

Liberales Argumente

- 18 / 21. September 2007 / 16. WP

- Online-Überwachung

Heimliche Online-Durchsuchungen greifen unverhältnismäßig tief in die Grundrechte der Bürger ein

Seit einiger Zeit wird die Einführung einer so genannten heimlichen Online-Durchsuchung gefordert. Mit Hilfe dieser Online-Durchsuchung soll Ermittlungsbehörden der Zugriff auf Computer gestattet werden, um diese Systeme zu durchsuchen und ggf. darauf befindliche Daten als Beweismaterial zu beschlagnahmen. Gegen die Online-Durchsuchung bestehen in rechtlicher und technischer Hinsicht erhebliche Bedenken.

Der Bundesgerichtshof (BGH) hat im Januar 2007 die heimliche Online-Durchsuchung mangels einer Ermächtigungsgrundlage für unzulässig erklärt. Nach der Entscheidung des BGH ist die verdeckte Online-Durchsuchung insbesondere nicht durch die Vorschriften über die Durchsuchung beim Verdächtigen gedeckt, weil die Durchsuchung in der Strafprozessordnung als eine offen durchzuführende Ermittlungsmaßnahme geregelt ist. Dies ergibt sich zum einen aus den Vorschriften des Durchsuchungsrechts zugunsten des Beschuldigten (Anwesenheitsrecht, Zuziehung von Zeugen) und zum anderen aus einem Vergleich mit den Ermittlungsmaßnahmen, die ohne Wissen des Betroffenen durchgeführt werden können, für die aber deutlich höhere formelle und materielle Anforderungen an die Anordnung und Durchführung bestehen (Telekommunikationsüberwachung, Wohnraumüberwachung).

Um eine heimliche Online-Durchsuchung durchführen zu müssen, müssen die Sicherheitsbehörden zunächst spezielle Spionageprogramme auf den verdächtigen Rechner installieren. Diese Programme müssen individuell geschrieben werden. Der Trojaner kommt als E-Mail-Anhang getarnt auf den Rechner oder von einer Internetseite, auf der man etwas herunter lädt. Das Programm startet sich dann von selbst und durchsucht die Daten auf der Festplatte. Ziel der Überwachung sind nicht nur E-Mails, sondern alle gespeicherten Daten, also auch gerade private Daten, wie Tagebücher oder digitale Urlaubsfotos. Berichten zufolge haben die Sicherheitsdienste inzwischen auch Spionageprogramme entwickelt, die über das Trojanerprinzip hinausgehen. Diese würden Computer automatisch nach gesicherten Einfallstoren durchsuchen, sobald sie sich im Internet anmelden. Nach getaner Arbeit deinstallieren sich die Spione selbst und verschwinden unerkant. Trojaner nutzen Sicherheitslücken, die nur mit großer Sachkenntnis

geschlossen werden können. So könnten Softwarehersteller bspw. gezwungen werden, Sicherheits-Updates für Betriebssysteme zurückzuhalten. Nur so kann gewährleistet werden, dass die Software der Ermittlungsbehörden auch tatsächlich zur Anwendung kommt.

Eine heimliche Online-Durchsuchung ist mit erheblichen technischen Problemen und Risiken verbunden. Es ist unklar, wie die Sicherheitsbehörden ihre Software auf die Computer von Verdächtigen aufspielen. Problematisch ist dabei, dass die Software der Ermittlungsbehörden auch von Kriminellen genutzt werden kann. Damit werden u. a. große Möglichkeiten für die Industriespionage eröffnet. Es ist nicht möglich zu erkennen, ob es sich um eine gute oder um böse Schadsoftware handelt. Im Ergebnis werden die Möglichkeiten der Sicherheitsbehörden, ihre Software auf die Computer der User aufzuspielen, das Vertrauen der Anwender in die Sicherheit des Internets erheblich erschüttern. Es ist auch möglich, dass die Software durch einen Virens Scanner entdeckt und dadurch die Maßnahme insgesamt vereitelt wird. Die Geeignetheit der heimlichen Online-Durchsuchung muss daher grundsätzlich in Frage gestellt werden. Es lässt sich auch nicht ausschließen, dass der „Bundestrojaner“ fehlerhaft ist und Daten auf dem Computer der Zielperson dadurch manipuliert, geändert und gefälscht werden. Hier ergeben sich vielfältige Probleme in Bezug auf den Beweiswert der ermittelten Daten. Anstatt die Internetsicherheit zu gefährden, sollte sich der Staat vielmehr auf die Bekämpfung der Computerkriminalität konzentrieren.

Darüber hinaus ist die Polizei personell völlig unzureichend ausgestattet mit IT-Spezialisten, die in der Lage sind, Online-Durchsuchungen durchzuführen. Die Spezialisten benötigen neben umfassenden technischen Fähigkeiten auch detaillierte Sprachkenntnisse, um die Kommunikation von Islamisten nachvollziehen zu können.

Es handelt sich bei der heimlichen Online-Durchsuchung unzweifelhaft um eine verdeckte Ermittlungsmaßnahme. Die Eingriffstiefe in Grundrechte ist bei der heimlichen Online-Durchsuchung erheblich, da sie im Gegensatz zu anderen verdeckten Ermittlungsmaßnahmen, wie der Telefonüberwachung und der akustischen Wohnraumüberwachung Informationen aus der Vergangenheit, der Gegenwart und der Zukunft erfasst. Es ist daher davon auszugehen, dass die Maßstäbe, die das Bundesverfassungsgericht in seinem Urteil vom 3. März 2006 über die akustische Wohnraumüberwachung aufgestellt hat, auch für die Online-Durchsuchung gilt. Auch hier wird die räumlich geschützte Privatsphäre der Betroffenen mit moderner Technik nach außen geöffnet. Der Wohnungsinhaber vertraut darauf, dass alle Sachen und Daten, die sich in seiner Wohnung befinden, vom Schutz der Wohnung umfasst werden. Dementsprechend werden vertrauliche Informationen, die auch dem Kernbereich der Persönlichkeit unterfallen und zuvor regelmäßig in körperlicher Form in der Wohnung aufbewahrt wurden, heute auch auf dem heimischen

Computer gespeichert. Daher muss es auch bei der heimlichen Online-Durchsuchung Schutzvorschriften für den Kernbereich der privaten Lebensgestaltung geben. Das Bundesverfassungsgericht hat dazu in seinem Urteil ausgeführt, die Überwachung müsse in solchen Situationen von vornherein unterbleiben, in denen Anhaltspunkte bestehen, dass die Menschenwürde durch die Maßnahme verletzt sei. Führe die Überwachung unerwartet zur Erhebung von absolut geschützten Informationen, müsse sie abgebrochen werden und die Aufzeichnungen müssen gelöscht werden. Jede Verwendung solcher im Rahmen der Strafverfolgung erhobener absolut geschützter Daten sei ausgeschlossen. Bei der heimlichen Online-Durchsuchung wird man auf eine Fülle von Daten stoßen, die den Bereich der Intimsphäre des Users betreffen. Es ist völlig unklar, wie diese Online-Durchsuchung als effiziente Maßnahme der Strafverfolgung zum Einsatz kommen soll, bei gleichzeitiger strenger Beachtung der Grundsätze des Bundesverfassungsgerichts zum Kernbereich der privaten Lebensgestaltung. Grundsätzlich ist es denkbar, eine Software zu installieren, die auf bestimmte Stichworte reagiert. Ein Ausfiltern nach Stichworten hat den Vorteil, dass die erfasste Datenflut begrenzt werden kann. Ein umfassender Kernbereichsschutz kann aber so auch nicht gewährleistet werden. Es wird sich daher oft nur im Nachhinein feststellen lassen, ob Informationen aus dem Kernbereich betroffen sind. Zu diesem Zeitpunkt ist der Grundrechtsverstoß jedoch bereits erfolgt. Vor diesem Hintergrund ist daher fraglich, ob die heimliche Online-Durchsuchung für die Kriminalitätsbekämpfung und die Strafverfolgung überhaupt einen Nutzen haben kann.

Es ist falsch zu behaupten, ohne die Möglichkeiten einer heimlichen Online-Durchsuchung könnten sich Terroristen unbehelligt im Netz bewegen. Bereits nach geltendem Recht gibt es Alternativen, die diese Online-Durchsuchung entbehrlich machen. Die Ermittlungsbehörden können einen Computer im Rahmen einer Durchsuchung beschlagnahmen oder zumindest die Festplatte kopieren. Eine Beschlagnahme kann stattfinden, soweit sie sich auf die Datenträger bezieht, auf denen Nachrichten gespeichert sind. Da bspw. E-Mails während des gesamten Übermittlungsvorgangs vom Absender bis zum Empfänger nahezu ständig auf irgendeinem Speichermedium festgehalten werden, ist eine Sicherstellung von Beweisgegenständen grundsätzlich möglich. Von dieser Möglichkeit der offenen Computerdurchsuchung wird jedoch in der Praxis nur sehr zurückhaltend Gebrauch gemacht. Grund hierfür ist die zum Teil unzureichende technische Ausbildung der Strafverfolgungsbehörden. Darüber hinaus ist bekannt, dass beschlagnahmte Computer aufgrund des Personalmangels bei der Polizei oft erst nach Jahren durchsucht werden.

Bereits heute ist darüber hinaus die Überwachung der E-Mail Kommunikation und die Suche danach, welche Webseiten ein Internetnutzer aufsucht, möglich. Kommunikation per E-Mail ist rechtstechnisch gesehen nichts anderes als

Kommunikation über Telefon. Beides fällt in den Bereich des Fernmeldeverkehrs. Hierzu gehören nicht nur herkömmliche Fernsprechverbindungen, sondern auch moderne digitale Formen der Datenkommunikation. Erfasst werden von der Überwachungs- und Aufzeichnungsbefugnis alle Vorgänge, die mit einem Datenübertragungsvorgang der Telekommunikationsanlagen in Verbindung stehen. Seit 2005 müssen alle Betreiber, die Telekommunikationsdienste für die Öffentlichkeit anbieten, d. h. öffentliche E-Mail Server betreiben, Möglichkeiten für die Überwachung bereitstellen. Provider sind verpflichtet, auf Anordnung die gesamte elektronische Kommunikation eines Kunden offenzulegen. Sobald eine E-Mail Überwachung angeordnet wird, muss sie unverzüglich durchgeführt werden.