Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)466

STELLUNGNAHME

Berlin, 3. September 2008

Deutscher Industrie- und Handelskammertag

Zum Thema: **Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKA-Gesetz)**

A. Vorbemerkungen

Die Wirtschaft hat ein erhebliches Interesse daran, am deutschen Markt ohne das allgegenwärtige Risiko terroristischer Anschläge agieren zu können. Die innere Sicherheit für die Unternehmen, ihre Arbeitnehmer und ihre Kunden ist ein wichtiger Standortfaktor, den es zu erhalten gilt. Seitens der Unternehmen wird ausdrücklich anerkannt, dass die Polizeibehörden bei ihren Ermittlungsmethoden mit den veränderten technischen Rahmenbedingungen Schritt halten müssen, um auch weiterhin dieses Maß an Sicherheit gewährleisten zu können.

Zum Erfolg unseres Wirtschaftssystems gehört es, dass Unternehmer Meinungen, Pläne, Kontakte, Erfindungen und (Geschäfts-)Geheimnisse unbeobachtet von allgegenwärtiger staatlicher Kontrolle entwickeln bzw. äußern können. Sie müssen Vertrauen in den Staat haben, dass er den eingerichteten und ausgeübten Gewerbebetrieb schützt und achtet. Es muss streng darauf geachtet werden, dass diese Möglichkeiten nicht beim Versuch des Erhalts der inneren Sicherheit vor terroristischen Anschlägen geopfert werden.

Mit der Möglichkeit, durch eine installierte Überwachungssoftware in informationstechnische Systeme einzugreifen, werden auch die Interessen von Unternehmen betroffen. Der Deutsche Industrie- und Handelskammertag als Vertreter von ca. 3,5 Mio. Unternehmen sieht es daher als seine Aufgabe an, zu dem Gesetzentwurf Stellung zu nehmen. Er beschränkt sich hierbei auf die für die Wirtschaft relevanten Paragrafen. Grundlage seiner Stellungnahme sind die in Zusammenarbeit mit Unternehmen erarbeiteten Anmerkungen der Industrie- und Handelskammern.

Wir haben Zweifel, ob mit dem Gesetz ein angemessener Ausgleich zwischen diesen Werten und der inneren Sicherheit gefunden worden ist. Niemand könnte sich mehr sicher sein, ob er den geplanten geheimdienstlichen Maßnahmen ausgesetzt ist, egal wie gesetzestreu er sich verhält. Allein der nicht nur zufällige Kontakt – geschäftlich oder privat – mit irgendeiner Zielperson, die nicht ein-

Deutscher Industrie- und Handelskammertag e.V. | Zertifiziert durch CERTQUA nach DIN EN ISO 9001
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Fax 030-20308-1000 | Internet: www.dihk.de

mal einer Straftat verdächtigt werden muss, kann ausreichen, um die Maßnahmen auszulösen. Dies kann zu einer Angst vor Bespitzelung führen, die sonst für demokratische Staaten untypisch ist.

Auch mit einer legalen Installierung eines „Trojaners“ auf dem PC wird eine neue Dimension der Ausforschung erreicht. Wer bisher davon ausgehen musste, dass er belauscht, abgehört, beschattet oder einem Bewegungsprofil unterzogen wird, kann dies immerhin noch steuern. Wenn aber faktisch ein anonymer Ermittler unerkannt das Kommando über den eigenen PC übernommen hat, ist der Betroffene hilflos von einem korrekten Umgang mit dieser Machtbefugnis abhängig. Werden von diesem PC aus Dateien kopiert und versand, werden von dort beispielsweise illegale Seiten abgerufen, hat der Betroffene keinerlei Chance, im Falle von Ermittlungen seine Unschuld zu beweisen. Niemand wird ihm glauben, dass der Abruf nicht von ihm persönlich erfolgt ist. Hier ist der Betroffene in einem Maß ausgeliefert, wie es bisher in unserer Rechtsordnung nicht vorstellbar war. Selbstverständlich wird niemand einen solch Existenz vernichtenden Missbrauch unterstellen oder gar erwarten, andererseits werden gegenwärtig in regelmäßigen Abständen offensichtliche Missbräuche von entsprechenden Instrumenten aufgedeckt.

Aus dem Gesetzentwurf und seiner Begründung geht nicht hervor, ob gemäß dem Urteil des Bundesverfassungsgerichts vom 27.02.2008 (Az.: 1 BvR 370/07; 1 BvR 595/07) zum Verfassungsschutzgesetz NRW analog zu dem Kernbereich privater Lebensgestaltungen auch ein Kernbereich geschäftlicher und betrieblicher Geheimnisse besteht, der einen absoluten Schutz genießt. Daraus würde sich ergeben, dass Unternehmen wesentlich schlechter gestellt sind als Privatpersonen.

Nach unserer Auffassung können die gewünschten Daten und Informationen über des Terrorismus verdächtige Personen bereits über die Regelungen in bisherigen Gesetzen (z. B. Zugang zur Wohnung in Abwesenheit und „Offline-Installation“ einer Software analog zur Installation von Abhörgeräten) sowie die Verwendung von Nutzungsdaten bei der Telekommunikation so umfassend erhoben werden, dass es weiter gehender Ausforschungsmöglichkeiten nicht bedarf.

B. Zu den einzelnen Vorschriften

1. Zu § 20 k

Zunächst ist unklar, ob das BKA-Gesetz auch für juristische Personen gilt. Wenn § 20 k Abs. 4 von Personen spricht, sind wohl natürliche Personen gemeint. Da diese aber auch Unternehmer bzw. in Unternehmen tätig sein können, unterstellen wir, dass auch Unternehmens-IT-Systeme vom BKA-Gesetz betroffen sind.

Nach der Entscheidung des Bundesverfassungsgericht halten es Fachleute durchaus für möglich, dass IT-Systeme durch Infiltration geschädigt werden (vgl. Rn 240). Selbst wenn man nicht diese

Auffassung des Bundesverfassungsgerichts teilt, muss trotzdem klar geregelt und auch überwacht werden, dass und ob der Eingriff in die IT-Systeme vollständig entfernt wurde.

Die Gesetzesformulierung lässt unklar, was wie protokolliert wird. Ebenfalls ist nicht eindeutig geregelt, was nach Abschluss der Maßnahme geschieht, insbesondere wenn sie unangemessen war.

Wenn davon auszugehen ist, dass die staatlich verwendete „Trojaner" sämtliche Sicherheits- und Schutzmaßnahmen der IT-Systeme überwinden können, ist die Befürchtung nicht von der Hand zu weisen, dass auch Dritte auf diesem Wege an die Daten Fremder gelangen können. Durch die vom BKA verwendete Infiltrationssoftware entsteht ein hohes Risiko des Missbrauchs durch Hacker. Dadurch werden Betriebs- und Geschäftsgeheimnisse massiv gefährdet und Industriespionage erleichtert.

Nach Einschätzung von Fachleuten ist es eine Illusion, dass man nur an bestimmten Rechnern angegriffen werden kann. Bei der heutigen betriebsinternen Vernetzungen z. B. auch mit der Produktionssteuerung können durch den Eingriff in betriebliche IT-Systeme Produktionsausfälle verursacht werden.

Für den Versuch des Einschleusens eines Programms werden Informationen zu dem System benötigt, in das man eindringen möchte. Daher steht zu vermuten, dass das BKA solche Informationen nur mit Hilfe der entsprechenden Anbieter gewinnen kann. Hierdurch wird das vom Bundesverfassungsgericht in seinem bereits zitierten Urteil entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme grundlegend gestört.

Die Vermutung, dass es nur wenige Anwendungsfälle für die Infiltrationssoftware geben wird, erscheint vor dem Hintergrund der erheblich steigenden Zahl der Telekommunikationsüberwachung eine falsche Einschätzung zu sein. Auch dadurch wird das Risiko für die Unternehmen erheblich vergrößert.

2. Zu § 20 l

Nach Einschätzung von Fachleuten ist die Mitteilung der Endgerätekennung nach Abs. 4 Nr. 2 nicht immer möglich. Es besteht daher die Befürchtung, dass zukünftig von der Wirtschaft verlangt wird, dies zu ermöglichen. Damit werden die Wirtschaft wiederum erhebliche Kosten als „Handlanger des Staates" treffen.

Die Regelung in Abs. 6 verlangt – zu Ende gedacht, alles automatisch aufzuzeichnen und dem Richter die gesamte Aufzeichnung weiter zu geben.

Zur Umgehung der Überwachung wird statt der SIM-Karte künftig das Handy gewechselt.

3. Zu § 20 m

Die Verpflichtung für Telemediendiensteanbieter nach Abs. 2 verlangt einen ungeheueren Aufwand insbesondere für kleine und mittlere Unternehmen, die nicht über entsprechende technische Vorrichtungen oder ausreichendes Personal verfügen, um den Anforderungen nachkommen zu können.

4. Zu § 20 w

Vor dem Hintergrund der explosionsartig zunehmenden Überwachungsfälle von Telekommunikationsanlagen halten wir es für notwendig, zu den im BKA-Gesetz vorgenommenen Überwachungsmaßnahmen entsprechende Statistiken zu veröffentlichen. Nur so kann eine öffentliche Diskussion über die im Gesetz vorgesehenen massiven Grundrechtseingriffe geführt werden.