

Pressegespräch im Rahmen des Forums Sicherheit

Innere Sicherheit und Hightech

28. November 2007, Berlin

Prof. Dieter Kempf

Mitglied des Präsidiums

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien

– es gilt das gesprochene Wort –

Seite 2

Meine sehr geehrten Damen und Herren,

auch meinerseits ein herzliches Willkommen zu unserer Pressekonferenz „Innere Sicherheit und Hightech“.

Folie 2: „Sicherheit und Hightech: Drei Dimensionen“

Das Themenfeld „Sicherheit und Hightech“ besteht aus drei große Komponenten: dem Bereich der Sicherheitstechnologie, der staatlichen Kommunikationsüberwachung und der individuellen IT-Sicherheit von privaten und geschäftlichen Anwendern. Für die Innere Sicherheit sind in diesem Zusammenhang vor allem die ersten beiden Dimensionen wichtig – also Sicherheitstechnologie und Überwachung.

In unserem Pressegespräch steht die staatliche Kommunikationsüberwachung im Mittelpunkt. Hier werden derzeit wiederum drei Aspekte intensiv diskutiert: die Telekommunikations- und Internetüberwachung, die Vorratsdatenspeicherung und die Online-Durchsuchung. In diesen Bereichen hat sich in den vergangenen Monaten und Wochen politisch und rechtlich viel geändert oder wird sich noch ändern. Diese drei Teilbereiche werden oft bewusst oder unbewusst vermischt. Ich will mich heute bemühen, die Unterschiede zu verdeutlichen.

Zunächst gilt es, bei der Datenspeicherung und dem Zugriff von Ermittlern zwei Dinge zu unterscheiden: zum einen die Speicherung von Verbindungsdaten, also die Protokollierung, wer wann mit wem telefoniert hat. Zum anderen das Abhören und Speichern der Inhalte von Kommunikation.

Folie 3: „Der Staat hört mit“

Lassen Sie uns einen Blick werfen auf jene Fälle, in denen Ermittler die Inhalte von Kommunikation überwachen, gewissermaßen das klassische Abhören. Die Zahlen der Bundesnetzagentur zeigen, dass zur Strafverfolgung überwiegend Handy-Gespräche mitgehört werden. Hier gab es im vergangenen Jahr ein leichtes Plus. Nur in Ausnahmefällen waren Telefonate per Internet betroffen. Steigend sind insbesondere die Zahlen der Überwachung der Internetzugänge und E-Mails.

Folie 4: „Überwachung von Gesprächsinhalten und Daten“

Straftaten, die eine Überwachung rechtfertigen, sind derzeit etwa Mord und Totschlag, sexueller Missbrauch, organisierte Kriminalität, auch Geldwäsche und Drogendelikte. Ab nächstem Jahr kommen einige Straftaten hinzu, etwa Korruption, schwere Steuerdelikte, Menschenhandel und Doping. Es bleibt dabei, dass in allen Überwachungsfällen zunächst ein Richter zustimmen muss; bei Gefahr im Verzug genügt die Zustimmung eines Staatsanwalts.

Folie 5: „Kommunikation: Speicherung Verbindungsdaten“

Kommen wir zur Speicherung der Verbindungsdaten. Der Bundestag hat den entsprechenden Gesetzentwurf vor wenigen Wochen in zweiter und dritter Lesung verabschiedet, Änderungen sind nicht mehr zu erwarten. In dieser Tabelle sehen Sie, was sich Anfang 2008 bei der Sprachtelefonie bzw. Anfang 2009 auch in den weiteren technischen Kommunikationsformen bei der Vorratsdatenspeicherung ändert.

Künftig sind sechs Monate Speicherung eine generelle Pflicht, für Festnetz und Handy bereits ab 1. Januar 2008. Außerdem wird die Datenspeicherung ausgedehnt, sowohl bei Festnetz- und Handygesprächen als auch bei E-Mails und Internet-Telefonie. Es müssen nun zum Beispiel auch Handy-Standortdaten und die IP-Adressen von Internetnutzern gespeichert werden.

Folie 6: „BITKOM-Position: Vorratsdatenspeicherung“

Wenn dadurch eine Reihe schwerer Straftaten aufgeklärt werden kann, dann lehnen wir diese Eingriffe in die Privatsphäre nicht grundsätzlich ab. Die Netzbetreiber und Provider sind hier im Interesse der allgemeinen Sicherheit ein verlässlicher Partner. Dennoch möchten wir hinterfragen, wie praxisgerecht die neue Regelung ausgestaltet ist. Nun, im Großen und Ganzen hält sich die Bundesregierung mit ihrem Gesetzentwurf an die EU-Richtlinie, aber in einigen wenigen Punkten geht sie darüber hinaus. So könnten nach dem verabschiedeten Entwurf die Daten auch dazu verwendet werden können, z.B. Beleidigungsdelikte im Internet zu verfolgen.

Leider wurde auch unserer dringenden Bitte, mit der Vorratsdatenspeicherung erst 2009 zu beginnen, nur teilweise nachgekommen. Die Firmen müssen für die erweiterte Datenspeicherung technisch und personell aufstocken. Dies ist in den kommenden fünf Wochen einfach nicht möglich. Schließlich ist das Gesetz noch immer nicht offiziell verabschiedet und veröffentlicht.

Und die Netzbetreiber dürfen auf ihren Ausgaben nicht sitzen bleiben. Innere Sicherheit ist eine genuine Staatsaufgabe. Allein für die Vorratsdatenspeicherung muss die ITK-Branche einmalig bis zu 75 Millionen Euro in Technik investieren. Hinzu kommen jährlich Betriebskosten in zweistelliger Millionenhöhe.

Folie 7: Entschädigungszahlungen für die VDS

Deshalb haben wir schon lange eine Entschädigungsregelung gefordert. Bisher bekommen Telcos und Internet Provider nur einen Bruchteil ihrer Kosten erstattet. Sie werden für Auskünfte bezahlt wie Tatzeugen – mit 17 Euro pro Stunde. Zudem müssen sie diesen Aufwand fallweise nachweisen. Die Folge: Da der Nachweis für den Aufwand oft höher ist als die Entschädigung, verzichten die Unternehmen bislang in vielen Fällen auf die Erstattung.

Mit dem künftigen Gesetz wird es endlich eine offizielle Entschädigungsregelung geben. Es sind pauschale Zahlungen vorgesehen, die Einzelnachweise fallen weg.

Doch leider sind die derzeit angedachten pauschalen Sätze viel zu niedrig – der Aufwand für die Unternehmen liegt beträchtlich über den Entschädigungen. Zum Vergleich haben wir aufgelistet, welche Summen die Behörden in der Schweiz und in Österreich an die TK-Unternehmen zahlen. Die komplette Tabelle finden Sie in Ihren Unterlagen.

Folie 8: „Entschädigungszahlen im Vergleich I“

Drei Beispiele möchte ich herausgreifen: Um einen analogen Telefonanschluss in Österreich neunzig Tage zu überwachen, erhält der TK-Anbieter knapp 2400 Euro, also 25 Euro pro Tag. In der Schweiz umgerechnet rund 800 Euro, in Deutschland gut 300 Euro. Denn bei uns wird die Übermittlung nicht pro Tag, sondern pro Monat abgerechnet. Die Folge wird wohl sein, dass sich Überwachungen in Deutschland über einen längeren Zeitraum hinziehen als in anderen Ländern.

Nach derzeitigem Entwurf zahlt der deutsche Staat noch 20 Prozent weniger für die Einrichtung einer Überwachung, wenn es sich eine so genannte zentrale Anforderung handelt. Wenn also beispielsweise ein Landeskriminalamt eine Überwachung anordnet, und nicht die örtliche Polizei. Grundsätzlich begrüßen wir es, wenn zentrale Stellen mit dem nötigen Know-How eingerichtet werden, die die von den TK-Anbietern übermittelten Daten auch interpretieren können. Wir fordern daher: Statt eines Abschlags bei zentraler Anforderung einen realen Aufschlag auf den Grundpreis bei dezentraler Anforderung.

Folie 9: „Entschädigungszahlen im Vergleich II“

Ein ähnliches Bild sehen wir bei den Auskünften zu so genannten Verkehrsdaten: In Österreich gibt es eine Staffelung je nach Dauer der Überwachung. In Deutschland werden zeitunabhängig fix pro Kennung 30 Euro erstattet.

Ich möchte betonen, meine Damen und Herren: Es geht uns nicht darum, hier ein Geschäftsmodell für unsere Unternehmen zu entwickeln. Wir wollen nur gerecht entschädigt werden. Schließlich sprechen wir hier über Summen im zweistelligen Millionenbereich pro Jahr, die letztlich von allen ehrlichen Kunden aufgebracht werden müssen.

Folie 10: „Überwachung von Gesprächsinhalten und Daten“

Meine Damen und Herren,

lassen Sie uns nun zum umstrittensten Thema kommen, der so genannten Online-Durchsuchung. Bisher gibt es nur einen Gesetzentwurf mit informellem Status. Im BKA-Gesetz soll der Online-Zugriff auf Computer geregelt werden. Nach diesem Entwurf sind prinzipiell alle Computersysteme ein mögliches Ziel staatlicher Überwachung, auch mobile Endgeräte und die Zentralrechner von E-Mail-Anbietern, die von einem Verdächtigen genutzt werden. Die rechtlichen Voraussetzungen sind hier nicht so klar definiert wie bei der Telefonüberwachung. Bei der Online-

Durchsuchung soll es aber nicht um die Strafverfolgung gehen, sondern um die Abwehr „dringender Gefahren“ und terroristischer Aktivitäten.

Zum Vergleich haben wir hier die Voraussetzungen für die Anordnung eines Großen Lauschangriffs angeführt, also für das Abhören von Gesprächen innerhalb von Wohnungen. Hier gelten besonders hohe gesetzliche Hürden.

Folie 11: Online-Durchsuchung: BITKOM-Position

Wir sind der Meinung, dass die Leitlinien des Bundesverfassungsgerichts zum Großen Lauschangriff auch bei der Online-Durchsuchung eine Orientierung geben sollten. Die Vielfalt der Daten, auch sehr privater Daten, die Sie auf einer Festplatte finden können, ist ähnlich umfang- und facettenreich wie die Kommunikation innerhalb von Wohnungen. Deshalb liegt es auf der Hand, dass auch hier besonders enge Voraussetzungen für die staatliche Überwachung gelten müssen. Das muss im Gesetzentwurf deutlicher werden.

Wenn das gelingt, müssen wir nicht mehr davon ausgehen, dass uns eine breit angelegte Überwachung von PCs und Festplatten droht. Das Bundeskriminalamt spricht inzwischen von fünf bis zehn einschlägigen Fällen pro Jahr. Wenn in solchen Einzelfällen tatsächlich terroristische Gefahren vermieden werden können, dann sollten wir dieses Instrument nicht prinzipiell ablehnen. Ob es zu einer solchen Gefahrenabwehr kommt, muss aber Jahr für Jahr überprüft werden. Wenn Online-Durchsuchungen in der forensischen Praxis keine Ergebnisse bringen, muss man bereit sein, sich davon auch wieder zu verabschieden. Ein entsprechendes Gesetz muss also mit einem harten Kontrollverfahren und einem Verfallsdatum versehen werden. Wenn es seine Nützlichkeit in der Praxis nicht erweist, sollte es wieder abgeschafft werden. Zuerst aber brauchen wir genauere Informationen über die Pläne des Innenministeriums – und eine klare Definition der juristischen Voraussetzungen von Online-Durchsuchungen. An beidem fehlt es bisher.

In der Diskussion um die Technik von Online-Durchsuchungen sind dabei vor allem zwei Aspekte zu beachten. Schon mehrfach wurde diskutiert, ob in Deutschland tätige Anbieter von Sicherheitssoftware standardisierte Hintertüren für den Staat einbauen müssen, damit ein so genannter Bundestrojaner Durchlass findet. Aus unserer Sicht bringt das wenig und schadet viel: Kriminelle können mit einem Mausklick auf ausländische Anbieter von Firewalls und Virenschaltern ausweichen. Eine rein deutsche Gesetzgebung wäre in diesem Punkt zwangsläufig zum Scheitern verurteilt. Außerdem müssten die Unternehmen auf dem deutschen Markt Nachteile befürchten, weil eine Sicherheitssoftware mit offizieller Hintertür nun einmal wenig attraktiv ist. Das kann ich auch als Chef eines Unternehmens sagen, das selbst Sicherheitslösungen anbietet. Wenn es nur um eine niedrige zweistellige Zahl an Durchsuchungen geht, dann ist die Online-Durchsuchung ein Fall für qualifizierte Spezialisten der Ermittlungsbehörden, nicht für eine generelle Software-Schnittstelle.

Problematisch ist aus unserer Sicht im Übrigen nicht zuletzt der Zugriff auf die Server von E-Mail-Providern. Auch hier ist ein nationaler Ansatz wenig sinnvoll, denn Nutzer

Seite 6

können ohne die geringsten Probleme über ausländische Anbieter ihren Email-Verkehr abwickeln.

Folie 12: Online-Durchsuchung: Varianten und offene Fragen

Meine Damen und Herren,

auch zu anderen technischen und rechtlichen Aspekten existieren noch offene Fragen. Kommt das Überwachungsprogramm als Trojaner, der im Hintergrund Daten ausspäht und an die Ermittler weiterleitet? Oder als Key-Logger, der Tastatur-Anschläge protokolliert? Wie erfolgt die Installation? Diese und weitere technische Details wird das Bundeskriminalamt sicher nicht öffentlich diskutieren, aus verständlichen Gründen. Wir wollen aber darauf hinweisen, dass es hier eine ganze Vielzahl möglicher Varianten gibt.

In jedem Fall müssen die Kriminalisten Firewalls und Virens Scanner umgehen, und sie müssen dafür sorgen, dass ihr Programm nicht irrtümlich auf weitere Rechner gelangt. Eine Online-Durchsuchung ist weit komplexer, als ein Telefon abzuhören. Das scheint noch nicht überall bewusst zu sein.

Ein weiterer Punkt: Juristisch relevant ist die Frage, ob für Festplatten ähnliche Schutzkriterien wie für Wohnräume gelten. Hier sind sich die Experten noch nicht einig. Unter anderem wird die Frage aufkommen, ob Erkenntnisse aus der Gefahrenabwehr anschließend in Strafprozessen überhaupt genutzt werden dürfen.

All diese Fragen müssen noch beantwortet werden, um eine vernünftige und sachdienliche Regelung mit Augenmaß zu entwickeln.

Folie 13: Online-Durchsuchung: Beispiele aus dem Ausland

Meine Damen und Herren,

auch in unseren Nachbarländern Österreich und Schweiz wird derzeit über die Online-Durchsuchung diskutiert. Die unterschiedlichen Ansätze sehen Sie auf diesem Chart, und wir haben ein weiteres Beispiel aus den USA angefügt. Es macht deutlich, dass wir in Deutschland einen Sonderweg beschreiten, wie er in freiheitlich verfassten Demokratien ansonsten unüblich ist. Das sollte uns zumindest nachdenklich stimmen.

All diese Diskussionen müssen wir sicher schnell führen, aber wir dürfen sie nicht überhastet. Und wir brauchen dafür fachlichen Sachverstand, den der BITKOM gerne allen Beteiligten zur Verfügung stellt.

Herzlichen Dank.