuchung von Hacker-Angriffen sein. Kursieren in einem Betrieb gefährliche Programme (z. B. Viren, trojanische Pferde, Würmer) oder andere vergleichbare Inhalte (z. B. Kettenbriefe), so kann es aus Sicherheitsgründen ebenfalls gerechtfertigt sein, in allen Postfächern der Mitarbeiter durch einen Computer (nicht Menschen) gezielt nach diesen Inhalten zu suchen, diese zu löschen und so das gesamte System zu säubern.

■ Leistungsabrechnung: Je nach Betrieb können die von einem Mitarbeiter versandten oder empfangenen E-Mails oder Zugriffe auf bestimmte Internet-Dienste für die Abrechnung seiner Leistung (z. B. zur Weiterrechnung an Kunden oder zur Lohnberechnung) nötig sein. Diese Auswertungen haben nach Möglichkeit entweder durch den Absender selbst oder maschinell zu geschehen. Es ist in der Regel nicht erforderlich, dass alleine zur Abrechnung von Leistungen eine Person das gesamte Postfach des betreffenden Mitarbeiters durchkämmen muss. Zudem wäre die Gefahr einer unerlaubten Verhaltenskontrolle gross.

Wichtig ist in allen Fällen, dass die Benutzer über diese Aktivitäten informiert werden, dass der Zugriff auf die Logbuch- und E-Mail-Daten genau geregelt erfolgt und technisch wie organisatorisch auf das nötige Mass beschränkt wird. Denn es ist zum Beispiel nicht erforderlich, dass die Geschäftsleitung eines Unternehmens Zugriff auf all diese Daten hat, wenn die Systemverwaltung von den dafür zuständigen Personen in der Informatikabteilung durchgeführt wird. Im Falle von Missbräuchen ist nach den beschriebenen Regeln zu verfahren, wobei es in der Verantwortung auch der zugriffsberechtigten Personen liegt, dass diese eingehalten werden.

Hinweise für Provider

Provider, die E-Mail-Postfächer oder Internet-Zugangssysteme für Dritte unterhalten, müssen zusätzliche Regeln bezüglich der Überwachung und Aufzeichnung von Daten ihrer Benutzer beachten. Für sie gilt neben den Bestimmungen des Datenschutzgesetzes und allfälliger vertraglicher Bestimmungen zusätzlich das Fernmeldegeheimnis.

In Art. 43 Fernmeldegesetz (FMG) heisst es dazu: Wer mit fernmeldedienstlichen Aufgaben betraut ist oder betraut war, darf Dritten keine Angaben über den Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern machen und niemandem Gelegenheit geben, solche Angaben weiterzugeben.

Diese Bestimmung gilt auch für Internet-Provider und erfasst sowohl den Inhalt der Daten, die Kunden über ihre Systeme austauschen, als auch die dazu gehörenden Randdaten wie etwa die Angaben über Absender, Absendezeitpunkt oder Empfänge von E-Mails.

Zwar dürfen und müssen Internet-Provider solche Angaben unter gewissen Umständen preisgeben, doch ist dafür entweder eine entsprechende Anordnung eines Strafrichters erforderlich (Art. 44 FMG) oder aber, mit Einschränkungen, das Einverständnis des Kunden (Art. 45 FMG). Der Kunde selbst kann aber lediglich Angaben über die für die Rechnungsstellung verwendeten Daten verlangen, wobei diese Informationen in der Regel nicht hilfreich sein werden. Immerhin können sie auch im Falle eines glaubhaft gemachten Missbrauchs vom Kunden einverlangt werden.

Weitere Fragen?

Die in dieser Broschüre behandelten Rechtsfragen im Bereich des Datenschutzes und des Arbeitsrechts lassen sich an dieser Stelle nicht abschliessend behandeln. Auch fehlt eine Gerichtspraxis. Firmen wie Verwaltungen werden in heiklen Situationen somit nicht nur Fingerspitzengefühl benötigen, sondern auch Erfahrungen im sinnvollen, vertraglichen Umgang mit dem neuen Medium Internet sammeln müssen. Nötigenfalls sollte ein Fachmann beigezogen werden, mit dem die geeigneten Internet-Nutzungsregeln und Überwachungs-Möglichkeiten noch konkreter diskutiert werden können.

Für Fragen rund um den Datenschutz steht zusätzlich auch der Eidgenössische Datenschutzbeauftragte, 3003 Bern, Telefon 031 322 43 95, <http://www.edob.ch>, zur Verfügung.
© Copyright by SYMANTEC Switzerland AG 21. Juni 2000