

Liberales Argumente

- Nr. 38 / 29. Mai 2009 / 16. WP
- Innenpolitik

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

Seit 1. Januar 2009 hat das Bundeskriminalamt die Befugnis, verdeckt in informationstechnische Systeme einzugreifen, sprich heimliche Online-Durchsuchungen vorzunehmen. Damit kann das BKA sich mittels eines Trojaners auf dem Computer des Betroffenen einloggen, die vorhandenen Dateien kopieren, speichern und auswerten. Gegen die Online-Durchsuchung bestehen in rechtlicher und technischer Hinsicht erhebliche Bedenken.

Um eine heimliche Online-Durchsuchung durchführen zu können, 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.

Das Bundesverfassungsgericht hat am 27. Februar 2008 in seinem Urteil zum nordrhein-westfälischen Verfassungsschutzgesetz festgehalten, dass Online-Durchsuchungen zwar nicht generell mit dem Grundgesetz unvereinbar seien, jedoch nur unter besonders hohen Voraussetzungen erfolgen dürften: So sei die verfassungsrechtliche Zulässigkeit nur dann anzunehmen, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut beständen. Überragend wichtig seien Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen

oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühre. Grundsätzlich sei die heimliche Infiltration eines informationstechnischen Systems unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, müsse Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.

Das ist nicht gleichzusetzen mit einer Aufforderung an den Gesetzgeber, bis an die gerade noch zulässige Grenze der Verfassung zu gehen und das Instrument der heimlichen Online-Durchsuchung auch tatsächlich gesetzlich zu verankern. Vielmehr ist das Parlament in der Pflicht, genau zu prüfen, ob die Einführung einer derart schwerwiegenden Maßnahme überhaupt notwendig ist. Die FDP-Bundestagsfraktion beantwortet dies mit einem klaren NEIN. Die heimliche Online-Durchsuchung ist weniger mit einer Telekommunikationsüberwachung oder auch einer akustischen Wohnraumüberwachung zu vergleichen, sondern am ehesten mit einer Wohnraumdurchsuchung. Wie bei letzterer wird auch mittels der heimlichen Online-Durchsuchung auf Daten zugegriffen, die sich, wenngleich nicht auf einem Biedermeier-Sekretär, auf dem Schreibtisch (Desktop = engl. Schreibtischplatte) oder in Ordnern (Dateiordner auf der Rechnerstruktur) befinden.

Die FDP-Bundestagsfraktion hat der Erweiterung der Befugnisse des BKA u. a. auf Grund ihrer ablehnenden Haltung gegenüber der Online-Durchsuchung die Zustimmung verweigert.

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 Virenschanner 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 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 Übermittlungs-vorgangs 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 Fernspreverbindungen, 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.

Die FDP-Bundestagsfraktion sieht auch das Instrument der sog. Quellen-Telekommunikationsüberwachung kritisch. Auch bei diesem Instrument wird auf dem betroffenen Rechner ein Programm (Trojaner) installiert, der dort auf Daten zugreift. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 27. Februar 2008 darauf hingewiesen, dass damit „die entscheidende Hürde zum Ausspähen des gesamten Systems“ genommen sei. Die FDP-Bundestagsfraktion dringt daher auf die Schaffung anderer technischer Möglichkeiten, um erforderlichenfalls verschlüsselte elektronische Telekommunikation auf dem Übermittlungswege und gerade nicht vor bzw. nach der Verschlüsselung auf einem Zielrechner zu überwachen.