Artikel aus Security Journal, Hauszeitschrift der GAI Netconsult, November 2005

Content-Security

Wenn ein Mitarbeiter früher keine Lust zum Arbeiten hatte, hatte er ein Problem. Heute gibt es ja zum Glück das Internet und damit Unterhaltung für den ganzen Bürotag. Bis man mit Spiegel Online, Heise Newsticker und Bild Online durch ist, ist schon Kaffeepause. Den restlichen Tag kann man sich dann mit Chatten, dem Durchstöbern von Online-Foren oder Online-Games um die Ohren hauen. Kurz vor Feierabend bietet sich dann ein Blick ins abendliche Fernsehprogramm an.

Die Versuchung ist für die Mitarbeiter groß, die Arbeitszeit für die private Nutzung des Internet zu verwenden. Spätestens wenn die Mitarbeiter per Instant Messenger sehen, wenn Bekannte und Freunde online sind, sind Stunden privater Nutzung keine Seltenheit mehr.

Da jeder Internetnutzer das Netz auch mal zu privaten Zwecken verwendet, ergibt sich nach einiger Zeit auch dann ein Recht zur privaten Nutzung, wenn nichts geregelt ist oder sogar wenn zwar ein Verbot existiert, aber längere Zeit die private Nutzung ohne Hinweis auf das Verbot toleriert wurde.

Häufig bleibt es aber nicht bei der normalen Privatnutzung, sondern es kommen rechtliche Probleme hinzu. Mitarbeiter laden sich zum Beispiel nicht juugendfreie Inhalte auf den Server herunter, die von Kolleginnen als sexuelle Belästigung eingestuft werden könnten. Andere richten auf den hauseigenen Servern MP3-Archive mit urheberrechtsgeschützter Musik und den neuesten Kinofilmen ein. Schließlich gibt es Hobbyhacker unter den Mitarbeitern, die versuchen fremde Server zu knacken oder wenigstens abzuschießen.

Für solche Inhalte haftet das Unternehmen seit Ende 2001 nach dem Gesetz über den elektronischen Geschäftsverkehr auch dann, wenn die Geschäftsleitung und der zuständige Administrator keine Kenntnis von den verbotenen Inhalten haben. Es reicht für die Haftung des Unternehmens bereits aus, dass ein Mitarbeiter die verbotenen Inhalte auf Rechnern des Unternehmens speichert und andere dadurch zu Schaden kommen.

Mitarbeiter fühlen sich im Internet relativ anonym und verhalten sich daher häufig wie kleine Kinder, die sich unbeobachtet fühlen. Solange die private Nutzung explizit oder via Gewohnheitsrecht erlaubt ist, haben die Mitarbeiter damit sogar recht: die Aktivitäten der Arbeitnehmer im Internet dürfen nicht ohne weiteres überwacht werden.

Zum einen ist bei privater Nutzung des Internets am Arbeitsplatz das Teledienstedatenschutzgesetz (TDDSG) anwendbar, da dessen Anwendungsbereich vom Gesetzgeber nur bei dienstlicher Nutzung am Arbeitsplatz ausgeschlossen wurde. Laut TDDSG ist die Protokollierung von privatem Surfen nach Ende der Nutzung zu löschen, es sei denn, die Daten würden noch zur Abrechnung benötigt. Aber auch in diesem Fall ist die Nutzung der Daten nur zu Abrechnungszwecken erlaubt, eine Auswertung der Logdaten zu Überwachungszwecken mithin ausgeschlossen.

Zum anderen wäre die Kontrolle privaten Surfens zugleich ein Verstoß gegen das Fernmeldegeheimnis, das in Deutschland durch 3 Gesetze geschützt ist. Die besondere Wichtigkeit des Fernmeldegeheimnisses unterstreicht sein Verfassungsrang in Artikel 10 des Grundgesetzes.

Zweitens wird es durch den § 88 des neuen Telekommunikationsgesetzes vom 22. Juni 2004 geschützt. In der Begründung zum früheren Telekommunikationsgesetz ist die Feststellung enthalten, dass das Fernmeldegeheimnis auch für die private Nutzung am Arbeitsplatz gilt, was dennoch von einigen Juristen vehement bestritten wird.
Drittens zeigt auch die hohe Strafdrohung von bis zu fünf Jahren Freiheitsstrafe ohne Strafantrag in § 206 des Strafgesetzbuches die Wichtigkeit der Vertraulichkeit von persönlicher Kommunikation.

Der Unternehmer steckt hier also in einem Dilemma: einerseits haftet er ohne Kenntnis für die Speicherung illegaler Inhalte auf seinen Rechnern durch Mitarbeiter und beaufsichtigte Personen, andererseits wird er bei fehlenden Nutzungsbedingungen durch den Datenschutz und das Fernmeldegeheimnis daran gehindert, die Entstehung von Haftungsrisiken durch illegale Inhalte zu kontrollieren.

Daher sind hier Maßnahmen zu empfehlen, die diesen Widerspruch auflösen: Zunächst einmal sollte die private Nutzung des Internets im Unternehmen untersagt werden. Das funktioniert soweit der Mitarbeiter dies selbst beeinflussen kann, also in allen Bereichen bis auf den Empfang von privaten E-Mails, den der Mitarbeiter beim besten Willen nicht verhindern kann.

Das Verbieten privater Nutzung ist einseitig möglich, es ist dazu weder eine Unterschrift des Mitarbeiters noch eine Betriebsvereinbarung notwendig. Falls ein Betriebsrat existiert, besitzt dieser jedoch Mitbestimmungsrechte im Bereich Leistungs- und Verhaltenskontrolle. Das bedeutet, dass der Betriebsrat bei allen Regelungen zur Kontrolle der Logdaten zustimmen muss, ansonsten kann von beiden Seiten die Einigungsstelle angerufen werden, die im Streitfall eine Entscheidung trifft.

Um die Anzahl potentieller Missbrauchsfälle von vorneherein einzugrenzen, empfiehlt sich zudem der Einsatz von moderner Content-Filter-Software. Dabei sind technisch auch Umgehungen möglich, die sich unter Umständen wie ein Lauffeuer im Unternehmen bei allen bis auf Geschäftsleitung und EDV-Abteilung verbreiten. Daher ist es notwendig, die technische Umgehung von Filtersoftware beispielsweise durch anonyme HTTPS-Proxies oder SSH-Tunnel oder X-Windows Server besonders und unter Androhung arbeitsrechtlicher Maßnahmen zu verbieten.

Im Bereich E-Mail ist natürlich der Einsatz von Viren- und Spamfiltern erforderlich, da ohne einen wirksamen Spamfilter in den meisten Unternehmen das Medium E-Mail sonst nicht mehr benutzbar ist.

Der Einsatz von Virenfiltern ist für Unternehmen unverzichtbar, da diese im Unterschied zu Privatpersonen im Rahmen von Verträgen verpflichtet sind, das Vermögen ihrer Geschäftspartner nicht zu schädigen. Da es um die technische Notwendigkeit geht, den Betrieb aufrecht zu erhalten, ist dies unproblematisch datenschutzrechtlich nach § 31 BDSG und telekommunikationsrechtlich nach § 88 Abs. 3 Satz 1 des neuen TKG zulässig.

Bei Spamfiltern tauchen jedoch zahlreiche rechtliche Tücken auf: Ein Spamfilter entfernt keine Schadsoftware, sondern fischt aus den normalen Mails nur unsinnige Werbemails heraus. Wenn einmal eine Spam-Mail nicht herausgefiltert wird, ist dies in aller Regel nicht so schlimm. Schadensträchtig sind vor allem die sogenannten „False Positive“-Filterungen, bei denen eine unternehmenswichtige Mail als Spam aussortiert wird. Dabei kann es aus rechtlicher Sicht zu einer erheblichen Haftung kommen, wenn z.B. ein Dienstleister einen

Spamfilter betriebt, der einen wichtigen Auftrag des Kunden über einige Millionen Euro als Spam einstuft und gegebenenfalls ohne Warnung löscht.
Die vom Spamfilter zu treffenden Maßnahmen sind wiederum durch rechtliche Vorgaben stark eingeschränkt. Da die eingehenden Mails auch privat sein könnten, ist es wegen dem Fernmeldegeheimnis nicht möglich, die unter Spamverdacht fallenden Mails ohne Einverständnis der Mitarbeiter einfach kommentarlos zu löschen.
Umstritten ist, ob bei Vorliegen von besonderen Verdachtsmomenten der Weitertransport abgelehnt werden kann und dem Absender zurückgeschickt werden kann. Meines Erachtens ist dies rechtlich dann zulässig, wenn eine hohe Wahrscheinlichkeit dafür gegeben ist, dass es sich um Spam handelt, etwa wenn ein Mailrelay verwendet wird, das auf einer dynamischen IP-Adresse läuft, weil bei Providern mit fixen IP-Adressen das Versenden von Mails wesentlich seltener vorkommt als bei dynamisch eingewählten PCs. Dann muss allerdings mindestens der Absender von der abgelehnten Verbindung benachrichtigt werden. Eine zentrale Quarantänelösung ist ebenfalls problematisch, weil der Weitertransport nur mit einer Einsichtnahme eines dazu datenschutzrechtlich nicht befugten Administrators erfolgen kann.

Zusammenfassend kann nur jedem Unternehmen geraten werden, sich mit der Erstellung von organisatorischen Regeln zur Internet (und IT-) Nutzung im Unternehmen zu beschäftigen, um nicht beherrschbare Haftungsrisiken zu vermeiden.

Bisher sind nur Telekommunikationsfirmen explizit dazu verpflichtet, ein umfassendes Sicherheitskonzept zu erstellen (§ 109 Abs. 3 TKG) und einen Sicherheitsbeauftragten zu bestellen.

Da alle Unternehmen, die automatisiert personenbezogene Daten verarbeiten ab 10 Mitarbeitern, die mit personenbezogenen Daten arbeiten, einen Datenschutzbeauftragten benötigen, wird schon dieser die Unternehmen auf die zahlreichen technischen und organisatorischen Sicherheitsvorschriften des § 9 Bundesdatenschutzgesetz hinweisen, die für alle Unternehmen bindend sind.

Bei rechtlichen Fragen zur Content-Sicherheit und zur Erstellung von rechtlich abgesicherten unternehmensweiten Nutzungsbedingungen/Security Policies kann sich der Leser gerne an unsere Kanzlei wenden.

Ulrich Emmert
Kanzlei esb Rechtsanwälte Stuttgart
Mail: ulrich.emmert@kanzlei.de